UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

AUDITORÍA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DEL APLICATIVO Y BASE DE DATOS DE LA UNIDAD EDUCATIVA "ÁRBOL DE VIDA" EN SUS PROCESOS ACADÉMICOS.

AUTOR

MEJILLÓN GONZÁLEZ KENYA GISSELL

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Ing. Haz López Lidice, Msi

Santa Elena, Ecuador

Año 2023

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgtr.
DIRECTOR DE LA CARRERA

Ing. Lídice Haz López, Msi.
TUTOR

Lsi. Daniel Quirumbay Yagual, Msia.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez, Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Mejillón González Kenya Gissell, como requerimiento para la obtención del título de Ingeniera en Tecnologías de la Información.

La Libertad, a los 3 días del mes de marzo del año 2023

Ing. Lídice Haz López, Msi.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, MEJILLÓN GONZÁLEZ KENYA GISSELL

DECLARO QUE:

El trabajo de Titulación, Auditoría informática para evaluar la seguridad del aplicativo y base de datos de la unidad educativa "Árbol de Vida" previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

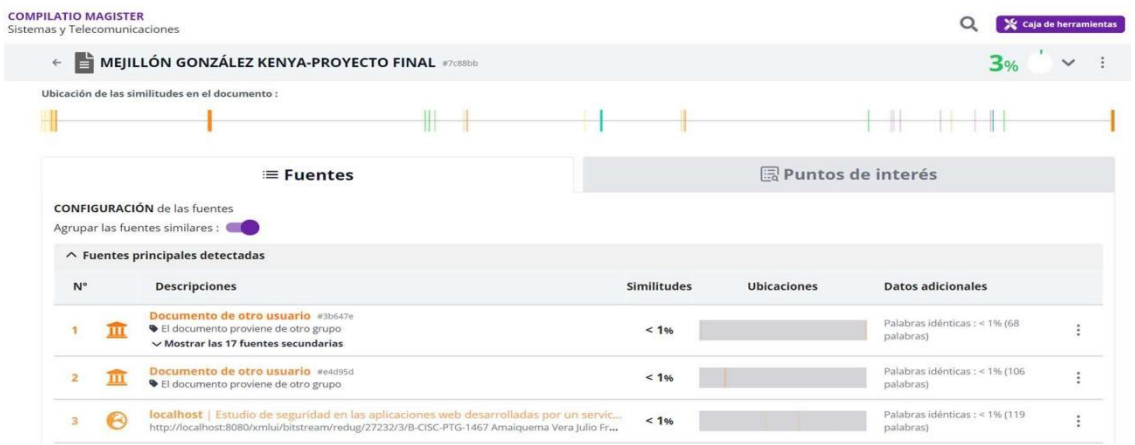
La Libertad, a los 3 días del mes de marzo del año 2023

Kenya Mejillón González

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado, Auditoría informática para evaluar la seguridad del aplicativo y base de datos de la unidad educativa "Árbol de Vida**",** presentado por el estudiante, Mejillón González Kenya Gissell fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Lídice Haz López, Msi

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

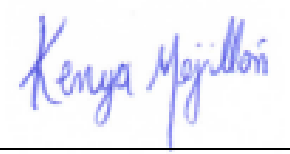
AUTORIZACIÓN

Yo, **MEJILLÓN GONZÁLEZ KENYA GISSELL**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 3 días del mes de marzo del año 2023



Kenya Mejillón González

AGRADECIMIENTO

Quiero expresar mi gratitud a todas aquellas personas que me han apoyado en este camino. En primer lugar, agradezco a Dios por darme la fortaleza y la perseverancia para culminar este proyecto.

También quiero agradecer a mi tutora de tesis, Ingeniera Lidice Haz Lopez, por su guía y apoyo en la dirección de este proyecto. Sus conocimientos y retroalimentación han sido invaluables para el éxito de esta investigación.

A mis amigos y familiares por su paciencia y comprensión a lo largo de este proceso. Sus palabras de aliento y su apoyo emocional han sido fundamentales para mantenerme enfocado en la meta.

Asimismo, quiero extender mi agradecimiento al personal de la institución que permitió la realización de esta auditoría, por brindarme acceso a sus recursos para el desarrollo de este trabajo.

Kenya Mejillón González

DEDICATORIA

Con gran alegría y gratitud, dedico este trabajo principalmente a Dios, por haberme bendecido siempre y permitirme alcanzar este momento tan importante en mi formación profesional.

También quisiera expresar mi profundo agradecimiento a mis padres, quienes me brindaron su incondicional apoyo durante todo mi proceso académico, dándome el ánimo necesario para enfrentar los desafíos que surgieron en este largo camino hacia la obtención de mi título de educación superior.

A mi familia, como un pilar fundamental en la vida de cada persona, que nos inculca los valores del amor y el respeto, y nos guía en el ejemplo de la lucha y la perseverancia.

A mi pareja y amigos, quienes me han apoyado constantemente desde el inicio de mi carrera hasta este momento en que llego a su fin, brindándome la motivación necesaria para alcanzar mis metas.

Kenya Mejillón González

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El proyecto, consistió en una auditoría informática al aplicativo web de la unidad educativa "Árbol de vida" que presenta problemas y fallas en su funcionamiento. El objetivo de esta auditoría fue evaluar la seguridad del aplicativo, identificar posibles vulnerabilidades y brindar un diagnostico a la institución

Para el desarrollo de este trabajo se utilizó metodología genérica que consta de 3 fases que son planificación, ejecución y cierre. Se realizaron escaneos con herramientas especializadas para identificar posibles vulnerabilidades, pruebas de funcionamiento del aplicativo y pruebas de seguridad, evaluando controles implementados.

Se realizó una recopilación de los resultados obtenidos de cada prueba, para la elaboración de un informe con un total de catorce observaciones y sus respectivas recomendaciones basadas en los estándares de seguridad internacionales. Estas recomendaciones buscan garantizar la seguridad del aplicativo y de la información que maneja, así como mejorar su rendimiento.

Palabras clave: aplicaciones web, seguridad, auditoría informática.

ABSTRACT

The project consisted of a computer audit of the "Árbol de Vida" educational unit's web application, which presented problems and failures in its operation. The objective of this audit was to evaluate the security of the application, identify possible vulnerabilities, and provide a diagnosis to the institution.

To develop this work, a generic methodology consisting of three phases was used: planning, execution, and closure. Scans were performed using specialized tools to identify possible vulnerabilities, application functionality tests, and security tests evaluating the implemented controls.

A compilation of the results obtained from each test was made to prepare a report with a total of fourteen observations and their respective recommendations based on international security standards. These recommendations seek to ensure the security of the application and the information it handles, as well as improve its performance.

Keywords: web applications, security, computer audit.

INTRODUCCIÓN

Con el auge de las tecnologías digitales, los aplicativos web se han convertido en una herramienta esencial para el funcionamiento de muchas organizaciones, ya sea para ofrecer servicios a los clientes o para el manejo interno de información. Sin embargo, a medida que el uso de estos aplicativos web se ha incrementado, también han aumentado los riesgos de seguridad informática, lo que puede poner en peligro la información y los recursos de la organización.

Es por ello que la auditoría informática se ha convertido en una herramienta importante para evaluar la seguridad de los aplicativos web ya que es un proceso sistemático que permite identificar y evaluar los controles de seguridad en una aplicación, con el fin de detectar vulnerabilidades y debilidades en la misma.

La unidad educativa Árbol de vida tiene un aplicativo web, integrado con Software Académico, Aula Virtual y Gestión administrativa y contable, el mismo que ha presentado fallas, mal rendimiento desde su adquisición, evidenciadas por personal del plantel. En este sentido, esta tesis se enfocará en el desarrollo de auditoría informática, para evaluar la seguridad del aplicativo web de la institución y luego establecer recomendaciones de seguridad.

Se utilizaran las metodologías de investigación diagnóstica y exploratoria, haciendo una revisión de trabajos similares al presente proyecto y una entrevista al personal encargado de la administración del aplicativo de la institución.

Las fases que se utilizarán en el presente proyecto son: planificación de actividades, ejecución de auditoría, cierre de auditoría que son parte de metodología genérica de auditoría informática, adaptada a las necesidades del proyecto para garantizar que se cubran adecuadamente los aspectos relevantes.

Se emplearán herramientas de seguridad de código libre para la ejecución de actividades y escaneos, tales como: Kali Linux, nmap, nikto, owasp zap. Las pruebas que se emplearán en el presente trabajo, están dirigidas para la evaluación del funcionamiento de interfaces del módulo matriculación e ingreso de notas que son los que soportan los procesos académicos de la institución, así mismo las pruebas de seguridad enfocadas en las vulnerabilidades más comunes en aplicativos web siendo: Cross site scripting,

Inyección sql, Ddos, clickjacking. Estas pruebas se realizaron con técnicas y herramientas específicas, diseñadas para identificar las vulnerabilidades.

Después de culminar todos los procesos y pruebas descritos anteriormente, se analizarán los resultados encontrados y se elaborará el informe final de auditoría, con las observaciones y recomendaciones basadas en estándares de seguridad como ISO 27001, NIST SP 800, COBIT 5.0, WCAG.

Este trabajo, se encuentra estructurado como se detalla a continuación:

El capítulo I, contiene los antecedentes, descripción del proyecto, objetivos, justificación y metodología del proyecto.

Así mismo, el capítulo II está conformado por el marco contextual, marco conceptual, marco teórico y componentes de la propuesta que abarca el desarrollo de las fases del proyecto que son la planificación, ejecución y cierre, mostrando los resultados, finalmente las conclusiones y recomendaciones.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1. ANTECEDENTES

En la actualidad, los sistemas y tecnologías de información han sido pieza clave durante el tiempo que se mantuvo el confinamiento por la pandemia, siendo un pilar fundamental para empresas e instituciones educativas, pasando a ser una herramienta principal para mantener las actividades escolares al día [1].

La Unidad Educativa "Árbol de Vida" se encuentra ubicada en la Parroquia José Luis Tamayo (Muey) del cantón Salinas, perteneciente a la provincia de Santa Elena, dedicada a brindar educación a niños de manera vespertina y anteriormente virtual, siendo una institución particular, maneja una base de datos de alumnos matriculados bajo una plataforma virtual administrada por el personal indicado por el rector [2].

Dicha institución cuenta con una tecnología fusionada en un solo aplicativo web constituida por un Software Académico, Aula Virtual y Gestión administrativa y contable, ya que, abarca con una gran cantidad de alumnos que son representados por sus respectivos padres de familias, los cuales, separan un cupo de matriculación para luego realizar el pago por la misma, teniendo en cuenta esto, el software cuenta con un módulo de pagos para registrar los ingresos recaudados por parte de los padres de familia, también lleva una nómina de notas donde se refleja el curso y las calificaciones de cada alumno asentadas por los docentes que inician sesión a la plataforma, teniendo múltiples aportaciones en cada espacio para que el estudiante complemente tareas, realice cuestionarios y lecciones virtuales.

En la entrevista realizada al encargado del mantenimiento del sistema (Ver Anexo 2), se pudo confirmar el uso que se ha dado en la plataforma y los posibles problemas que abarca la misma, dando por entendido que uno de los inconvenientes principales, es que no existe un sistema de resguardo de la información al solicitar una copia de seguridad, para prevenir a futuro una falla del programa y sea necesario el respaldo adecuado.

De la misma manera, entre las falencias que se detectaron con el personal docente, es que en ciertos navegadores el aplicativo no funciona correctamente presentando algunos problemas en sus procesos, como retrasos en el registro de notas, retardo en inicios de sesión o muchas veces intentos múltiples para poder ingresar a su perfil personal. Estos

inconvenientes generan pérdidas, que son en muchas ocasiones de los registros generados al momento que ingresan notas, creando inconveniente al visualizar las calificaciones en la plataforma.

La información que se determinó por medio del método de observación que se realizó al aplicativo (Ver Anexo 3), es que no contiene ninguna forma de realizar una actualización al mismo, tampoco cuenta con un espacio determinado para poder mejorarlo y la institución no contiene un método de raíz administrativa donde se pueda realizar cambios al sistema, esto provocará a futuro, que el programa comience a decaer en eficiencia y rapidez en el registro de información, así mismo, baja la protección a nuevos métodos de extracción de datos si surge un ataque.

En base a la investigación realizada, se halló que, en la Universidad de la Costa, ubicada en Colombia, se efectuó un trabajo de tesis para la auditoria de sistemas informáticos (SAC) en la Secretaría de educación departamental de la Guajira por Roger Raúl Foronda García y Gabriel Alfonso Galván Suarez, el cual posee como misión ser un canal de comunicación entre Docentes, Directivos Docentes, Estudiantes, Personal Administrativo y personal Educacional, teniendo como objetivo auditar los procesos del SAC, con el fin de mantener la certificación de ICONTEC en el marco del proyecto de modernización liderado desde el Ministerio de Educación Nacional [3].

Así mismo, a nivel nacional en la provincia de Azuay, Jaime Rafael Benítez Iglesias, realizó su sustentación de tesis con el tema “Elaboración de un manual de usuario de auditoría interna para la Unidad Educativa intercultural trilingüe Mushuk Kawsay del cantón el Tambo”, teniendo como finalidad establecer instrumentos operativos para la gestión de auditoría interna y realizar un manual que se elaboró de acuerdo a las necesidades y exigencias de la entidad, para dar un mejor funcionamiento institucional [4]. Este proyecto se basó en la orientación de los procesos educativos fundamentados en los niños, niñas, adolescentes y jóvenes; donde los maestros y los padres de familia unan esfuerzos por formar educandos capaces de cumplir papeles protagónicos dentro de la sociedad [4].

Por otro lado, en Ambato se realizó un trabajo de auditoría para la optimización del funcionamiento de los sistemas y equipos informáticos de la facultad de ingeniería en sistemas, electrónica e industrial realizada por Mayra Gabriela Acosta Jordán,

desarrollada a partir de la necesidad de conocer el estado en que se encuentra el funcionamiento de los sistemas y equipos informáticos, para lo cual, se realizó la ejecución de una auditoria informática utilizando una metodología basada en COBIT 4.1 (Control Objetives for information and related technology) para evaluar los controles del sistema de Control de Docentes y Laboratorio de la Facultad [5]. Usando aplicaciones de pruebas de cumplimiento y pruebas sustantivas cuyos resultados demuestran que el funcionamiento del sistema es factible y debido a sus permanentes modificaciones no permite que sea óptimo [5]. Los equipos del laboratorio satisfacen las necesidades de herramientas de software de los estudiantes, la infraestructura y cableado, para el óptimo funcionamiento de equipos y transmisión de datos [5].

Después de revisar los trabajos anteriores, se pudo determinar que la auditoría de sistemas en instituciones, es un proceso fundamental, ya que ayuda a identificar falencias en los controles de acceso, de la misma forma, minimiza los riesgos de accesos no autorizados y previene el robo o manipulación de información sensible perteneciente a la entidad. Por esta razón, el presente trabajo propone realizar la auditoría informática a los sistemas de matriculación e ingreso de notas de docentes de la Unidad Educativa "Árbol de vida", mediante herramientas que faciliten el análisis de los mismos, verificando la protección de datos que poseen.

1.2. DESCRIPCIÓN DEL PROYECTO

El presente trabajo se orienta a la Auditoría de un aplicativo Web que posee la Unidad Educativa "Árbol de Vida", situada en la parroquia José Luis Tamayo "Muey", del cantón Salinas, en la provincia de Santa Elena, el cual presentó múltiples inconvenientes de uso durante el tiempo de pandemia, siendo indispensable para las tareas cotidianas que enfrentaba la institución en el área administrativa, los docentes en el cumplimiento escolar, los padres de familia en la matriculación y pago de la misma, y finalmente, los estudiantes en la plataforma virtual.

El presente proyecto se realiza en base a una metodología genérica, adaptada con fases principales de auditoria informática, con el fin de identificar vulnerabilidades y hacer un análisis en aplicativo web. Se divide en las siguientes fases: planificación, ejecución y cierre, recomendaciones empleando buenas prácticas, varios consejos profesionales y

herramientas, tales como: nmap, nikto, owasp zap, slow loris, social-Engineer Toolkit, sensepost Jack, sqlmap.

FASE DE PLANIFICACIÓN

En esta fase se comprenderá todo el seguimiento del proyecto mediante un cronograma, el cual registra todas las actividades que se van a realizar durante todo el trabajo de auditoría, junto con las fechas y el tiempo que se tomará ejecutar cada etapa. En específico, su función es ayudar con la planificación y cumplimiento de entrega del trabajo en el tiempo previsto.

De la misma manera determinarán las herramientas que se utilizarán en la auditoría, las cuales dependerán de los programas que se establecerán para este proyecto y los recursos físicos que se utilizarán durante la auditoria.

FASE DE EJECUCIÓN

La fase de ejecución se centrará en la búsqueda de las partes susceptibles del aplicativo mediante un levantamiento de información, pudiendo ser este reconocimiento pasivo o activo, en ambos se implica la recopilación de información útil. En el pasivo, el auditor recolecta datos sobre un objetivo potencial con acciones sencillas y de bajo riesgo. Por otro lado, en el activo, el auditor busca por la red un blanco específico, que aún no tiene prefijado, de manera arriesgada.

Se obtendrá información necesaria para tener un indicio de los problemas que presenta el aplicativo web de la institución, reconocimiento de partes susceptibles, posteriormente una exploración en el aplicativo para conocer su funcionamiento, sus formas de navegación entre diversos navegadores (Google Chrome, Internet Explorer y Mozilla Firefox), su actividad en ejecución tanto en Windows como Linux, su forma de seguridad, etc.

Empleando las herramientas mencionadas anteriormente se realizaran diversos escaneos para cono los puertos abiertos, análisis SSL y vulnerabilidades. También se ejecutarán pruebas para evaluar funcionamiento de interfaces de ingreso de datos en el módulo matriculación e ingreso de notas y pruebas de seguridad en el aplicativo web, mencionadas a continuación: cross site scripting (XSS), inyección sql, pruebas de denegación de servicios e ingeniería social para evidenciar la seguridad de contraseñas

de los usuarios. Esta fase también comprende la recopilación de los resultados obtenidos en cada prueba.

FASE DE CIERRE

En esta fase, se comienza a interpretar y documentar la información obtenida en los pasos anteriores, elaborando un informe detallando las observaciones y sus respectivas recomendaciones basadas en estándares de seguridad, para que la institución lo analice y pueda solicitar a los desarrollares una mejor alternativa para dar una solución correcta, y poder salvaguardar su información privada, mejorando el funcionamiento del mismo.

Este proyecto contribuirá a la línea de investigación Tecnología y Sistemas de la Información (TSI), sub línea TSI en las organizaciones y en la sociedad [6].

1.3. OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Ejecutar una auditoría en el aplicativo web que soporta el proceso académico, mediante herramientas de auditoría informática, para identificar vulnerabilidades y proponer mejoras de seguridad.

1.3.2 OBJETIVOS ESPECÍFICOS

- Planificar las actividades a realizar durante la auditoría, mediante un cronograma que detalle el tiempo y los recursos a utilizarse.
- Evaluar incidentes de seguridad, mediante un testeo al aplicativo, para distinguir las partes susceptibles y brindar un diagnóstico de los procesos.
- Aplicar técnicas y herramientas de seguridad informática que permitan identificar vulnerabilidades en el aplicativo web y la base de datos.
- Elaborar un informe final de observaciones y recomendaciones describiendo los hallazgos encontrados durante la auditoria.

1.4. JUSTIFICACIÓN DEL PROYECTO

Los ciberataques son técnicas maliciosas que con el tiempo ha incrementado de manera antiética para diversos países incluyendo Latinoamérica, entre los países que en tendencia crece con este método delictivo el cual va en aumento de 24% en los último ocho meses

se refleja que entre la lista de países más vulnerable a estos ataque de ciber delincuencia lidera Ecuador con un 75% a diferencia de sus países vecinos como Perú, Panamá, Guatemala y Venezuela [7], entre los ataque más relevantes en el último año existieron fue en el Municipio de la capital del país el cual quedo afectado con una pérdida del 15% al 20% de información con el uso de un virus "ransomware" de la cepa "blackCat" [8].

El éxito de una organización radica en la capacidad para gestionar los riesgos, por esta razón, es importante realizar auditorías informáticas con la finalidad de determinar fortalezas y debilidades en el sistema de información de la entidad [9]. En el entorno global, la auditoría informática se realiza con un fin crítico, selectivo y sistemático, el cual propone evaluar la eficiencia y eficacia del uso adecuado de los recursos informáticos, gestión computacional y si estas, brindan un soporte adecuado a las metas y objetivos del negocio [9].

Las auditorías informáticas deben hacerse de manera periódica, de tal forma que puedan detectar falencias o fallas y luego ayudar a prevenirlas o mitigarlas [10]. Además, el avance de la tecnología, ha permitido integrar nuevos controles para las tecnologías de la información, haciendo uso de las técnicas y estrategias de análisis, permitiendo al auditor tener una herramienta de gestión, que le ayude en los procesos de la auditoría [10].

A causa de los incidentes de seguridad que suscitan en el aplicativo web de la Unidad Educativa "Árbol de vida", se propone realizar una auditoría informática a los sistemas de matriculación e ingreso de notas de docentes, permitiendo determinar las vulnerabilidades y amenazas de seguridad.

La ejecución de la auditoría informática en la entidad, beneficiará a las autoridades, docentes, padres de familia y estudiantes, analizando las opciones que posee la aplicación web, identificando vulnerabilidades, verificando si se cumplen todos los protocolos de seguridad, para posteriormente realizar medidas de corrección y acciones de prevención.

Los beneficiarios principales son las autoridades de la Unidad educativa, ya que son los encargados de administrar todas las opciones del aplicativo web y contarán con un informe detallado del análisis de las vulnerabilidades encontradas y posibles soluciones

para ayudar a mitigarlas o corregirlas, además de, proteger los datos que almacenan en la aplicación, brindando seguridad a los demás usuarios.

Así mismo, el presente proyecto beneficia a los docentes, padres de familia y estudiantes, ya que, son usuarios que acceden al sistema para realizar distintas funcionalidades, dependiendo del rol asignado. Este trabajo va dirigido para la Unidad educativa "Árbol de vida", ubicada en la Parroquia José Luis Tamayo (Muey) del cantón Salinas, en la provincia de Santa Elena, sin embargo, al ser una auditoría informática con vulnerabilidades y amenazas encontradas en un aplicativo web, se puede usar de referencia para analizar otros sistemas de otras instituciones.

La auditoría informática se alinea al Plan de creación de oportunidades, en el eje social, según el objetivo 7, el cual busca potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos los niveles [11]. Así mismo, en eje Seguridad Integral, según el objetivo 9 se basa en garantizar la seguridad ciudadana, orden público y gestión de riesgos [11].

1.5. METODOLOGÍA DEL PROYECTO

1.5.1. METODOLOGÍA DE INVESTIGACIÓN

Debido a la escasa información referente a proyectos de auditoria informática en aplicativos webs de instituciones educativas, identificando vulnerabilidades y amenazas, se utilizará la metodología de investigación de tipo exploratoria [12]. Después de realizar la búsqueda de trabajos similares, se determinaron las semejanzas y diferencias de los mismos, para emplearlos como guía en el presente proyecto.

Para determinar los inconvenientes existentes en el aplicativo web de la institución que abarca el presente proyecto, se emplearon diversas técnicas de recolección de información, centrándose en el lugar de los hechos, comprendiendo el contexto y analizándolo, para esto se empleó la metodología de investigación de tipo diagnóstica [12].

Con este estudio, se pretende tener un mayor número de vulnerabilidades encontradas en el aplicativo web, con el fin de proponer soluciones. Todo eso, se realizará aplicando la

metodología genérica de auditoría de aplicativos web en conjunto con ciertas pruebas de seguridad y así brindar un informe a la institución.

1.5.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para realizar la recopilación de información, con respecto a los incidentes de seguridad que posee la unidad educativa "Árbol de vida" en su aplicativo web, se utilizaron métodos de recolección de datos, para ello se aplicó la metodología de investigación de tipo diagnóstica [12]. Se realizó una entrevista dirigida al rector y encargado de la institución (Ver Anexo 2), determinando los inconvenientes que poseen en los sistemas de matriculación e ingreso de notas.

De la misma forma, se ejecutó la técnica de observación en el aplicativo que posee la unidad educativa (Ver Anexo 3), verificando las problemáticas existentes, conociendo los módulos del sistema y la funcionalidad de los mismos.

El presente trabajo de auditoría tiene como finalidad ayudar a la institución en el análisis de vulnerabilidades y amenazas de seguridad en los sistemas de matriculación e ingreso de notas. Además, realizar un informe que presente todo lo que halló, adjuntando medidas de prevención, para salvaguardar la información.

BENEFICIARIOS DIRECTOS	N° PERSONAS
Autoridades (Rector y vicerrector)	2
Docentes	13

Tabla 1: Beneficiarios directos

1.5.3. METODOLOGÍA DE DESARROLLO DEL PROYECTO

Con el objetivo de realizar una auditoría informática a los sistemas de matriculación e ingreso de notas de docentes de la Unidad Educativa "Árbol de vida", se propone utilizar una metodología genérica de auditoría informática en el aplicativo web que maneja la institución, permitiendo realizar un informe de las vulnerabilidades en el sistema que utilizan y medidas para prevenir dichos incidentes [13].

El presente trabajo tiene las siguientes fases:

FASE DE PLANIFICACIÓN.

En esta fase se detallarán puntos importantes como: cronograma de actividades a realizarse, procedimiento de pruebas, herramientas o métodos de ejecución dependiendo de las pruebas, recursos utilizables en la auditoria, equipo de trabajo, tipo de ejecución, duración, fechas de inicio, fecha fin y estado de la actividad.

FASE DE EJECUCIÓN

Comprende levantamiento de información donde se recolectará toda la información necesaria, tomando en cuenta los datos brindados por la entrevista y la observación realizada en el aplicativo web. Se realizará el mapeo de la aplicación con herramientas de escaneo, determinando las posibles vulnerabilidades, las mismas que se detallarán en la siguiente fase.

Se iniciarán pruebas y ataques siendo los siguientes:

- **Prueba de funcionalidad**
- **Cross Site Scrip Ting (Xss).**
- **Sql Inyection.**
- **Pruebas Stress (Ddos).**

Se recopila los resultados obtenidos en cada actividad que servirán para la elaboración del informe de la ultima fase.

FASE DE CIERRE

En esta fase, se plasma la información obtenida de la auditoría ejecutada del aplicativo, en una documentación, ya que, el presente trabajo se orienta al estudio de los problemas que se originan, dando carta abierta a la institución, si es viable recomponer el sistema, al analizar las recomendaciones brindadas bajo estándares de seguridad y accesibilidad..

CAPÍTULO II

2. LA PROPUESTA

2.1. MARCO CONTEXTUAL

2.1.1. ESCUELA DE EDUCACIÓN BÁSICA ÁRBOL DE VIDA

La Escuela de educación básica Árbol de Vida, es una institución privada ubicada en el cantón Salinas de la Provincia de Santa Elena en la República del Ecuador, la cual posee

7 docentes de género femenino, 3 docentes de género masculino, con un total de 10 profesores; 4 personas en el personal administrativo y 176 estudiantes en el establecimiento [14]. Las autoridades pertinentes del plantel, son: Douglas Martín Maldonado Caicedo (director), Mirna Elizabeth Soriano Quirumbay (secretaria general), Jean Carlos Maldonado Burbano (coordinador administrativo y financiero) [14].

Está localizada en el cantón Salinas de la Provincia de Santa Elena.

Figura 1. Ubicación geográfica de la unidad educativa.

2.1.2. MISIÓN

La Escuela de educación básica Árbol de Vida, se propone formar individuos con una educación de calidad, integral e innovadora, con el más alto nivel de enseñanza; fomentando de esta forma, el criterio de valores morales e independencia, de honestidad y justicia en los estudiantes; donde la excelencia académica **es** su horizonte y puedan ser capaces de enfrentar los nuevos retos que les presente la vida [14].

2.1.3. VISIÓN

Nuestra visión es ofrecer una orientación de calidad, para que el estudiante pueda desarrollar una formación innovadora e integral, que les permita ser personas centradas apegadas a los valores y principios; así como, usar estrategias pedagógicas que les facilite elevar y lograr un aprendizaje efectivo [14].

2.1.4. SEGURIDAD INFORMÁTICA EN SISTEMAS WEB DE UNIDADES EDUCATIVAS

Los sistemas de gestión educativa como base del proceso de enseñanza general, y la utilización de las tecnologías de información en la educación, tanto de manera pública o

particular, la implementación de tecnología es esencial para brindar una educación de calidad y con estándares de eficiencia e innovación [15].

La seguridad informática en las instituciones educativas, debe contener un sistema de gestión de seguridad de la información, en donde se contemplen parámetros como: ciclo de vida de los datos, además de un software especializado para dicho proceso. Por otro lado, hay normas que se deben cumplir desde las personas que manejan la información, hasta las que administran los sistemas [15].

Los riesgos en sistemas informáticos están relacionados con la seguridad de la información, debido a esto se ha convertido en una necesidad implementar protocolos de seguridad para la información, empleando procesos de autenticación, secuencia y encriptado de datos de las instituciones u organizaciones [16].

2.1.5. USO DE HERRAMIENTAS TECNOLÓGICAS EN LA COMUNIDAD ACADÉMICA

Actualmente la tecnología avanza grandes escalas, así mismo el desarrollo de herramientas tecnológicas ha optimizado las actividades en la vida cotidiana [17]. En el ámbito educativo, el uso de herramientas tecnológicas para realizar tareas académicas es común, ya que facilitan el proceso de enseñanza-aprendizaje de los estudiantes [17].
A continuación, se listan las herramientas tecnológicas que los estudiantes más utilizan:

- **Microsoft Word:** Procesador de textos, que permite manipular, guardar, imprimir y compartir información [18].
- **Power Point:** Es un programa de presentación, utilizado en diversos campos de la enseñanza, los negocios, entre otros, también permite agregar animaciones en texto e imágenes prediseñadas [19].
- **Microsoft Excel:** Es un software de hojas de cálculo y una herramienta avanzada de análisis y visualización de datos [20].
- **Gmail:** Servicio de correo electrónico, permitiendo acceder a servicios de la nube y sus beneficios [21].
- **Adobe Acrobat:** Es una familia de aplicaciones informáticas que fue diseñada para visualizar, crear o modificar archivos en formato PDF [22].

- **Google Chrome:** Es un navegador web gratuito, diseñado para realizar consultas en internet de una forma sencilla, rápido y seguro [23].
- **Google:** Es un motor de búsqueda, que permite recibir millones de búsquedas cada día a través de sus distintos servicios [24].
- **Avast:** Es un software antivirus inteligente, que detecta virus, malware, spyware, ransomware, phishing, entre otras amenazas [25].
- **Zoom:** plataforma que brinda servicio de videoconferencia basado en la nube que se utiliza para reunirse virtualmente con otras personas [26].
- **Moodle:** Plataforma de aprendizaje diseñada para proporcionar a docentes y estudiantes, un sistema para crear ambientes de aprendizaje personalizado [27].
- **Drive:** Servicio de almacenamiento de datos, guardados en la nube [28].

2.2. MARCO CONCEPTUAL

2.2.1. AUDITORÍA INFORMÁTICA

Una auditoría informática es la herramienta principal para dar a conocer el estado de seguridad en la que se encuentra una empresa o entidad, en relación con sus sistemas informáticos, acceso a internet y de comunicación [29]. Estas auditorías permiten la mejora de los sistemas, incrementando la ciberseguridad, siendo esenciales para poder garantizar el funcionamiento de la entidad y proteger la integridad de los datos que manejan [29].

2.2.2. SEGURIDAD INFORMÁTICA

La seguridad informática es conocida por ser la mejor aliada de las organizaciones, empresas y grupos con presencia online, de modo que les permite proteger su información y mantener su imagen y prestigio [30].

También es llamada ciberseguridad, que se dedica a proteger sistemas informáticos de amenazas internas y externas; las amenazas externas son las que provienen del entorno exterior en el que se encuentra el sistema, por ejemplo: virus, ataques informáticos, robos de información, entre otros; mientras que, las amenazas internas son provenientes del

propio sistema, como: exposición de credenciales, errores humanos, desactualización en el software, etc [31].

Es por esto, que la seguridad informática, es sumamente importante para detectar vulnerabilidades en los sistemas, detectando el peligro y conservando la confidencialidad e integridad de los sistemas informáticos [32].

2.2.2.1. TIPOS DE SEGURIDAD INFORMÁTICA

Los principales tipos de seguridad informática, se describen a continuación [30]:

Seguridad	Descripción
Hardware	Este tipo de seguridad está relacionada con la protección de dispositivos que se utilizan para proteger sistemas y redes; aplicaciones y programas de amenazas exteriores, frente a distintos riesgos.
Software	Empleado para salvaguardar los sistemas frente a ataques maliciosos de hackers y otras amenazas relacionadas con las vulnerabilidades que pueden presentar los softwares.
Red	Está relacionada con el diseño de actividades para proteger la información que sea accesible por medio de la red y que exista la posibilidad de que sea modificada, robada o usada incorrectamente.

Tabla 2. Tipos de seguridad informática.

2.2.3. SISTEMA WEB

Un sistema web también llamado aplicación web se define como una aplicación de software que se puede utilizar en un servicio web a través de internet o intranet desde un navegador; actualmente, el sistema web es muy empleado por razón de qué es muy práctica y rápida en el navegador web [33]. Pues, de hecho, las aplicaciones web evitan costos, lo que significa que no será necesario aprender a manejar nuevos programas que impliquen costos, pudiendo trabajar en cualquier lugar donde esté [33].

2.2.4. SISTEMA DE GESTIÓN ESCOLAR

La gestión escolar es una de las tareas que requiere mayor tiempo, ya que, para contar con una organización eficiente tanto a nivel administrativo como a nivel académico, se requiere de más esfuerzo para no sobresaturar la labor de los directivos [34].

La gestión educativa se conforma por tres dimensiones: la pedagógica – curricular, la administrativa – financiera y la operacional; en otras palabras, se puede decir que la gestión educativa hace referencia a la relación entre estrategias, estructura, capacidades del personal docente y objetivos de la institución [35].

Hoy en día existen herramientas digitales que ayudan a los directivos y docentes para optimizar el proceso de gestión escolar como los sistemas ERP, son programas que permiten la integración de las distintas áreas de gestión de una institución de formación: administrativa, financiera, comunicación, organización educativa, sistemas de calificación, entre otros [36] . En resumen, es un software creado para optimizar la gestión y coordinar los proyectos de diversas áreas, garantizando el buen funcionamiento del establecimiento [36].

2.2.5. PRUEBAS DE AUDITORÍA

Proceso llevado a cabo por un auditor externo o interno para evaluar la precisión y fiabilidad de los procesos de una empresa o entidad. Estas pruebas incluyen la revisión de documentos, entrevistas a empleados y la realización de pruebas específicas diseñadas para detectar errores o incongruencias en la información y todos los datos obtenidos sirven como evidencias comprobatorias [37].

2.2.5.1. PRUEBAS SUSTANTIVAS

Son pruebas de auditoría para obtener evidencia de la validez y propiedad de los procesos relacionado con exactitud, integridad de los datos. Su objetivo es tener evidencias suficientes para que el auditor emita juicio en los hallazgos [38].

Se pueden identificar 8 diferentes pruebas sustantivas [39]:

- Pruebas para detectar fallos en el procesamiento o de vulnerabilidades en la seguridad o privacidad.

- Prueba para garantizar la calidad de los datos.
- Prueba para identificar la consistencia de los datos.
- Confirmaciones de datos con fuentes externas.
- Prueba para confirmar la adecuada comunicación.
- Prueba para identificar falta de seguridad.
- Prueba para detectar problemas de legalidad.

2.2.5.2. PRUEBAS DE CONTROL

También conocida como prueba de cumplimiento es un procedimiento de auditoría, orientado, en verificar si el sistema de control interno de la empresa auditada está siendo aplicado de acuerdo a las especificaciones brindadas al auditor y con los objetivos del negocio; es importante, ayuda a conocer si las políticas implementadas por la administración se están cumpliendo correctamente [40].

2.2.6. CHECKLIST

Es una lista de tareas o puntos de verificación que se utilizan para evaluar la seguridad y el cumplimiento de los sistemas y procesos de informática. El objetivo es asegurarse de que todos los aspectos relevantes sean considerados y revisados durante la auditoría, y para asegurar la cobertura completa y consistente de todas las áreas de la evaluación. Estos checklists pueden incluir preguntas sobre la política de seguridad, la configuración del sistema, el monitoreo de seguridad, la gestión de parches y actualizaciones, entre otros [41].

2.2.7. VULNERABILIDAD

Es un punto débil o una debilidad en un sistema, red o aplicación que podría ser explotada por un atacante para causar daños, robar información o acceder a recursos restringidos; las vulnerabilidades pueden ser causadas por una serie de factores, incluyendo errores en el diseño o la implementación de software, la falta de parches o actualizaciones de seguridad, y la configuración incorrecta de los sistemas [42].

2.2.8. RIESGO

Es una posible amenaza o situación incierta que podría tener un impacto negativo en un sistema, red o aplicación. Los riesgos pueden ser causados por una variedad de factores, incluyendo errores humanos, fallos en el hardware o software, y ataques

malintencionados; la identificación y evaluación de riesgos es un aspecto importante de la auditoría de seguridad informática, ya que permite a los profesionales de seguridad tomar medidas para mitigar o prevenir la materialización de los riesgos y proteger los sistemas y los datos sensibles [43].

2.2.9. PROBABILIDAD

Es un concepto que se utiliza para medir la posibilidad de que un evento específico ocurra. Se refiere a la frecuencia con la que se espera que un evento ocurra en un período de tiempo determinado, se puede expresar en términos numéricos, se combina con la estimación del impacto potencial para determinar el nivel total de riesgo y tomar medidas para mitigar o prevenir los riesgos [44].

2.2.10. IMPACTO

Se refiere a las consecuencias negativas que pueden resultar de una amenaza o situación incierta, se utiliza para estimar la magnitud de los daños o pérdidas que podrían resultar de un evento específico; el impacto puede ser financiero, operativo, reputacional o de cumplimiento legal, entre otros [45].

2.2.11. NMAP

Nmap o mapeador de redes, es una herramienta de código abierto para explorar la red y auditar la seguridad; está diseñado para analizar de forma rápida grandes redes, aunque funciona bien contra equipos individuales; Nmap emplea paquetes IP en sus formas originales para determinar qué equipos se encuentran disponibles en la red, qué servicios ofrecen, qué sistemas operativos ejecutan, qué clase de filtros de paquetes o cortafuegos se están usando, así como otras características [46].

Generalmente, Nmap se utiliza en auditorías de seguridad, muchos administradores de redes o sistemas, lo encuentran muy útil para realizar deberes rutinarios, como puede ser: inventario de la red, planificación de actualización de servicios y monitorización del tiempo que los servicios o equipos se mantienen activos [46].

2.2.12. NIKTO

Nikto es un escáner de servidores web de código abierto y de uso gratuito que realiza escaneos de vulnerabilidades en servidor web, con la finalidad de buscar múltiples elementos, incluyendo archivos y programas maliciosos, buscando versiones

desactualizadas de software del servidor web [47]. Además, comprueba si hay errores de configuración del servidor y posibles vulnerabilidades que se puedan haber introducido [47].

2.2.13. KALI LINUX

Es una distribución de Linux basada en Debian, diseñada con el fin de temas de seguridad variados, como análisis de redes, análisis forenses, ataques inalámbricos, entre otros, contiene herramientas para llevar a cabo o realizar todas las pruebas de análisis y seguridad, posee una multitud de herramientas, tanto en modo gráfico como por comandos, lo que lo convierte en un sistema muy completo, ya sea para defensores como para atacantes [48].

Se destacan algunos aspectos disponibles [48]:

- Recopilar información
- Análisis de vulnerabilidad
- Aplicaciones web
- Ataques inalámbricos
- Pruebas de estrés
- Mantener el acceso
- Hacking de hardware
- Herramientas de información
- Ataques de contraseña

2.2.14. CROSS SITE SCRIP TING (XSS)

Los ataques de Cross-Site Scripting (XSS) se refieren a una técnica de inyección que implica la inserción de scripts maliciosos en sitios web que de otra manera serían seguros y confiables. Estos ataques ocurren cuando un agente malintencionado utiliza una aplicación web para enviar código malicioso, comúnmente en forma de un script del lado del cliente, a un usuario final distinto. Las vulnerabilidades que permiten que estos ataques tengan éxito son comunes y pueden presentarse en cualquier lugar donde una aplicación web utilice la entrada de un usuario en la salida que genera sin validarla o codificarla adecuadamente [49].

2.2.15. INYECCIÓN SQL

La inyección de código SQL es una táctica de ataque empleada para aprovechar vulnerabilidades en sitios web que utilizan instrucciones SQL basadas en las entradas proporcionadas por el usuario. Otros tipos de inyección funcionan de manera similar, como en los argumentos de un programa o en un sistema operativo, donde si no se filtran adecuadamente las cadenas de texto que se introducen, se pueden ejecutar acciones que la aplicación no está preparada para manejar. [50].

2.2.16. OWASP ZAP (ZED ATTACK PROXY)

Es el escáner de vulnerabilidades más utilizado en el mundo, es completamente gratuito y de código abierto, por lo que puedes personalizarlo según tus necesidades. Este programa es mantenido activamente por una comunidad internacional de voluntarios que están trabajando para mejorar gradualmente la herramienta y también incorporar nuevas características [51].

2.2.17. PRUEBA DE CAJA NEGRA

También conocida como black box testing, se puede definir como una técnica que intenta verificar la funcionalidad del software o la aplicación que se analiza sin hacer referencia a la estructura del código interno, las rutas de tipos internas o la información de implementación., realizando pruebas se llevan a cabo con desconocimiento del funcionamiento del sistema interno, debido a que se enfoca en la entrada y salida de un software, tomando como base sus especificaciones y requisitos [52].

2.2.18. PRUEBA STRESS

Las pruebas de estrés implican probar los límites de lo que un sistema puede soportar para evaluar la disponibilidad y estabilidad. Este tipo de prueba generalmente envía más solicitudes para comprender el comportamiento de la aplicación de las que el software normalmente puede manejar [53].

2.2.19. DENEGACIÓN DE SERVICIO (DDOS)

Un ataque de denegación de servicio (DdoS) es un tipo de ciberataque en el que un usuario malicioso tiene como propósito que un ordenador o dispositivo no esté disponible para los demás usuarios a los que va dirigido, interrumpiendo su funcionamiento [54]. Los ataques DoS funcionan al sobrecargar una máquina objetivo con solicitudes hasta que el

tráfico es incapaz de ser procesado, lo cual provoca la denegación de servicio a los usuarios de la adición; pueden ser de dos categorías: ataques de desbordamiento de búfer y ataques de inundación [54].

2.2.20. CLICKJACKING

Clickjacking es una técnica de ataque de seguridad en la que un atacante hace que un usuario haga clic en un enlace o botón que no es evidente o que parece ser algo diferente. El atacante utiliza una técnica de superposición de elementos de la página web para hacer que el usuario haga clic en un enlace o botón que parece ser seguro, pero en realidad es un enlace malicioso o una acción no deseada [55].

2.2.21. SOCIAL ENGINEERING TOOLKIT

Es una herramienta de seguridad de código abierto diseñada para realizar pruebas de ingeniería social y evaluar la seguridad de la información de una organización. SET utiliza técnicas de phishing, engaño y manipulación psicológica para simular una amenaza real y evaluar la respuesta de los empleados y la seguridad de la información. La herramienta está diseñada para ser utilizada por profesionales de seguridad informática con fines educativos y de investigación, y no debe ser utilizada para realizar ataques ilegales o para causar daño a otros [56].

Es importante tener en cuenta que la ingeniería social es ilegal en muchos países y puede tener graves consecuencias legales. Por lo tanto, su uso debe ser responsable y seguir las leyes y regulaciones aplicables [56].

2.2.22. SLOW LORIS

Es un tipo de ataque de denegación de servicio (DoS) en el que un atacante envía una cantidad lenta y constante de solicitudes HTTP a un servidor web, consumiendo recursos y eventualmente haciendo que el servidor se bloquee y no pueda responder a las solicitudes legítimas. Este tipo de ataque aprovecha una vulnerabilidad en algunos servidores web antiguos, que no pueden manejar adecuadamente un flujo lento y constante de solicitudes [57].

No requiere una gran cantidad de ancho de banda o recursos para ser efectivo. Por lo tanto, puede ser fácilmente ejecutado por un solo atacante y puede tener un impacto significativo en la disponibilidad de un sitio web. Para protegerse contra ataques, es

importante utilizar servidores web y soluciones de seguridad actualizados y mantener un monitoreo constante de las solicitudes y los recursos del servidor [57].

2.2.23. SENSEPOST JACK

Es un software de seguridad informática y pentesting, que permite evaluar la seguridad de redes y sistemas, identificando posibles vulnerabilidades y debilidades. Fue desarrollado por la compañía de seguridad informática SensePost. El objetivo de JACK es ayudar a los profesionales de seguridad a mejorar la seguridad de sus redes y sistemas mediante la identificación y corrección de posibles vulnerabilidades [58].

2.2.24. SQLMAP

Es una herramienta para la comprobar la existencia de penetración de código abierto detectando y explotando las fallas de inyección SQL tomando el control de servidores de base de datos. Incluye un potente motor de detección y una amplia gama de interruptores que son tomadas de una base de datos de huellas dactilares, para la recuperación de datos de la base de datos y así acceder al sistema de archivos subyacente y ejecutar comandos en el sistema operativo a través de conexiones fuera de banda [59].

2.2.25. PHISHING

es una técnica de suplantación de identidad utilizada para engañar a las víctimas para que revele información confidencial o sensibles, tales como contraseñas y detalles de tarjetas de crédito. Se realiza a menudo a través de mensajes de correo electrónico o mensajes de texto fraudulentos que parecen ser de una fuente legítima, como una empresa o una entidad de confianza, y que solicitan información personal o financiera. El objetivo del phishing es obtener información confidencial de las víctimas y, a menudo, se utiliza como parte de un ataque más amplio a la seguridad informática [60].

2.2.26. DDOS RIPPER

Un servidor de ataque denegado de servicio distribuible que corta objetivos o infraestructura circundante en una avalancha de tráfico de Internet, omo un atasco inesperado en una carretera, evitando que el tráfico regular llegue a su destino [61].

2.3. MARCO TEÓRICO

2.3.1. APLICACIONES EDUCATIVAS DIGITALES Y LA FALTA DE SEGURIDAD DE LOS DATOS PERSONALES DE SUS USUARIOS

La pedagogía impartida mediante documentos impresos y de pizarra está siendo sustituida en la actualidad por entornos virtuales que se adecuan a los estilos de enseñanza – aprendizaje de docentes y alumnos, favoreciendo el aprendizaje colaborativo, la interactividad e interdisciplinariedad; Por tal razón, resulta ineludible transmutar las salas de clase en espacios de aprendizaje más participativos, atrayentes y productivos [62].

En el contexto educacional, los ambientes digitales se contemplan como medios masivos capaces de compartir un mensaje de forma casi inmediata y con amplia capacidad de almacenar los datos; mediante los mismos, se acortan las distancias y se tiene disponible la información en cualquier momento, siempre y cuando se tenga acceso a un dispositivo electrónico conectado a la red, se puede decir, que a partir de la década de los 80 se empezó a utilizar en el ámbito universitario, las tecnologías de la información y comunicación en gran medida, lo cual origina la integración de diversas herramientas por parte de estudiantes y docentes en el proceso de enseñanza – aprendizaje [62].

Ahora bien, la incorporación creciente de espacios electrónicos en el área educativa, y la utilización del ciberespacio, representan grandes retos para las generaciones actuales de estudiantes, ya que, hoy en día la seguridad cibernética es un tema que alcanza a las plataformas virtuales; teniendo en cuenta esta problemática, surgen los riesgos derivados a la exposición de información personal en la impartición de cursos con modalidades virtuales, por esto, el presente estudio examina si existe seguridad de la información en entornos digitales educativos [63]. Para conocer si los usuarios son conscientes de los peligros en internet y si adoptan medidas de seguridad adecuadas en las cuentas que abren con fines educativos [63].

Se seleccionaron 29 plataformas educativas que son frecuentemente utilizadas por estudiantes de licenciatura, teniendo como conclusiones que, las plataformas no proveen medidas de seguridad, de acuerdo con la revisión, el 86% de las mismas, comparte información del usuario con terceros y no controla el acceso a otras personas; así mismo, en cuanto a los usuarios que tienen conocimientos sobre seguridad cibernética, el 95%

tienen un bajo nivel sobre este tema. Advirtiendo así, que no existen mecanismos seguros por parte de los proveedores de internet [62].

2.3.2. VULNERABILIDADES EN LOS SISTEMAS INFORMÁTICOS OWASP TOP 10: REVISIÓN BIBLIOGRÁFICA

El OWASP Top 10 es una lista de las 10 mayores amenazas de seguridad de aplicaciones web. Es actualizada regularmente por la OWASP Foundation (Open Web Application Security Project) para reflejar las últimas tendencias y desafíos en materia de seguridad de aplicaciones web. La última versión, OWASP Top 10 2021, fue lanzada en noviembre de 2021 y proporciona una guía actualizada sobre las amenazas de seguridad más importantes que deben ser abordadas por los desarrolladores y profesionales de seguridad [64].

A continuación, se muestran los riesgos de seguridad recogidos en el informe OWASP Top 10 de 2021 [64]:

Top	**Descripción**
A01:2021 - Pérdida de Control de Acceso	Se refiere a la falta de control sobre quién tiene acceso a las aplicaciones web y sus datos.
A02:2021 - Fallas Criptográficas	Se refiere a la implementación incorrecta de la criptografía, lo que puede permitir a los atacantes acceder a información confidencial y manipularla.
A03:2021-Inyección	Una de las vulnerabilidades más comunes en las aplicaciones web, ya que es la posibilidad de que un atacante inyecte código malicioso en una aplicación web, lo que puede resultar en la exposición de datos sensibles.
A04:2021 - Diseño Inseguro	Falta de seguridad en el diseño de la aplicación web, falta de validación de entrada, validación de salida y falta de consideración de los errores y las excepciones.
A05:2021-Configuración de Seguridad Incorrecta	Mala configuración de la seguridad en la aplicación web y en el servidor que la aloja.

A06:2021 - Componentes Vulnerables y Desactualizados	Se refiere a la utilización de componentes de software vulnerables o desactualizados en la aplicación web. Puede incluir la utilización de bibliotecas o herramientas que contengan vulnerabilidades conocidas y que no han sido corregidas.
A07:2021 - Fallas de Identificación y Autenticación	Falta de seguridad en los procesos de identificación y autenticación de usuarios en la aplicación web. la falta de encriptación de contraseñas, la utilización de contraseñas débiles o predeterminadas, la exposición de información de inicio de sesión en el cliente y la falta de control de intentos de inicio de sesión fallidos.
A08:2021 - Fallas en el Software y en la Integridad de los Datos	Falta de seguridad en el software y en la integridad de los datos, falta de validación de datos y la falta de protección contra ataques de denegación de servicio.
A09:2021 - Fallas en el Registro y Monitoreo	Falta de registro de eventos críticos, la exposición de información confidencial en los registros y la falta de protección contra la manipulación de registros por parte de atacantes.
A10:2021 - Falsificación de Solicitudes del Lado del Servidor (SSRF)	Posibilidad de que un atacante falsifique solicitudes del lado del servidor y acceda a información confidencial o ejecute acciones no autorizadas en la aplicación web.

Tabla 3: Top 10 OWASP 2021

2.3.3. CIBERSEGURIDAD EN PLATAFORMAS EDUCATIVAS INSTITUCIONALES DE EDUCACIÓN SUPERIOR

En el Ecuador, el Consejo de Educación Superior es el organismo que se encarga de planificar, regular y coordinar el sistema de Educación Superior mediante la LOES,

garantizando una educación de calidad; estas garantías se detallan en el Art 8, literal a, que corresponde a los fines de educación superior, en donde se aporta al desarrollo del pensamiento universal y a la promoción de las transferencias e innovaciones tecnológicas [65]. Por otra parte, la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) es responsable de velar que los propósitos de la Educación Superior se cumplan a cabalidad mediante la elaboración, ejecución y evaluación de políticas, programas y proyectos que se plasman para garantizar una educación de calidad [65].

La infraestructura digital actual permite la conectividad en línea a través de las aplicaciones móviles, en donde los alumnos se integran hacia nuevas experiencias del estudio remoto, mediante plataformas educacionales disponibles para gestionar y conectarse desde cualquier parte del mundo, lo cual proporciona una oportunidad para que los docentes implementen estrategias nuevas de enseñanza – aprendizaje enmarcadas en las limitaciones del contexto virtual [66]. Esta es una realidad en la educación remota que se fortaleció a raíz de la pandemia del COVID 19, a pesar de que aún existen inconvenientes con la conectividad de internet en las zonas rurales [66].

Un estudio realizado demuestra que los medios electrónicos más vulnerables en la red doméstica son: teléfonos inteligentes, tablets, computadoras de escritorio, portátiles y los routers; por los siguientes factores: manipulación de datos, fuga de información, fallas en la interfaz de voz, detección del comportamiento de la persona, interrupción y autenticación de las cuentas del usuario; debido a que, no disponen de mecanismos de seguridad apropiados y utilizan medidas simples como: contraseñas débiles y credenciales predeterminadas como datos personales, lo que trae consigo, riesgos al precautelar su información confidencial [67].

Con este fin, se desarrolló un procedimiento de gestión de seguridad para las plataformas educativas existentes, con el propósito que reduzca vulnerabilidades y riesgos de ciberseguridad en los Institutos Tecnológicos Superiores y en las instituciones de educación Superior del Ecuador [67].

2.3.4. AUDITORÍA INFORMÁTICA: UN ENFOQUE EFECTIVO

En un entorno cambiante, el éxito de una entidad se ha relacionado con su capacidad para gestionar los riesgos; a medida que las organizaciones se vuelven cada vez más dependientes de los datos para una ventaja competitiva y la información gana incluso mayor proporción en el valor agregado en los productos y servicios de las empresa, la capacidad de proteger datos valiosos y sensibles se ha convertido en una capacidad estratégica asegurando la sostenibilidad empresarial y el valor total de la entidad [9].

Para las organizaciones empresariales, es muy importante que se evalúen constantemente todos los procesos que se llevan a cabo en ella, con la finalidad de verificar su suficiencia y calidad en cuanto a los requerimientos de negocio para la información: confidencialidad, integridad y control [5]. A medida que los negocios van evolucionando, el volumen de la información y las transacciones incrementan, por lo que las organizaciones tuvieron la necesidad de recurrir a la automatización de los sistemas de información, por ejemplo: la automatización de los registros contables y varios procesos operativos, los cuales son soportados por activos de tecnología, como redes, servidores, software y hardware especializado [5].

Un gran número de empresas considera que la información y tecnología que se asocia a ella, representan sus activos más importantes, los requerimientos de calidad, controles y seguridad que son indispensables; la comprobación de la aplicación de los mecanismos mencionados es deber de la auditoría informática; cada vez con mayor frecuencia, se hace necesario acceder a información confidencial e intercambiarlos entre sistemas informáticos complejos, protegiendo la confidencialidad de los datos, desarrollando numerosos mecanismos de control de acceso, los cuales, intentan prevenir todo tipo de acciones antes de que ocurran, decidiendo sobre la marcha si el acceso es concedido o no [68].

La importancia de realizar auditorías informáticas radica en que permiten establecer las fortalezas y debilidades de la gestión de proyectos, así mismo, el nivel de funcionalidad de los sistemas de información automatizados, la adecuación de configuración de la plataforma informática, nivel de calidad de los servicios prestados por la unidad y la situación de los contratos con diversos proveedores de servicios y productos, entre otros

aspectos, todo esto, con el ámbito de la aplicación de las tecnologías de la información en la organización [9].

2.4. COMPONENTES DE LA PROPUESTA

2.4.1. FASE PLANIFICACIÓN

En la presente fase, se establecerá la planificación de las actividades o procesos necesarios en la auditoría, comenzando con los procesos previamente a las pruebas que se realizarán en el aplicativo web, como levantamiento de información, mapeo o escaneo, posteriormente las pruebas de funcionalidades y seguridad especificando procedimientos, herramientas, fechas, que se detallarán en las matrices a continuación

2.4.1.1. PLANIFICACIÓN DE PROCESOS DE AUDITORÍA DEL APLICATIVO

Procesos	Actividades	Fecha de inicio	Fecha fin	Tiempo de ejecución	Equipo de trabajo	Estado	Evidencia
Levantamiento de información	Investigación del entorno operacional de la institución	21-10-2022	21-10-2022	2h	Auditor de T.I	Por ejecutar	Anexo 4
	Análisis de resultado de entrevista	24-10-2022	24-10-2022	2h	Auditor de T.I	Por ejecutar	Anexo 5
	Análisis de resultado de observación	25-10-2022	25-10-2022	2h	Auditor de T.I	Por ejecutar	Anexo 6
	Exploración de funcionalidades del aplicativo web	28-10-2022	28-10-2022	3h	Auditor de T.I	Por ejecutar	Anexo 7
Escaneos	Escaneo del aplicativo con nmap	30-10-2022	30-10-2022	2h	Auditor de T.I	Por ejecutar	Anexo 8
	Escaneo del aplicativo con nikto	05-11-2022	05-11-2022	2h	Auditor de T.I	Por ejecutar	Anexo 9
	Escaneo de vulnerabilidades con owasp zap	15-11-2022	15-11-2022	3h	Auditor de T.I	Por ejecutar	Anexo 10
Ejecución de pruebas	Evaluación de interfaces de ingreso de datos y pruebas de seguridad del aplicativo	17-01-2023	17-01-2023	29h	Auditor de T.I	Por ejecutar	Anexo 11-Anexo18
Informe	Detallar observaciones encontradas en la ejecución de actividades con sus respectivas recomendaciones	5-02-2023	7-02-2023	10h	Auditor de T.I	Por ejecutar	Anexo 19

Tabla 4. Planificación de procesos de auditoría del aplicativo.

2.4.1.2. MATRIZ DE PRUEBAS DE INTERFAZ DEL APLICATIVO

PLANIFICACION DE LAS PRUEBAS DE AUDITORIA EN LA APLICACIÓN INFORMATICA											
REFERENCIA	**ACTIVIDADES**	**TIPOS DE PRUEBA**	**PROCEDIMIENTO DE LA PRUEBA**	**HERRAMIENTAS/MÉTODO**	**TIPO DE EJECUCIÓN**	**EQUIPO DE TRABAJO**	**DURACIÓN**	**FECHA INICIO**	**FECHA FIN**	**RESULTADOS ESPERADOS**	**ESTADO**
A001	Evaluar el ingreso de datos para el proceso de matriculación en el sistema informático de la institución arbol de vida	Pruebas sustantivas	Verificar/validar el ingreso correcto de datos en el formulario de matriculación. Verificar la no duplicación de registros de estudiantes. Verificar el envío de correo de validación en el registro del estudiante Verificar el proceso de los estados de solicitud de cupo de matricula	Observación, check list	Virtual	Auditor de T.I	4h	17/1/2023	17/1/2023	El sistema no debe permitir duplicación de registros, debe existir validación de datos y orden lógico de procesos	Ejecutado
A002	Evaluar el ingreso de datos para el proceso de ingreso de notas del sistema informático de la institución de arbol de vida	Pruebas sustantivas	Verificar el correcto cálculo de promedio Verificar no modificación de notas/actividades en periodos no vigentes. Validar el Ingreso correcto de números en el campo de notas.	Observación, pruebas	Virtual	Auditor de T.I	2h	18/1/2023	18/1/2023	El sistema no permite el ingreso de numeros negativos, caracteres alfabéticos, especiales. Modificación de notas/actividades en periodos académicos cerrados.	Ejecutado
A003	Evaluar el ingreso de datos para el proceso de inicio de sesión del sistema informático de la institución de arbol de vida.	Pruebas sustantivas	Validación de ingreso de datos correctos en campos requeridos para acceso aplicativo Verificar que la funcionalidad de cambio/recuperación de contraseña solicite la contraseña anterior, la nueva contraseña y una confirmación	Observación, pruebas	Virtual	Auditor de T.I	2h	19/1/2023	19/1/2023	Permitir el ingreso de usuarios registrados, caso contrario, mostrar respectivos mensajes de error según sea el caso. El cambio/recuperación de contraseña debe exigir requisitos de seguridad en la creación de nueva contraseña	Ejecutado

Tabla 5. Matriz de pruebas de interfaz del aplicativo

2.4.1.3. MATRIZ DE PRUEBAS DE SEGURIDAD DEL APLICATIVO

PLANIFICACION DE LAS PRUEBAS DE AUDITORIA EN LA APLICACIÓN INFORMATICA											
REFERENCIA	**ACTIVIDADES**	**TIPOS DE PRUEBA**	**PROCEDIMIENTO DE LA PRUEBA**	**HERRAMIENTAS/MÉTODO**	**TIPO DE EJECUCIÓN**	**EQUIPO DE TRABAJO**	**DURACIÓN**	**FECHA INICIO**	**FECHA FIN**	**RESULTADOS ESPERADOS**	**ESTADO**
A004	Evaluación de la existencia del manual de usuario del sistema de la institución	Pruebas de control	Revisión de existencia, aprobación, actualización del manual de usuario del aplicativo de la institución	Observación, técnica de entrevista al encargado de la administración del aplicativo	Virtual	Auditor de T.I	2h	20/1/2023	20/1/2023	Evidenciar la existencia del manual de usuario de la institución educativa con sus respectivas firmas.	Ejecutado
A005	Evaluar falla de seguridad de Cross site scripting (XSS) en proceso matriculación del sistema informático árbol de vida.	Pruebas sustantivas	Verificar efectividad de inserción de script malicioso en formulario de ingreso de datos en el proceso de matriculación Verificar efectividad de captura de cookies del sitio web mediante un script insertado en los formularios.	Observación, inserción de scripts	Virtual	Auditor de T.I	4h	23/1/2023	23/1/2023	El sistema valida y filtra datos de entrada.	Ejecutado
A006	Evaluar falla de seguridad de Cross site scripting (XSS) en el módulo ingreso de notas del sistema de la institución	Pruebas sustantivas	Verificar efectividad de inserción de Script en el campo de observaciones de calificaciones	Observación, inserción de scripts	Virtual	Auditor de T.I	2h	23/1/2023	23/1/2023	El sistema valida y filtra datos de entrada.	Ejecutado

Tabla 6. Matriz de pruebas de seguridad del aplicativo

PLANIFICACION DE LAS PRUEBAS DE AUDITORIA EN LA APLICACIÓN INFORMATICA											
REFERENCIA	**ACTIVIDADES**	**TIPOS DE PRUEBA**	**PROCEDIMIENTO DE LA PRUEBA**	**HERRAMIENTAS/MÉTODO**	**TIPO DE EJECUCIÓN**	**EQUIPO DE TRABAJO**	**DURACIÓN**	**FECHA INICIO**	**FECHA FIN**	**RESULTADOS ESPERADOS**	**ESTADO**
A007	Evaluar falla de seguridad de inyección sql en el aplicativo de la institución	Pruebas sustantivas	Verificar efectividad de inyección de sentencias Sql en formularios de entrada de datos	Observación, inserción de sentencias sql, sqlmap	Virtual	Auditor de T.I	3h	25/1/2023	25/1/2023	Bloqueo de peticiones con sentencias SQL, no obtener información de la base de datos.	Ejecutado
A008	Evaluar disponibilidad del sistema informático de la institución con pruebas de stress (Ddos)	Pruebas sustantivas	Verificar la estabilidad y fiabilidad del sistema en condiciones extremas	Observación, herramienta slow loris, DdoS ripper, kali linux, simbolo de sistema	Virtual	Auditor de T.I	4h	26/1/2023	26/1/2023	Correcta respuesta del aplicativo ante sobrecarga de solicitudes, prueba fallida, protección contra el ataque	Ejecutado
A010	Evaluar seguridad de contraseñas mediante ingeniería social	Pruebas sustantivos	Verificar el nivel de seguridad de contraseñas de los usuarios.	Observación, red social whatsapp, herramienta social enginering toolkit, kali linux, codigo QR	Virtual	Auditor de T.I	5h	29/1/2023	30/1/2023	No obtener credenciales, en caso de obtenerlas verificar que tengan contraseñas robustas y no adivinables.	Ejecutado

Tabla 7. Matriz de pruebas de seguridad del aplicativo

2.4.2. FASE DE EJECUCIÓN

Se procede a realizar la matriz de ejecución de pruebas de auditoria al aplicativo, el cual, cumple las funciones administrativas, curriculares y académicas de la Unidad Educativa Árbol de vida y que en ocasiones se ha manifestado incidentes al momento de procesar información tales como ingreso de notas por parte de docentes, ingreso de matriculaciones por parte del área administrativa. Se detallan diversas pruebas para verificar el óptimo funcionamiento del sistema con pruebas de funcionalidad de interfaces de ingreso de datos y de seguridad. También se recopilara los resultados obtenidos en cada prueba que aportará para la elaboración del informe de auditoría en la última fase.

2.4.2.1. EJECUCIÓN DE PRUEBAS DE EVALUACIÓN DE INTERFACES DE INGRESO DE DATOS DEL APLICATIVO MÓDULO MATRICULACIÓN

				Análisis de controles					Calificación del riesgo			Evidencia
Módulo	**Referencia**	**Riesgo**	**Procedimiento de prueba**	**Controles implementados**	**Tipo de control**	**Resultado prueba de control**	**Efectividad de control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**	**Anexo**
Matriculación	A001	Información errónea en el proceso de matriculación	Verificar/validar el ingreso correcto de datos en el formulario de matriculación.	Validación de número de cédula	Preventivo	Control de validación de número de cédula no funciona.	Inefectivo	Insuficiente	Media	Media	Media	Anexo 11
				Validacion de almacenamiento de entradas en NULL.	Preventivo	No permite guardar campos en null	Efectivo					
				Validar el ingreso de fecha de nacimiento en rango de edad apropiado para un estudiante	Preventivo	Incorrecta validación en campos de fecha	Inefectivo					
			Verificar la no duplicación de registros de estudiantes.	Generación automática de numero de matrícula	Preventivo	Se genera número de matrícula correctamente	Efectivo					
				Comprobación/verificación de datos (cédula) ya registrados en el sistema	Preventivo	Control de comprobación de datos registrados funciona correctamente	Efectivo					
			Verificar el envío de correo de confirmación en el registro del estudiante	Validación de dirección de correo electrónico existente.	Preventivo	El control de validación de correo electrónico no funciona	Inefectivo					
			Verificar el proceso de los estados de solicitud de matricula	Deshabilitar opciones del proceso matrícula cuando el estado de la solicitud esta reprobado	Preventivo	Se deshabilitan opciones de registro cuando el estado de solictud es reprobado.	Efectivo					

Tabla 8. Evaluación de interfaces del ingreso de datos en el módulo de matriculación del aplicativo.

2.4.2.2. EJECUCIÓN DE PRUEBAS DE EVALUACIÓN DE INTERFACES DE INGRESO DE DATOS DEL APLICATIVO MÓDULO INGRESO DE NOTAS

				Análisis de controles					Calificación del riesgo			Evidencia
Módulo	Referencia	Riesgo	Procedimiento de prueba	Controles implementados	Tipo de control	Resultado prueba de control	Efectividad de control	Efectividad conjunta de controles	Probabilidad	Impacto	Severidad	Anexo
Ingreso de notas	A002	Manipulación de notas en periodos no vigentes	Verificar el correcto cálculo de promedio	Generación de promedio automático	Preventivo	Control de generación de promedio automático funciona correctamente	Efectivo	Confiable	Media	Bajo	Baja	Anexo 12
			Verificar no modificación de notas/actividades en periodos no vigentes.	Reflejo del estado de parciales (abierto, cerrado)	Preventivo	El control de reflejar el estado de parciales funciona	Efectivo					
				Deshabilitar edición de observación de notas en periodos no vigentes	Preventivo	No se deshabilita agregar observación en notas y permite agregar insumos	Inefectivo					
				Deshabilitar edición de notas /agregar insumos en periodos no vigentes	Preventivo	Se deshabilita el botón de edición de notas mientras el periodo esta cerrado	Efectivo					
			Validar el Ingreso correcto de números en el campo de notas.	Validar el ingreso de nota no mayor al límite	Preventivo	El control de validación de ingreso de nota no mayor al limite establecido funciona correctamente.	Efectivo					
				Calificación con decimales mediante punto	Preventivo	El control funciona.	Efectivo					

Tabla 9. Evaluación de interfaces del ingreso de datos en el módulo de ingreso de notas del aplicativo.

2.4.2.3. EJECUCIÓN DE PRUEBAS DE EVALUACIÓN DE INTERFACES DE INGRESO DE DATOS DEL APLICATIVO MÓDULO INICIO DE SESIÓN

				Análisis de controles					Calificación del riesgo			Evidencia
Módulo	Referencia	Riesgo	Procedimiento de prueba	Controles implementados	Tipo de control	Resultado prueba de control	Efectividad de control	Efectividad conjunta de controles	Probabilidad	Impacto	Severidad	Anexo
Inicio de sesión	A003	Obtención de acceso al sistema de forma fraudulenta	Validación de ingreso de datos registrados en campos requeridos para acceso aplicativo	Verificación de datos	Preventivo	El control de verificación de datos funciona	Efectivo	Adecuado	Bajo	Medio	Bajo	Anexo 13
			Verificar que la funcionalidad de cambio/recuperación de contraseña solicite la contraseña anterior, la nueva contraseña y una confirmación de la contraseña.	Establecer requisitos para creación de contraseñas seguras	Preventivo	Si se establecen requisitos para la creación de contraseña segura	Efectivo					
				Solicitar confirmación de contraseña nueva	Preventivo	El control de solicitar confirmación de contraseña nueva funciona, pero también debería solicitar el ingreso de alguna contraseña antigua	Efectivo					

Tabla 10. Evaluación de interfaces del ingreso de datos en el módulo de Inicio de sesión del aplicativo.

2.4.2.4. EJECUCIÓN DE PRUEBAS DE SEGURIDAD CROSS SITE SCRIPTING

			Análisis de controles					Calificación del posible riesgo			Evidencia
Referencia	**Posible riesgo**	**Procedimiento de prueba**	**Controles implementados**	**Tipo de control**	**Resultado prueba de control**	**Efectividad de control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**	**Anexo**
A005	Captura de cookies, robo de datos	Verificar efectividad de inserción de script malicioso en formulario de ingreso de datos (estudiante, representante y factura) en el proceso de matriculación	Codificación de variables string	Preventivo	La codificación de variable string no funciona correctamente en todos los campos.	No efectivo	No efectivo	Baja	Medio	Media	Anexo 14
			Validación de datos de entradas	Preventivo	La validación de datos no funciona	No efectivo					
		Verificar efectividad de captura de cookies del sitio web mediante un script insertado en los formularios.	Codificación de variables string	Preventivo	La codificación de variable string no funciona correctamente en todos los campos.	No efectivo					
			Validación de datos de entradas	Preventivo	La validación de datos no funciona	No efectivo					
A006		Verificar efectividad de inserción de scripts en los items de selección	Codificación de variables string	Preventivo	El control de codificación funciona	Efectivo	Efectivo	Baja	Bajo	Baja	N/A
			Validación de datos de entradas	Preventivo	La validación de datos funciona	Efectivo					
		Verificar efectividad de inserción en los campos de notas	Codificación de variables string	Preventivo	El control de codificación funciona	Efectivo					
			Validación de entrada para cada tipo de datos.	Preventivo	La validación de datos funciona	Efectivo					
		Verificar efectividad de inserción de Script en el campo de observaciones de calificaciones	Codificación de variables string	Preventivo	El control de codificación funciona	Efectivo					
			Validación de entrada para cada tipo de datos.	Preventivo	La validación de datos funciona	Efectivo					

Tabla 11. Evaluación de la seguridad de la aplicación pruebas de Cross site scripting

2.4.2.5. EJECUCIÓN DE PRUEBAS DE SEGURIDAD INYECCIÓN SQL

			Análisis de controles					Calificación del posible riesgo			Evidencia
Referencia	**Posible riesgo**	**Procedimiento de prueba**	**Controles implementados**	**Tipo de control**	**Resultado prueba de control**	**Efectividad de control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**	**Anexo**
A007	Divulgación de información de la base de datos.	Verificar efectividad de inyección de sentencias Sql en formularios de entrada de datos Url del aplicativo	Codificacion de caracteres especiales	Preventivo	La codificación de caracteres en la url funciona correctamente	Efectivo	Efectivo	Baja	Alto	Alta	Anexo 15

Tabla 12. Evaluación de seguridad del aplicativo - prueba inyección SQL

2.4.2.6. EJECUCIÓN DE PRUEBA DE DENEGACIÓN DE SERVICIO

			Análisis de controles					Calificación del posible riesgo			Evidencia
Referencia	**Posible riesgo**	**Procedimiento de prueba**	**Controles implementados**	**Tipo de control**	**Resultado prueba de control**	**Efectividad de control**	**Efectividad conjunta de controles**	**Probabilidad**	**Impacto**	**Severidad**	**Anexo**
A008	Saturación del sistema de alojamiento del aplicativo de la institución	Verificar la estabilidad y fiabilidad del sistema en condiciones extremas	Servidor web con protección a ataques denegación de servicios	Preventivo	La protección al ataque Ddos funciona	Efectivo	Adecuado	Bajo	Medio	Media	Anexo 16

Tabla 13. Evaluación de seguridad del aplicativo – denegación de servicio

2.4.2.7. EJECUCIÓN DE PRUEBA DE CLICKJACKING

			Análisis de controles					Calificación del posible riesgo			Evidencia
Referencia	Posible riesgo	Procedimiento de prueba	Controles implementados	Tipo de control	Resultado prueba de control	Efectividad de control	Efectividad conjunta de controles	Probabilidad	Impacto	Severidad	Anexo
A009	Robo de credenciales	Verificar vulnerabilidad de ataque clickjacking	N/A	N/A	No cuenta con control, se recomienda activar protección anticlickjacking	Inefectivo	No confiable	Media	Medio	Media	Anexo 17

Tabla 14. Evaluación de seguridad del aplicativo - clickjacking

2.4.2.8. EJECUCIÓN DE PRUEBA DE SEGURIDAD DE CONTRASEÑAS

			Análisis de controles					Calificación del posible riesgo			Evidencia
Referencia	Posible riesgo	Procedimiento de prueba	Controles implementados	Tipo de control	Resultado prueba de control	Efectividad de control	Efectividad conjunta de controles	Probabilidad	Impacto	Severidad	Anexo
A010	Robo de credenciales de acceso	Verificar el nivel de seguridad de contraseñas de los usuarios (Cambio de la contraseña que le asignaron manualmente en el registro)	N/A	N/A	No tienen control, deberían exigir cambios de contraseña y que estas sean seguras, también ofrecer capacitaciones a miembros para concienciar la exposición de datos ante ingeniería social	Inefectivo	No confiable	Media	Medio	Media	Anexo 18

Tabla 15. Evaluación de seguridad de contraseñas de usuarios del aplicativo

2.4.2.9. RECOPILACIÓN DE RESULTADOS

- **Exploración en el aplicativo web**

Durante la interacción en el aplicativo web se encontró lo siguiente (Ver anexo 7):

- El diseño no es responsivo al acceder desde diferentes navegadores.
- No posee opción de resguardo de información
- Cargar información falla o es incompleta, haciendo necesario actualizar la página.
- En la sección de personas registradas en el sistema, se encontró un usuario sin tener datos llenos.
- Registros duplicados.
- Sesión activa luego de horas de inactividad.

- **Mapeo con nmap**

Análisis: En el escaneo de puertos del aplicativo web, se obtuvo información de los servicios que utilizan en el entorno web. Esta actividad es importante realizarla debido a que se puede conocer el estado de los puertos, buscar vulnerabilidades de los servicios y explotarlos. Los puertos que se encontraron abiertos son de tipo tcp, para transferencia y recepción de datos. (Ver anexo 8)

Puerto	Nombre	Uso	Vulnerabilidad
80	http	Navegación web de forma no segura	Ataque Ddos
443	Ssl/https	Navegación web de forma segura, cifrando datos	
8080	http proxy	Puerto alternativo para navegación web, normalmente usado en pruebas.	
8443	Ssl/https-alt	Puerto para navegación web segura alternativo	

Tabla 16. Puertos abiertos

- **Mapeo con nikto**

Análisis: En el escaneo con la herramienta nikto se obtuvo información del sitio web, como ip, servidor web, errores de configuraciones que permiten ejecución de ataques como clickjacking, cross site scripting y cookies no seguras, dichos aspectos se detallan a continuación (Ver anexo 9)

Información obtenida		
Multiples ip	172.66.43.64	172.66.40.192
Servidor:	Cloudflare	
Sitio vulnerable a ataque clickjacking por falta del encabezado X-Frame-Options anti-clickjacking		
No está definido el encabezado de protección xss (X-xss-protection header is not defined)		
No está configurado la Cabecera X-Content-Type-Options,		
No se crean con el indicador seguro las cookies laravel session		

Tabla 17. Resultados del escaneo con NIKTO

- **Mapeo con owasp zap**

Al ejecutar escaneos con la herramienta owasp zap se detectaron 3 alertas de vulnerabilidades con riesgo medio y 3 alertas con riesgo bajo, las mismas que se detallan a continuación.(Ver anexo 10)

Alerta	Riesgo	Confianza	Descripción
Content Security Policy (CSP) header not set	Medio	Alta	Es una capa adicional de seguridad que permite detectar y mitigar diversos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de dato
Missing anti-clickjacking header	Medio	Alta	No incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options, protegiendo contra los ataques de 'ClickJacking'.
Vulnerable JS library	Medio	Media	Utiliza una o más bibliotecas de JavaScript que son vulnerables
Cookie without Secure flag	Bajo	Media	Configuración de cookie sin el indicador de seguridad
Cookie without samesite attribute	Bajo	Media	Configuración una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud de 'entre sitios'.
Cross-domain JavaScript Source file inclusion	Bajo	Media	La página incluye uno o más archivos de script de un dominio de terceros.

Tabla 18. Resultados del escaneo con OWASP ZAP

EVALUACIÓN DE INTERFACES DE INGRESO DE DATOS DEL APLICATIVO

- **Resultados en interfaz de matriculación.**

Se realizó validación, verificación de datos y proceso de matriculación (Ver anexo 11).

Como resultado se obtuvo:

Resultados en interfaz de matriculación			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	4 horas	Herramienta/método	**Observación, checklist**
Resultados encontrados		Observaciones	
La interfaz de matriculación presenta problemas de validación de datos en los campos de ingreso de datos del estudiante, representante y datos facturación: • Número de cédula • Fecha de nacimiento • Fecha de matrícula • Correo electrónico. • Dirección Ingreso de información errónea/ilógica • Fecha de nacimiento (Registro de personas con 0 años de edad) • Fecha de la solicitud (ingreso de fechas futuras o de periodos antiguos)		Se deben implementar controles para evitar el ingreso de datos inválidos/incorrectos. Se permite generar ficha y certificado de matrícula cuando la matricula no ha sido procesada y se encuentra en solicitud de cupo.	

Tabla 19. Resultados del interfaz de matriculación

- **Resultados en interfaz de ingreso de notas**

Se realizó validación y verificación de correcto ingreso de datos (Ver anexo 12). Se obtuvo

Resultados en interfaz de ingreso de notas			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	2 horas	Herramienta/método	**Observación,checklist**
Resultados		Observaciones	
Se cumple correctamente el proceso de ingreso de notas, existe las respectivas validaciones según el tipo de dato que se solicita; Se puede agregar insumos/actividades en periodos académicos no vigentes, también agregar observaciones en las notas de periodos académicos no vigentes.		El cálculo de promedio de notas es de forma automática y se realiza de forma correcta. La opción de editar calificaciones en periodos no vigentes se deshabilita.	

Tabla 20. Resultados del interfaz de ingreso de notas.

- **Resultados en interfaz de inicio de sesión**

Se realizaron entradas controladas para la verificación, validación de credenciales y cambio/recuperación de contraseña (Ver anexo 13)

Resultados en interfaz de inicio de sesión			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	2 horas	Herramienta/método	**Observación,checklist**
Resultados		Observaciones	
El campo cedula permite el ingreso de: letras, números con más y menos de 10 dígitos Para reestablecer la contraseña se verifica que la contraseña este registrada en el sistema.		El proceso de recuperar contraseña solicita que se cumplan los requisitos establecidos para la creación de una contraseña segura, mientras no se cumpla no permite restablecer.	

Tabla 21. Resultados del interfaz de inicio de sesión.

1. EVALUACIÓN DE SEGURIDAD DE APLICATIVO

- **Resultados de prueba de cross site scripting(XSS) en módulo matriculación**

Se realizó inserción de scripts en campos de formularios de matriculación (Ver anexo 14)

Resultados de prueba de xss en módulo de matriculación			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	4 horas	Herramienta/ método	**Observación, inserción de scripts.**
Resultados		Observaciones	
Fue posible la inserción de scripts en varios campos de las secciones de datos de estudiante, representante y datos facturación en formulario de matriculación. También captura cookies mediante el <script>alert(document.cookie)</script>		En la ejecución de esta prueba se observaron las alertas luego de guardar los datos ingresados. En ciertos navegadores se ejecutaba el script para capturar cookies pero no mostraba la información en la alerta, sin embargo en el navegador Chrome sí.	

Tabla 22. Resultados de pruebas XSS en el módulo de matriculación

- **Resultados de prueba de cross site scripting(XSS) en módulo ingreso de notas**

Resultados de prueba de xss en módulo de ingreso de notas			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	2 horas	Herramienta/método	**Observación,checklist**
Resultados		Observaciones	
No se pudo hacer la inserción de scripts malicioso en los campos de ingreso de datos, selección, observación en notas.		En los campos de ingreso de datos no cuentan con la propiedad value que recepta el dato que se ingresa.	

Tabla 23. Resultados de pruebas XSS en el módulo de ingreso de notas

- **Resultados de prueba de inyección sql en el aplicativo**

Se realizó inserción de sentencias sql en formulario y url (Ver anexo 15) se obtuvo

Resultados de prueba inyección sql en el aplicativo			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	3 horas	Herramienta /método	**Observación, inyección de sentencias sql, sqlmap.**
Resultados		Observaciones	
Se insertó sentencias sql en formularios de entrada de datos en el aplicativo, Intento inyección en URL que enviaba un parámetro, no se obtuvo, ni se extrajo información de la base de datos. Con la ejecución de las herramientas, se obtuvo que no tiene vulnerabilidad de inyección sql.		En la inyección de código en la URL, existe codificación de caracteres especiales que evita que evita que sean interpretados como parte una consulta SQL.	

Tabla 24. Resultados de inyección SQL en aplicativo

- **Resultados de prueba de denegación de servicios(Ddos) en el aplicativo**

Se realizó el envío de varias cantidades de peticiones al servidor para evaluar su disponibilidad Se obtuvo (Ver anexo16):

Resultados de Denegación de servicios			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	4 horas	Herramienta /método	**Observación, slow loris, kali Linux, Ddos ripper**
Resultados		Observaciones	
Envío de diferentes cantidades de solicitudes al servidor, tuvo una correcta respuesta		Se evidencio cambio en los tiempos de respuestas de las solicitudes, durante el ataque, rompen los bots haciendo que no tenga éxito.	

Tabla 25. Resultados de DDOS en el aplicativo

- **Resultados de prueba clickjacking**

Se realizó la comprobación de vulnerabilidad del ataque clickjacking (Ver anexo 17)

Resultados de prueba clickjacking en el aplicativo			
Tipo de prueba		Sustantiva	
Horas Ejecutadas	2 horas	**Herramienta/método**	Observación, Jack sensepost, kali Linux.
Resultados		**Observaciones**	
Se verificó que el aplicativo web es susceptible al ataque mediante POCs clickjacking. Fue posible cargar la interfaz del aplicativo con esta herramienta, se pudo suplantar campos del formulario de inicio de sesión.		El aplicativo en el lado del servidor no tiene establecido anticlikjacking en cabecera X-Frame-Options	

Tabla 26. Resultados prueba de ClickJacking

- **Resultados de prueba de ingeniería social**

Se realizó phishing mediante la red WhatsApp enviando código QR (Ver anexo 18)

Resultados de ataque generado por redes sociales WhatsApp.			
Tipo de prueba		Sustantiva.	
Horas Ejecutadas	5 horas	**Herramienta/método**	Observación, Phishing - Mensaje texto en WhatsApp (QR), social engineering toolkit, kali Linux.

Resultados	Observaciones
De las 13 víctimas, 12 recibieron y leyeron el mensaje, de las cuales 5 escanearon e ingresaron sus credenciales en la página clonada, 7 de las víctimas no se re direccionaron con el QR	Al enviar el mensaje con el código Qr, 7 de nuestras posibles víctimas ignoraron el mensaje. Se comprobó la veracidad de los datos que ingresaron las víctimas. Se evidenció que 4 de las 5 víctimas tenían la misma contraseña siguiendo secuencia del uno al ocho, lo que hace que sean contraseñas débiles y adivinables para ciberdelincuentes. Se produjo que solicitaran el cambio de contraseña a todos los usuarios del sistema,

Tabla 27. Resultados de prueba de Ingeniería social

2.4.3. FASE DE CIERRE

Se realizó un informe dirigida a la unidad educativa "Árbol de vida", con la finalidad de comunicar los resultados, detallando las observaciones halladas durante la ejecución de las diferentes pruebas de funcionamiento de interfaces y de seguridad, además se emiten recomendaciones fundamentadas en estándares de seguridad y buenas prácticas (Ver anexo 19).

CONCLUSIONES

- La elaboración de planificación de las actividades es un punto muy importante en el ámbito de auditorías, ya que permite organizar y administrar el trabajo de auditoría para que este se efectúe de manera sistemática, efectiva y eficiente. Se realizó un plan de trabajo con el detalle de las actividades que se ejecutaron durante la auditoria. Este plan incluyó el tiempo, herramientas, responsable, tipo de prueba y procedimientos para realizar las evaluaciones.

- Se diseñaron y ejecutaron nueve procedimientos de prueba para evaluar los incidentes de seguridad mediante un testeo al aplicativo web. En esta verificación se evaluó el funcionamiento de interfaz de los módulos que soportan los procesos académicos de la institución, comprobando la existencia de fallas e identificación de partes susceptibles, también se elaboró una matriz, para la evaluación de los controles que están implementados en el aplicativo.

- Durante la auditoría de seguridad, se llevaron a cabo cinco pruebas de seguridad para identificar vulnerabilidades conocidas en el aplicativo. Se utilizaron técnicas y herramientas especializadas de seguridad informática para evaluar la resistencia del sistema ante posibles amenazas. Gracias a estas pruebas, se pudo detectar una serie de malas configuraciones en el servidor que representaban un riesgo para la seguridad del sistema. Con esta información, se podrán implementar medidas para mejorar la seguridad y prevenir futuros ataques.

- Al finalizar los procedimientos planificados de la auditoría, se elaboró un informe técnico que detalla las observaciones obtenidas a partir de la ejecución de las pruebas de seguridad en los módulos evaluados, también incluye recomendaciones fundamentadas en estándares de seguridad y mejores prácticas que contribuyen a la protección de información y del aplicativo. Este informe se presentará a las autoridades de la institución para que evalúen las debilidades identificadas y tomen las medidas necesarias para corregirlas y mejorar su seguridad.

RECOMENDACIONES

- Antes de iniciar cualquier trabajo de auditoría, es fundamental elaborar un plan detallado, que incluya todos los recursos necesarios para llevar a cabo la auditoría de manera eficiente y efectiva. La planificación previa permitirá determinar la inversión de tiempo estimado para la realización de la auditoría, garantizando así una gestión adecuada de los recursos y una ejecución exitosa del trabajo.

- Es necesario que se diseñen pruebas periódicas para evaluar vulnerabilidades en el aplicativo web, mediante evaluaciones de las interfaces de usuario, es posible identificar cualquier debilidad que pueda ser explotada y tomar medidas para corregirlas antes de que sean explotadas por un atacante. Además, es importante evaluar no solo las interfaces de usuario, sino también las interfaces de programación de aplicaciones (API). Esto permitirá identificar cualquier debilidad que pueda ser explotada y tomar medidas para proteger la aplicación y los datos sensibles de los usuarios.

- Mantenerse actualizado sobre las últimas amenazas y vulnerabilidades en la seguridad cibernética, para poder responder rápidamente ante cualquier situación, también el uso de herramientas de seguridad pagadas para realizar evaluaciones más exhaustivas y precisas debido a que tienen una funcionalidad más avanzada y completa que las herramientas gratuitas, suelen contar con una base de datos de amenazas más actualizada lo que permite una detección más efectiva de vulnerabilidades y amenazas.

- Es necesario que en la elaboración de informes de auditorías se integre un plan de acción para la implementación de las recomendaciones y monitorear su efectividad, del mismo modo el brindar un glosario de términos para que las autoridades de la institución puedan entender su contenido.

- Para trabajos futuros, se recomienda realizar auditoría que contemplen más pruebas sustantivas y analíticas en otros módulos del aplicativo web de la institución, incluyendo análisis de riesgos y un seguimiento para la verificación y validación de implementación de las recomendaciones brindadas, calificando la efectividad de los mismos.

BIBLIOGRAFÍA

[1] AdminACTI, «audiconsulti,» 22 Agosto 2019. [En línea]. Available: https://www.audiconsulti.com/importancia-de-la-auditoria-de-sistemas/.

[2] J. E. G. RETAMOZO, «AUDITORIA DE SEGURIDAD INFORMÁTICA PARA LA INSTITUCIÓN,» CALDAS, CEAD–LA DORADA , 2017.

[3] R. R. Foronda García, «Auditoría a los procesos de atención al ciudadano (SAC) en la secretaría de educación departamental de la Guajira, con miras a mantener la certificación de Icontec bajo el proyecto de modernización,» Barranquilla, 2018.

[4] J. R. Benítez Iglesias, «Elaboración de un manual de auditoría interna para la Unidad Educativa Intercultural Trilingue Mushuk Kawsay del cantón El Tambo,» Cuenca, 2021.

[5] M. G. Acosta Jordán, «Auditoría informática para la optimización del funcionamiento de los sistemas y equipos informáticos de la Facultad de ingeniería en sistemas, electrónica e industrial,» Ambato, 2017.

[6] U. J. UNIVERSITARIA, «Ley N° 110,» Santa Elena, 2019.

[7] Primicias, «Ecuador lidera la lista de países más vulnerados por los ciberataques,» Ecuador lidera la lista de países más vulnerados por los ciberataques, 21 02 2021. [En línea]. Available: https://www.primicias.ec/noticias/tecnologia/ciberataques-latinoamerica-elevan-pirateria-trabajo-remoto/. [Último acceso: 11 09 2022].

[8] swissinfo.ch, «El Municipio de Quito, víctima de ciberataque que afectó el 15 % de sus datos,» swissinfo.ch, 18 04 2022. [En línea]. Available: https://www.swissinfo.ch/spa/ecuador-ciberataque_el-municipio-de-quito--v%C3%ADctima-de-ciberataque-que-afect%C3%B3-el-15---de-sus-datos/47525602. [Último acceso: 11 09 2022].

[9] D. Arcentales Fernández y X. Caycedo Casas, «Auditoría informática: un enfoque efectivo,» Dialnet, vol. 3, p. 17, 2017.

[10] A. Martínez, B. Blanco Alfonso y L. Loy Marichal, «Auditoría con informática a sistemas contables,» Redalyc, vol. 6, nº 2, p. 15, 2021.

[11] Ecuador, «Plan de Creación de Oportunidades 2021-2025,» 2021. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf.

[12] R. H. Sampieri, Metodología de la investigación Sexta edición, Sexta edición ed., M. I. R. Martínez, Ed., México D.F.: Interamericana editores S.A de C.V., 2018.

[13] H. H. Vargas García, «METODOLOGÍA DE AUDITORÍA INFORMÁTICA PARA EVALUAR EL ÁREA DE CONTROL DE CALIDAD DE SOFTWARE EN BANCOS PRIVADOS MEDIANOS DEL ECUADOR, BASADA EN EL MARCO DE REFERENCIA COBIT",» UNIVERSIDAD INTERNACIONAL SEK, 2019.

[14] Árbol de vida, «arboldevida.runacode.com,» 2023. [En línea]. Available: https://arboldevida.runacode.com/.

[15] J. D. Muñoz, «Metodología para seleccionar políticas de seguridad informática en un establecimiento de educación superior,» 2017.

[16] B. Guerra, «Instituciones educativas en riesgo informático,» Udla, 15 12 2021. [En línea]. Available: https://www.udla.edu.ec/liderazgo/blog/2021/12/15.

[17] M. D. C. Molinero y U. Cháves Morales, «Herramientas tecnológicas en el proceso de enseñanza - aprendizaje en estudiantes de educación superior,» Scielo, vol. 10, nº 19, p. 11, 15 05 2020.

[18] Microsoft, «microsoft.com,» [En línea]. Available: https://www.microsoft.com/es-es/microsoft-365/word.

[19] Microsoft, «microsoft.com,» [En línea]. Available: https://www.microsoft.com/es-es/microsoft-365/powerpoint.

[20] Microsoft, «microsoft.com,» [En línea]. Available: https://www.microsoft.com/es-ww/microsoft-365/excel.

[21] google, «google.com,» [En línea]. Available: https://www.google.com/intl/es/gmail/about/.

[22] Adobe, «adobe.com,» [En línea]. Available: https://www.adobe.com/la/acrobat/complete-pdf-solution.html?mv=search&ef_id=Cj0KCQjw8amWBhCYARIsADqZJoVghPSYdsXYpaHVfTd8MreQwynRJXrJAiTK2t4cnLiIbXPAMBLRUowaAjo_EALw_wcB:G:s&s_kwcid=AL!3085!3!584124841135!e!!g!!adobe%20acrobat!1781882837!68877166443&gclid=.

[23] Google, «google.com,» [En línea]. Available: https://www.google.com/intl/es/chrome/.

[24] Google, «google.com,» [En línea]. Available: https://www.google.com/.

[25] Avast, «avast.com,» [En línea]. Available: https://www.avast.com/es-ww/lp-ppc-hp-

v5?ppc_code=012&ppc=a&gclid=Cj0KCQjw8amWBhCYARIsADqZJoWN1POxgzVXm3-LxwmzY68XbMTAOq-RINzAtrThOlHmwZQ_U-32mgIaAvgMEALw_wcB&gclsrc=aw.ds#pc.

[26] Zoom, «zoom.us,» [En línea]. Available: https://zoom.us/.

[27] Moodle, «moodle.org,» [En línea]. Available: https://moodle.org/?lang=es.

[28] Google, «workspace.google.com,» [En línea]. Available: https://workspace.google.com/intl/es-419/products/drive/?utm_source=google&utm_medium=cpc&utm_campaign=latam-T1-all-es-dr-bkws-all-all-trial-e-dr-1011272-LUAC0012558&utm_content=text-ad-none-any-DEV_c-CRE_479487543818-ADGP_Hybrid%20%7C%20BKWS%20-%20EXA%20.

[29] A. M. Cruz Chóez, «La actividad de auditoría informática y su impacto en el rendimiento de la auditoría interna. Un estudio basado en competencias.,» Universidad y sociedad, vol. 14, nº S5, p. 10, 10 10 2022.

[30] Unir, «ecuador.unir.net,» 15 06 2021. [En línea]. Available: https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/.

[31] A. Zuñiga y E. Jalón, «Análisis de seguridad informática,» Revista Universidad y Sociedad, vol. 13, nº 3, p. 6, 2021.

[32] S. Quiroz, «Seguridad en informática: Consideraciones,» Dialnet, vol. 3, nº 5, p. 13, 30 01 2017.

[33] T. I. Mina Quiñonez, «Desarrollo de aplicaciones web y móvil para la gestión de publicaciones científicas,» vol. 6, nº 6, p. 11, 2021.

[34] M. Soriano, «igniteonline.la,» 2020. [En línea]. Available: https://igniteonline.la/7310/.

[35] M. Farfán y I. Reyes, «Gestión educativa estratégica y gestión escolar del proceso de enseñanza - aprendizaje,» REencuentro. Análisis de Problemas Universitarios, vol. 28, nº 73, pp. 45-61, 06 2017.

[36] TicPortal, «Enterprise Resource Planning (ERP),» 2 11 2022. [En línea]. Available: https://www.ticportal.es/temas/enterprise-resource-planning.

[37] P. L. Constantini, «La auditoria interna y el auditor,» Anuario de la Facultad de Ciencias Económicas del Rosario, p. 13, 2019.

[38] A. M. Cóccaro, «LOS DESAFÍOS DE LA AUDITORÍA A DISTANCIA,» Revista Desarrollo y Gestión, pp. 1-6, 06 2021.

[39] J. M. Manrique Plácido, Introducción a la auditoría, 2019.

[40] E. Jara, «Control Interno dentro de una Organizacion,» 5 11 2018. [En línea]. Available: https://sites.google.com/site/controlinterno1997.

[41] V. De la Cruz Vaca, DISEÑO DE UN CHECK LIST BASADO EN LA NORMA ARCSA DE-067-2015-GGG PARA LA FÁBRICA DE EMBUTIDOS "MAYBE" DE LA CIUDAD DE LATACUNGA, Ambato, Euador, 2018.

[42] J. P. Muñoz Hernández, «Auditoria en seguridad de la información, para identificar el análisis de riesgo y vulnerabilidad en la Alcaldía Municipal de Valencia.,» Agosto 2022. [En línea]. Available: http://www.knowledgecap.bigstarcreative.com/handle/20.500.12494/46135.

[43] J. J. De Almeida, «Riesgo y paradigmas de la auditoría,» Novos desafios na Gestão, Innovação ou renovação?, pp. 395-402, 2002.

[44] G. Westreicher, «Probabilidad,» Economipedia, 25 Agosto 2020. [En línea]. Available: https://economipedia.com/definiciones/probabilidad.html.

[45] M. Álvarez Torres, «Consultoría Empresarial | 3 Conceptos para evaluar los riesgos empresariales,» 22 Junio 2021. [En línea]. Available: https://www.grupoalbe.com/consultoria-empresarial-3-conceptos-sobre-como-evaluar-los-riesgos-empresariales/.

[46] Nmap, «nmap.org,» 2023. [En línea]. Available: https://nmap.org/man/es/index.html.

[47] Nikto, «ciberseguridad.com,» 2021. [En línea]. Available: https://ciberseguridad.com/herramientas/software/nikto/.

[48] Kali, «kali.org,» 2023. [En línea]. Available: https://www.kali.org/.

[49] KirstenS, «Secuencias de comandos entre sitios (XSS),» owasp, [En línea]. Available: https://owasp.org/www-community/attacks/xss/. [Último acceso: 10 06 2022].

[50] J. L. C. FLOREZ, «PROPUESTA DE AUDITORIA A LAS APLICACIONES WEB DE LA EMPRESA C&M CONSULTORES APLICANDO HERRAMIENTAS DE SOFTWARE LIBRE,» UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD, Bogota, 2017.

[51] ZAP, «zaproxy,» Zap, 06 05 2021. [En línea]. Available: https://www.zaproxy.org/. [Último acceso: 19 06 2022].

[52] Imperva, «Black Box Testing,» Imperva, 2022. [En línea]. Available: https://www.imperva.com/learn/application-security/black-box-testing/. [Último acceso: 23 11 2022].

[53] Grafana k6, «Stress testing,» Grafana Labs k6, 2021. [En línea]. Available: https://k6.io/docs/test-types/stress-testing/. [Último acceso: 23 11 2022].

[54] J. Márquez Díaz, «Riesgos y vulnerabilidades de la denegación de servicio distribuido,» Scielo, vol. 1, nº 46, p. 12, 2019.

[55] H. Lin-Shung, A. Moshchuk, H. J. Wang, S. Schechter y C. Jackson, «Clickjacking: Attacks and Defenses,» USENIX security symposium, pp. 413-428, 2012.

[56] I. Jácome y G. Diaz, «Phishing utilizando SET (Social-Engineer Toolkit) en Kali Linux,» Nexos Científicos, vol. 1, nº 4, pp. 12-19, 2020.

[57] R. Greyrat, «Herramienta de ataque Slowloris DDOS en Kali Linux,» Barcelona Geeks, 5 Julio 2022. [En línea]. Available: https://barcelonageeks.com/herramienta-de-ataque-slowloris-ddos-en-kali-linux/. [Último acceso: 29 Enero 2023].

[58] SensePost, «GitHub,» SensePost, 23 Septiembre 2016. [En línea]. Available: https://github.com/sensepost/jack.

[59] B. Damale y M. Stampar, «sqlmap,» 2023. [En línea]. Available: https://sqlmap.org/.

[60] R. Balboa y J. Francisco, «Ransomware, hacking y phishing: conducta típica del delito de daños informáticos.,» Reunir, 17 Junio 2018. [En línea]. Available: https://reunir.unir.net/handle/123456789/6929.

[61] Palahsu, «DDoS-Ripper,» GitHub, 3 02 2021. [En línea]. Available: https://github.com/palahsu/DDoS-Ripper.

[62] P. L. De la Rosa Rodríguez, «Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios,» Scielo, vol. 12, nº 23, p. 10, 18 10 2021.

[63] P. Rivera y R. Vargas, «Plataformas digitales en educación. Por el derecho a la privacidad y protección de los datos personales,» 2022.

[64] K. B. Álava Zambrano, W. E. Basurto Vidal y R. R. Tóala Vera, «VULNERABILITIES IN COMPUTER SYSTEMS OWASP TOP 10: BIBLIOGRAPHIC REVIEW,» Journal Business Science-ISSN: 2737-615X, vol. 3, nº 2, pp. 1-8, 29 12 2022.

[65] P. I. Morales Paredes y P. Medina Chicaiza, «Ciberseguridad en plataformas educativas institucionales de Educación Superior,» Ambato, 2021.

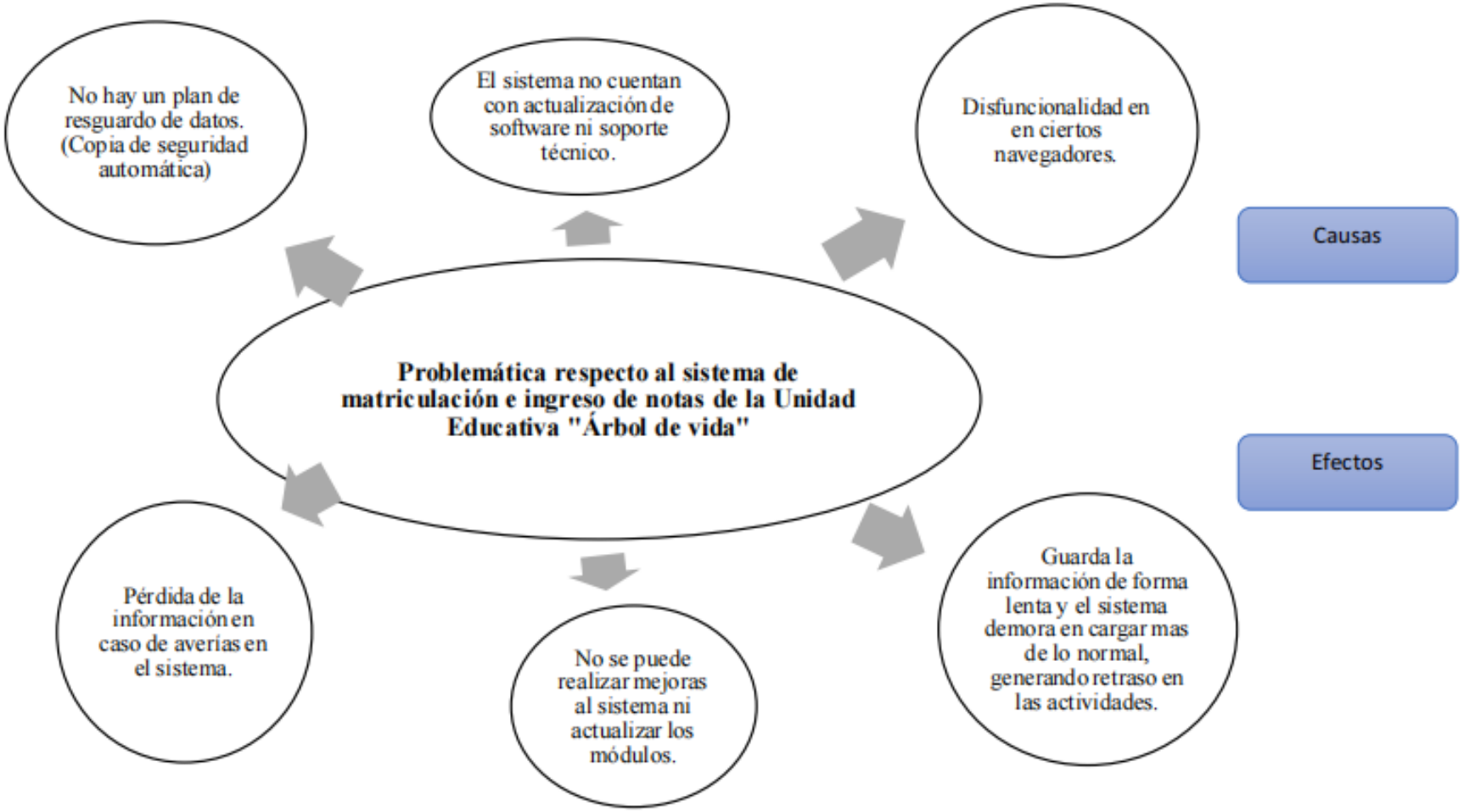
[66] C. Santamaría, «Control de seguridad en una plataforma educativa institucional,» Ambato, 2022.

[67] M. Peñafiel, «Ingeniería social en una institución de educación superior aplicando técnicas computacionales y no computacionales,» La Libertad, 2022.

[68] A. Urquizo, «Auditoría informática para la protección de la información digital a la COAC Acción y desarrollo Ltda,» Riobamba, 2021.

ANEXOS

Anexo 1. Árbol de problemas



Anexo 2. Entrevista dirigida al encargado de la Unidad Educativa "Árbol de vida"

<table>
<tr><td colspan="3">Universidad Estatal Península de Santa Elena
Facultad de Sistemas y Telecomunicaciones
Carrera de Tecnología de la Información.</td></tr>
<tr><td colspan="3">Entrevista dirigida al encargado de la Unidad Educativa "Árbol de vida"</td></tr>
<tr><td colspan="3">Objetivo: Determinar los inconvenientes con respecto a los sistemas de matriculación e ingreso de notas de la Unidad Educativa "Árbol de vida".</td></tr>
<tr><td>1.</td><td colspan="2">¿Cuáles son los módulos principales que contienen los sistemas de matriculación e ingreso de notas?</td></tr>
<tr><td>2.</td><td colspan="2">¿Qué personas pueden acceder al sistema?</td></tr>
<tr><td>3.</td><td colspan="2">¿Alguna vez se ha realizado una auditoría en los sistemas que posee la institución?</td></tr>
<tr><td>4.</td><td colspan="2">¿Los sistemas permiten realizar copia de seguridad de los datos, frecuentemente?</td></tr>
<tr><td>5.</td><td colspan="2">¿Los sistemas funcionan correctamente en cualquier navegador?</td></tr>
<tr><td>6.</td><td colspan="2">¿Presentan problemas al registrar cierta información en los sistemas de matriculación e ingreso de notas? Si es afirmativo, ¿Qué problemas presentan?</td></tr>
<tr><td>7.</td><td colspan="2">¿Tienen a su disposición manual de usuario?</td></tr>
<tr><td>8</td><td colspan="2">¿Ha habido el caso de pérdida de información en los sistemas?</td></tr>
<tr><td>9</td><td colspan="2">¿Está de acuerdo con que se realice una auditoría en los sistemas que posee la Unidad Educativa?</td></tr>
<tr><td>10</td><td colspan="2">¿Cree usted conveniente tener conocimiento acerca de los riesgos y robo de información en los sistemas y saber cómo prevenirlos?</td></tr>
<tr><td colspan="2">Resumen:</td><td>Recolección de información en busca de falencias en los sistemas de matriculación e ingreso de notas de la Unidad Educativa "Árbol de vida".</td></tr>
<tr><td colspan="2">Responsable:</td><td>Kenya Gissell Mejillón González.</td></tr>
</table>

Anexo 3. Registro de la técnica de observación aplicada en la Unidad Educativa "Árbol de vida".

<table>
<tr><td colspan="2">Registro descriptivo de la información</td></tr>
<tr><td colspan="2">Fecha: 10 de Julio del 2022 Lugar: Unidad Educativa "Árbol de vida"</td></tr>
<tr><td colspan="2"># Personas: 1
Proceso: Búsqueda de inconvenientes en los sistemas de matriculación e ingreso de notas.
Duración: 3 horas.</td></tr>
<tr><td>Tipo de observación</td><td>Clasificación de la observación</td></tr>
<tr><td>Directa</td><td>Mediano Riesgo</td></tr>
<tr><td colspan="2">Hechos observados</td></tr>
<tr><td colspan="2">• La Unidad Educativa posee una gran cantidad de alumnos que son representados por sus respectivos padres de familia.
• Los padres de familia, separan un cupo de matriculación para luego cancelar un pago por la misma.
• El sistema de matriculación, cuenta con un módulo de pagos, que registra los ingresos recaudados por parte de los padres de familia.
• El sistema de ingreso de notas lleva una nómina donde se refleja el curso y las calificaciones de cada alumno asentadas por los docentes que inician sesion en la plataforma.
• Dicho sistema, posee un espacio para que el estudiante realice tareas, cuestionarios y lecciones virtuales.
• No existe un resguardo de información al solicitar una copia de seguridad.
• En ciertos navegadores, no funciona correctamente el aplicativo.
• No contiene ninguna forma de realizar actualización del aplicativo ni de mejorarlo.
• No posee un método de raíz administrativa, donde se pueda realizar cambios al sistema.</td></tr>
<tr><td>Resumen:</td><td>Se pudo determinar que la Unidad Educativa posee falencias en los sistemas que posee, por lo cual, se necesita auditar dicha información.</td></tr>
<tr><td>Responsable:</td><td>Kenya Gissell Mejillón González.</td></tr>
</table>

Anexo 4. Entorno Operacional

La **escuela de educación básica "Árbol de vida"** se encuentra ubicada en la provincia de **Santa Elena**, en el cantón **Salinas** de la parroquia **José Luis Tamayo (Muey)**. Es un centro educativo de Ecuador perteneciente a la **Zona 5** geográficamente, es un **centro educativo rural**, su modalidad es **Presencial** en jornada **Matutina**, con tipo de educación regular y con nivel educativo: **Inicial y EGB**.

Es Institución educativa que obtiene sus recursos para desarrollar sus actividades (Sostenimiento) de manera Particular, está en el **régimen escolar Costa**. Tienen un total aproximado de **13 docentes** y **145 estudiantes**.

Organigrama

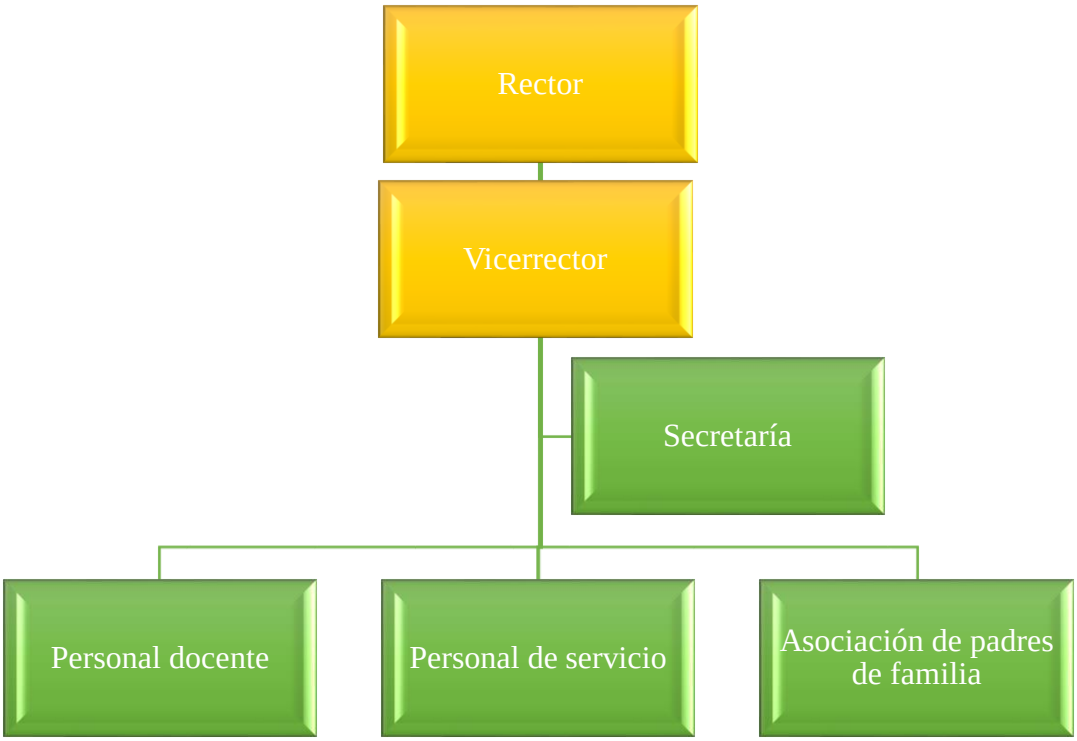


Figura 2: Organigrama de la Unidad Educativa "Árbol de vida"

Usuarios del sistema

ADMINISTRADOR: Es el administrador del sistema, donde tiene acceso a todas las opciones, tales como: Ingreso de usuarios, dar permiso a los módulos, entre otros.

SECRETARIA: Su función es brindar apoyo a la dirección de la escuela, realizando los procesos establecidos, tales como: matriculación, registro de padres, alumnos, materias, horarios de clases, asignar fechas de pagos, costos administrativos, entre otros.

DOCENTE: Se encarga de registrar tareas para los estudiantes, asistencia, notas, planificar su calendario, entre otros.

PADRES DE FAMILIA: Ingresan al sistema para ver el proceso de sus hijos, es decir, ver calificaciones, avisos importantes de la escuela y realizar la debida matriculación.

Anexo 5. Análisis De Resultados De Entrevista

Los resultados obtenidos mediante la entrevista realizada al encargado del sistema de la unidad educativa "Árbol de vida", son los siguientes:

Informante: Encargado del sistema web de la escuela	
Pregunta	Respuesta
¿Cuáles son los módulos principales que contienen los sistemas de matriculación e ingreso de notas?	Los módulos principales que posee el aplicativo web, son ingreso de notas y matriculación.
¿Qué personas pueden acceder al sistema?	Las personas que pueden acceder al sistema son: autoridades, docentes, padres de familia y estudiantes.
¿Alguna vez se ha realizado una auditoría en los sistemas que posee la institución?	Nunca se ha realizado una auditoría al sistema web.
¿Los sistemas permiten realizar copia de seguridad de los datos, frecuentemente?	No existe un sistema de resguardo de la información al solicitar una copia de seguridad, que ayude a prevenir a futuro una falla del programa.

¿Los sistemas funcionan correctamente en cualquier navegador?	En ciertos navegadores, el aplicativo no funciona correctamente, presentando algunos problemas en sus procesos.
¿Presentan problemas al registrar cierta información en los sistemas de matriculación e ingreso de notas? Si es afirmativo, ¿Qué problemas presentan?	Existen retardos en el inicio de sesión, registros de notas o muchas veces, intentos múltiples para poder ingresar al perfil personal.
¿Tienen a su disposición manual de usuario?	No contamos con manual de usuario, pero nos facilitaron capacitaciones y videos tutoriales disponibles en el aplicativo y en canal de youtube.
¿Ha habido el caso de pérdida de información en los sistemas?	Por los inconvenientes antes mencionados, se generan pérdidas, que en muchas ocasiones son los registros al momento de ingresar notas.
¿Está de acuerdo con que se realice una auditoría en los sistemas que posee la Unidad Educativa?	Si estoy de acuerdo.
¿Cree usted conveniente tener conocimiento acerca de los riesgos y robo de información en los sistemas y saber cómo prevenirlos?	Si tengo conocimientos acerca de los riesgos informáticos, sin embargo, no sé cómo prevenirlos.

Tabla 28: Resultados de la entrevista

Conclusión: A través de la entrevista realizada se pudo determinar que, existen diversos inconvenientes con respecto a la seguridad en el aplicativo web, dando como consecuencias, fallos en los registros, carga lenta de información, pérdida de datos y retrasos en los procesos realizados dentro del sistema. Debido a esto, se pretende realizar una auditoría informática en la aplicación web, que permita controlar toda la problemática, brindando soluciones y una guía que será útil en la Unidad Educativa "Árbol de Vida".

Anexo 6. Análisis De Resultados De Método De Observación

<table>
<tr><td>FECHA</td><td>25/10/2022</td><td>HORA INICIO</td><td>2 PM</td><td>HORA TERMINO</td><td>4 PM</td><td>HORAS OCUPADAS</td><td>2</td></tr>
<tr><td colspan="2">DIVISIÓN/AREA</td><td colspan="2">Técnica</td><td colspan="2">SECCION/DEPTO</td><td colspan="2">Técnico</td></tr>
<tr><td colspan="3">TRABAJADOR SUPERVISOR
Jean Carlos Maldonado</td><td colspan="3">TIEMPO EN LA OCUPACION
5 años</td><td>TIEMPO EN LA EMPRESA
7 años</td></tr>
<tr><td rowspan="2">Observación Inicial</td><td rowspan="2">x</td><td rowspan="2">Seguimiento</td><td rowspan="2"></td><td rowspan="2">Fue avisado el administrador</td><td>SI</td><td>NO</td><td>Observación planeada</td><td></td></tr>
<tr><td>x</td><td></td><td>Observación no planeada</td><td>x</td></tr>
<tr><td colspan="8">Razones de la observación</td></tr>
<tr><td>Acc. Repetido</td><td></td><td>Bajo Rendimiento</td><td>x</td><td>Temerario</td><td></td><td>Trabajo peligroso</td><td></td><td>Trabajo critico</td><td></td><td>Otros</td><td></td></tr>
<tr><td colspan="8">Descripción del trabajo observado
➢ El aplicativo web se divide en varios sistemas, los cuales son: ingreso de notas y matriculación.
➢ En la aplicación pueden acceder, las autoridades, docentes, padres de familia y estudiantes.
➢ Las autoridades son las encargadas de administrar todos los sistemas.
➢ Los docentes acceden a la plataforma para ingresar notas, enviar deberes y revisarlos.
➢ Los padres de familia inician sesión en el sistema, para matricular a los niños y verificar las notas de los mismos.
➢ Los estudiantes ingresan al sistema para subir deberes y ver información acerca de sus clases.
➢ El sistema de matriculación cuenta con un módulo de pagos, que registra los ingresos recaudados por parte de los padres de familia.
➢ El sistema de ingreso de notas lleva una nómina donde se refleja el curso y calificaciones de cada alumno.
➢ El aplicativo web, posee un espacio para que el estudiante realice tareas, cuestionarios y lecciones virtuales.
➢ No existe un resguardo seguro de información al solicitar copia de seguridad.
➢ En ciertos navegadores, no funciona correctamente el aplicativo.
➢ No contiene ninguna forma de actualizar la información de la aplicación, ni de mejorarlo.</td></tr>
<tr><td colspan="4">DESCRIPCIÓN DE LA CONDUCTA INSEGURA O CONDUCTA SEGURA</td><td colspan="4">DESCRIPCIÓN DE LA ACCIÓN CORRECTIVA O REFORZAMIENTO DE LA CONDUCTA SEGURA</td></tr>
<tr><td colspan="4">A través de la técnica de observación realizada al aplicativo web de la unidad educativa “Árbol de vida”, se determinó que cuenta con varias falencias a nivel de ejecución, actividad y datos causando incomodidad a parte del personal que lo opera y administra.</td><td colspan="4">Debido a la problemática encontrada y las falencias que posee el aplicativo web de la unidad educativa “Árbol de vida”, es importante auditar el mismo, para poder prevenir fallas de seguridad y resguardar la información.</td></tr>
<tr><td colspan="8"></td></tr>
<tr><td colspan="3">Nombre y firma del supervisor:
Jean Carlos Maldonado.</td><td colspan="3">Nombre y firma del observador
Kenya Gissell Mejillón González</td><td colspan="2">Revisado por:
Unidad Educativa Árbol de Vida.</td></tr>
</table>

Tabla 29: Resultados del método de observación

Anexo 7. Interacción en el aplicativo

SISTEMA WEB (MÓDULOS)

- El aplicativo web tiene una interfaz de inicio de sesión, muestra contenido diferente de acuerdo al rol o perfil de cada usuario.

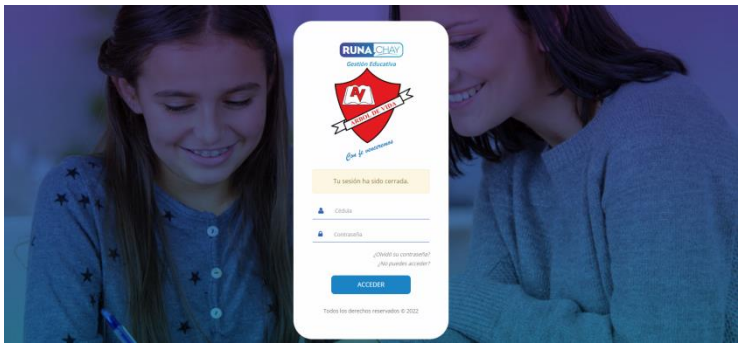


Figura 3: Login del sistema

- Interfaz principal desde el rol de administrador

Figura 4: Página principal del sistema

- El perfil de administrador puede observar todos los datos de los usuarios registrados en el sistema

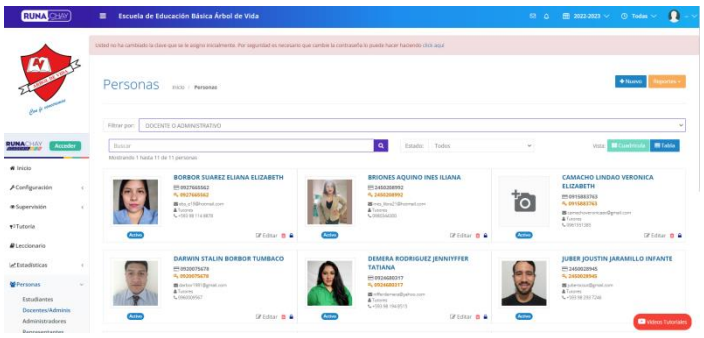


Figura 5: Organigrama Usuarios del sistema

- Configuración de fases (ciclos académicos)

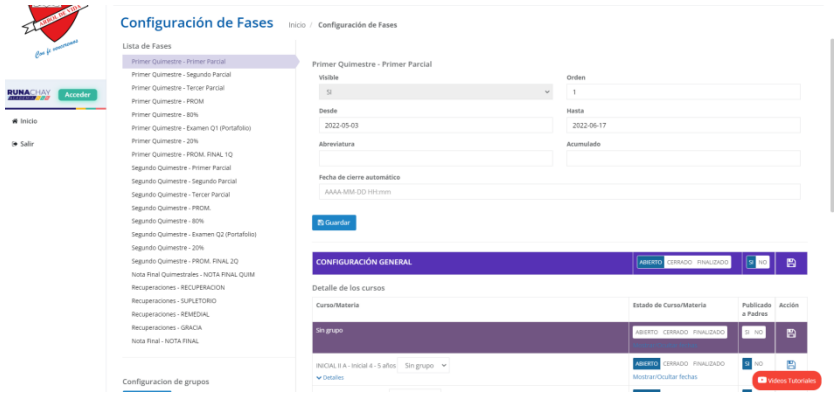


Figura 6: Configuración de fases del sistema

- El aplicativo web tiene la opción de editar datos de la institución

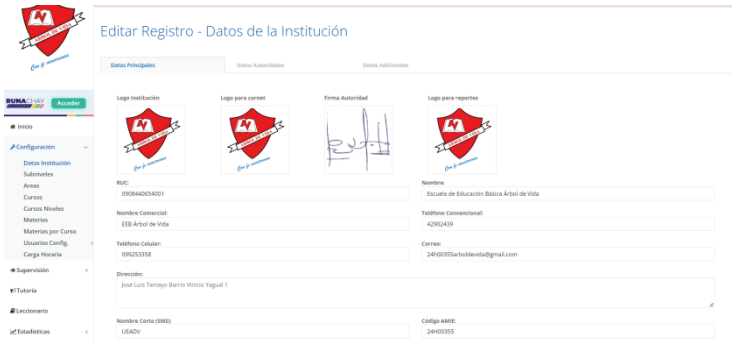


Figura 7: Editar datos de la institución

- Desde el perfil administrador se puede agregar cursos

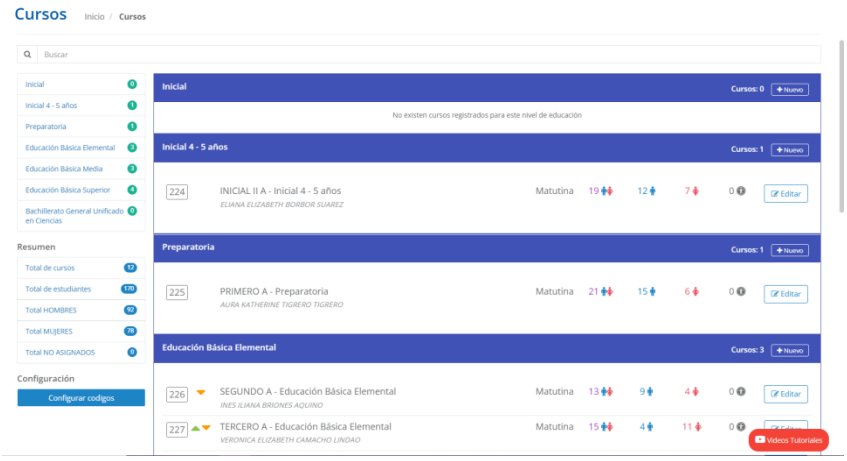


Figura 8: Cursos de la Unidad Educativa "Árbol de vida"

- Actualización de la información o configuración de los cursos

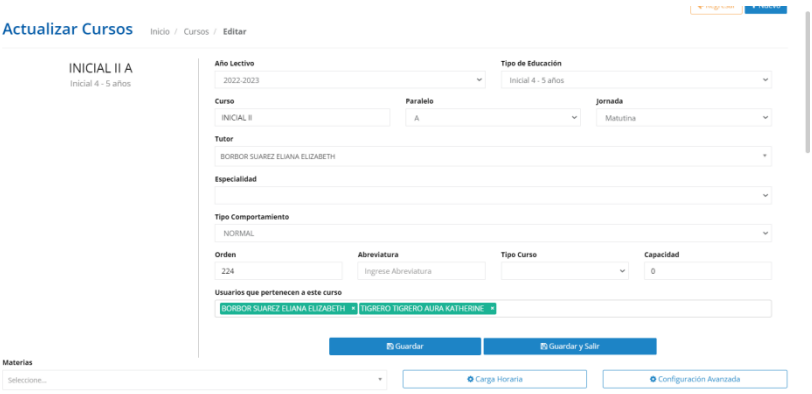


Figura 9: Actualizar cursos

- El perfil administrador tiene acceso para agregar materias

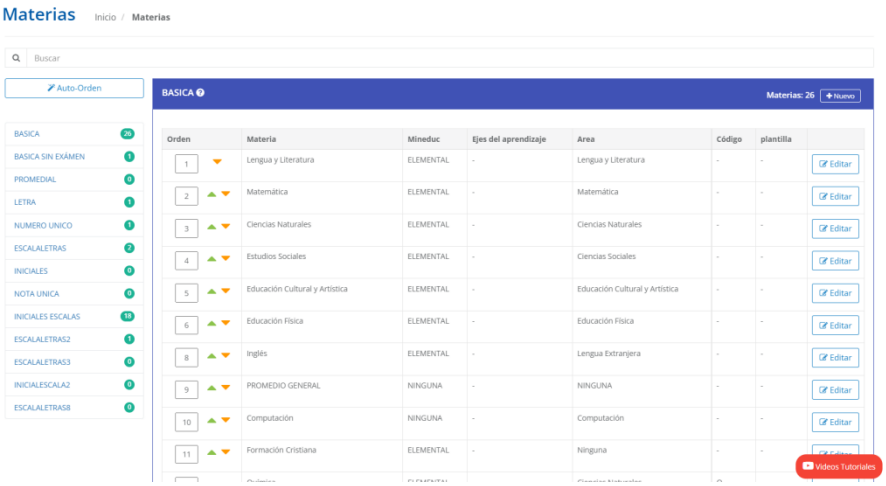


Figura 10: Agregar materias

- Agregar estudiantes

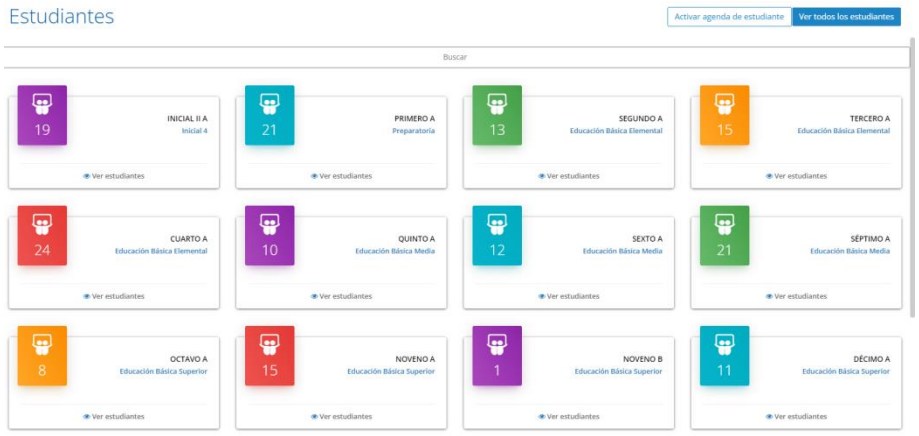


Figura 11: Agregar estudiantes

- Creación de horarios

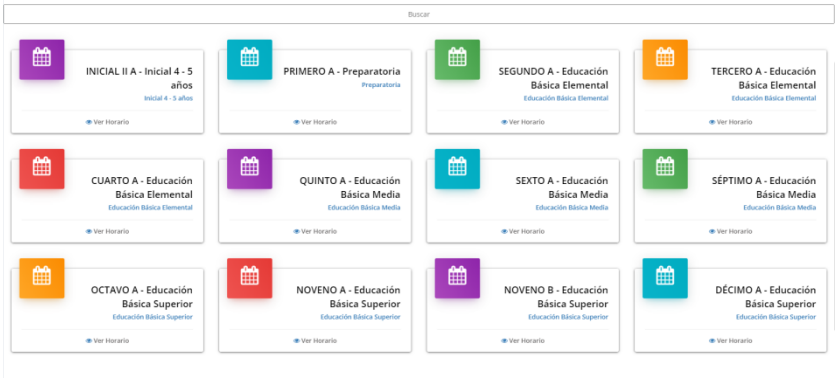


Figura 12: Horarios de clases

Figura 13: Creación de horarios en el sistema

- Desde el perfil administrativo se pueden hacer consultas de recaudaciones en intervalos de tiempo

Interacción con el aplicativo desde el navegador Mozilla.

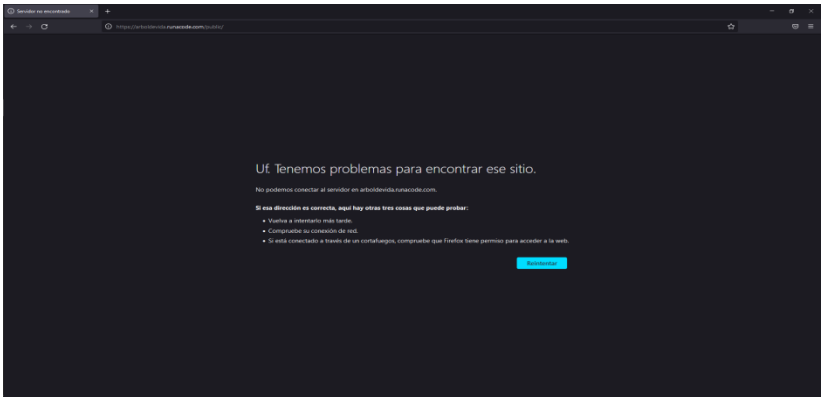


Figura 14: Fallos encontrados en el navegador Mozilla

En repetidas ocasiones los problemas se relacionan en computadores de profesores con preferencia a otros navegadores, su entorno es inaccesible.

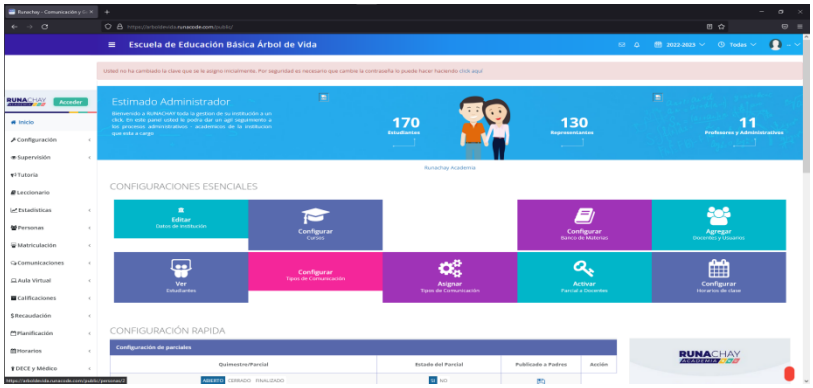


Figura 15: Entorno inaccesible

Además, el método de cargar información falla o es incompleta haciendo que usuarios, repetidas veces tengan que actualizar la página.

Interacción con el aplicativo desde el navegador Internet Explorer.

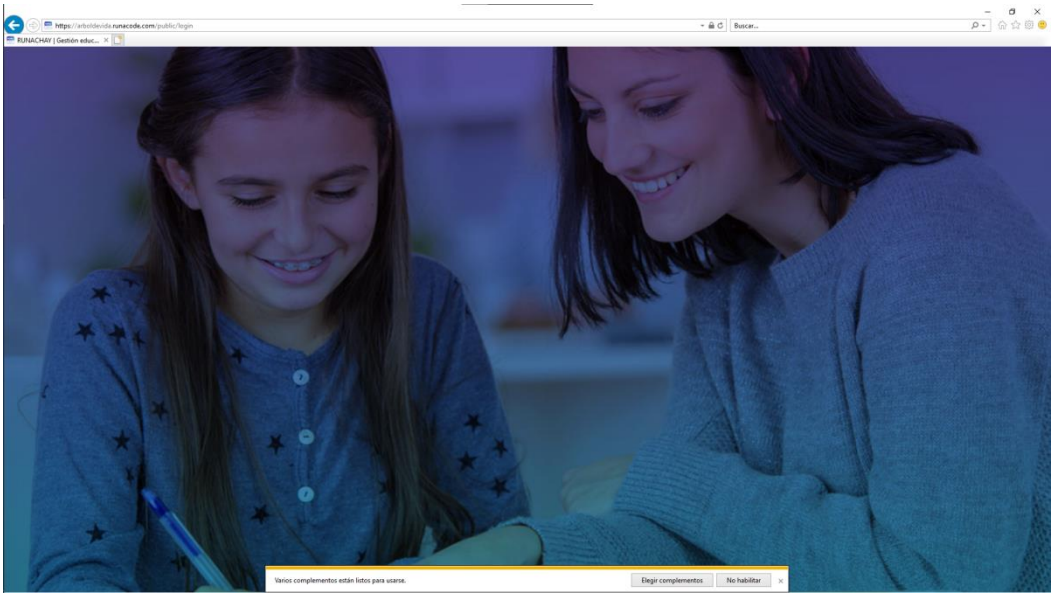


Figura 16: Fallos encontrados en el navegador Internet Explorer

En el caso de navegadores predeterminados, presenta fallas de carga o mucha lentitud haciendo tedioso el proceso de ingreso al sitio.

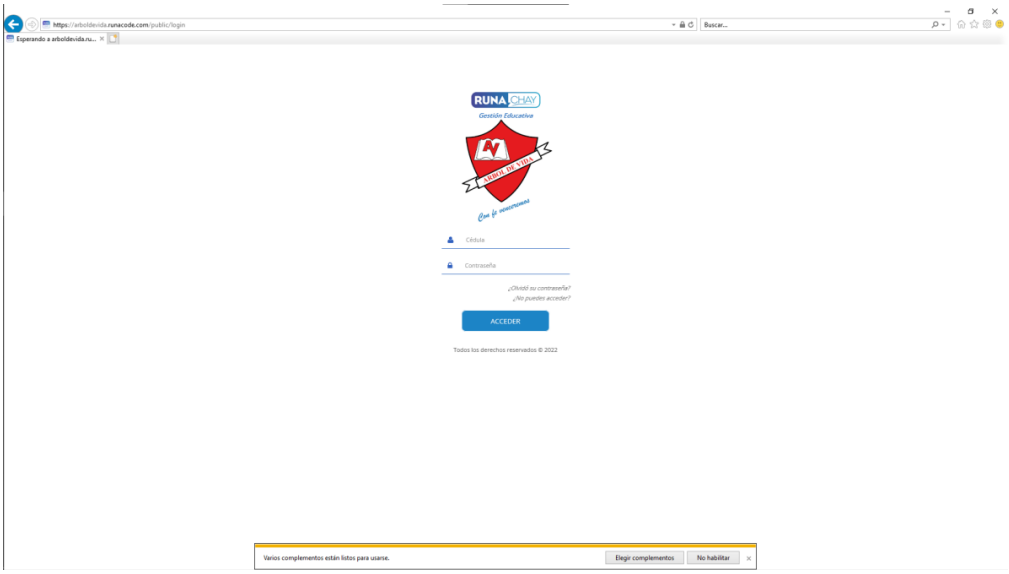


Figura 17: Lentitud al cargar en el navegador

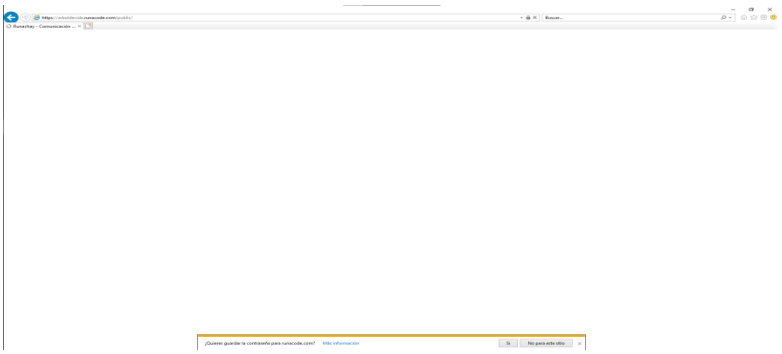


Figura 18: Fallos en navegador

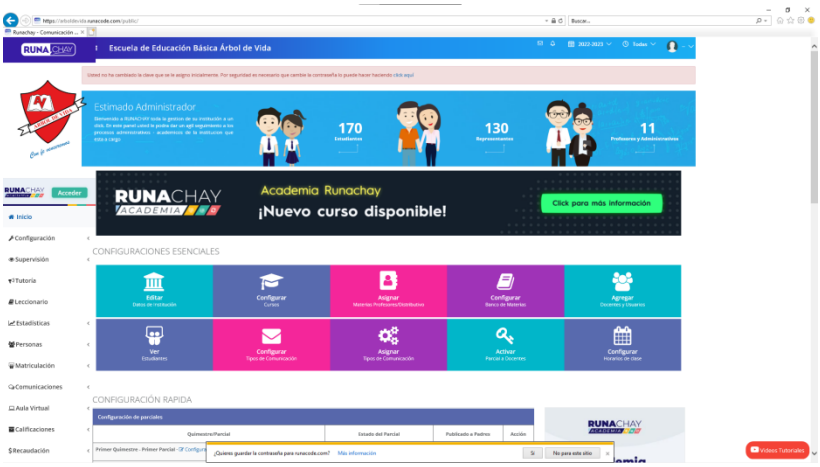


Figura 19: Interfaz incompleta por fallos

El entorno también se muestra diferente, como la imagen del logo se visualiza de forma descuadrada conforme al diseño original.

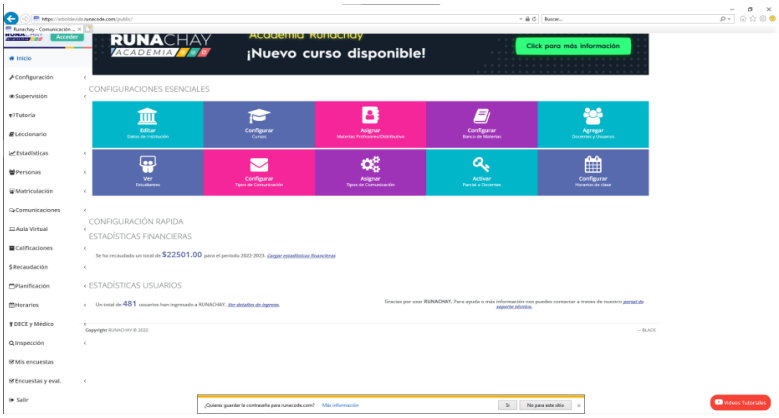


Figura 20: Entorno se muestra distinto

- No existe un resguardo seguro de información al solicitar copia de seguridad.

Figura 21: No existe un módulo de resguardo de información

- No contiene ninguna forma de actualizar la información de la aplicación, ni de mejorarlo.
- Al interactuar con el aplicativo desde un perfil docente, se evidenció retardos en la carga de información.

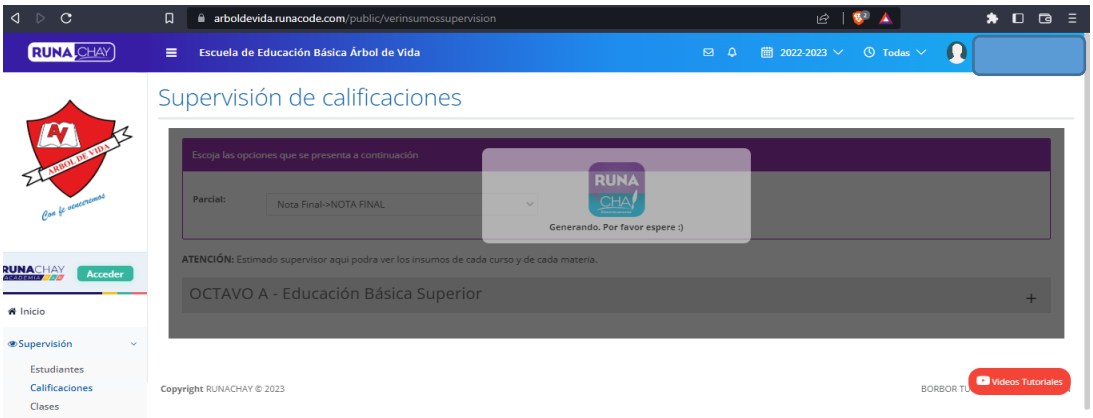


Figura 22: Módulo ingreso de notas tiene retardos de carga de información

- Desde el perfil administrador, se visualizó los representantes registrados en el aplicativo, hallando registro duplicados

Figura 23: Registros duplicados

- **Se encontró un registro vacío (sin datos)**

Figura 24: Registro vacío

Se visualizó el registro para verificar si estaba vacío.

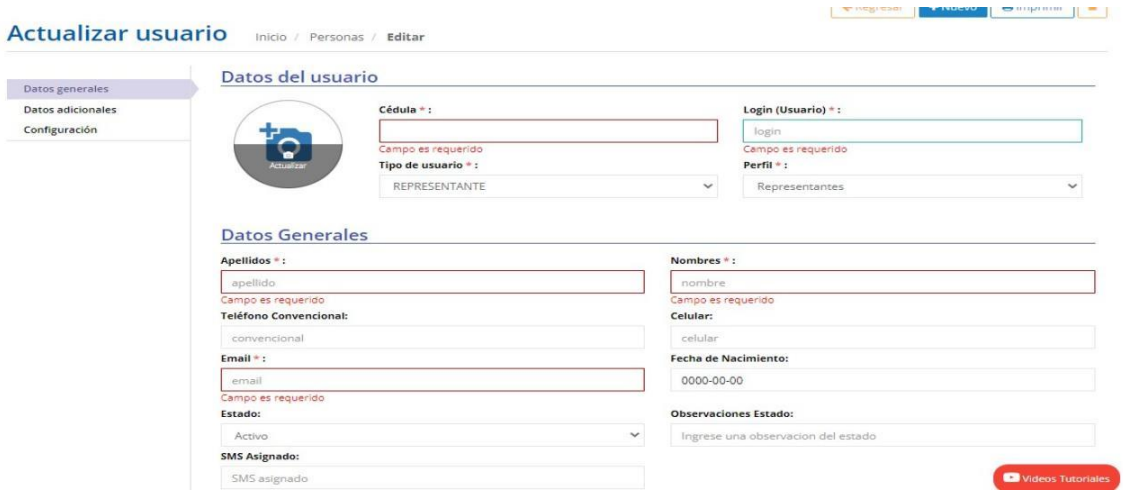


Figura 25: Visualización de registro vacío

Interacción desde un dispositivo móvil

- Carga incompleta del aplicativo

Figura 26: Carga incompleta del logo desde dispositivo móvil

- El contenido es confuso por su orden

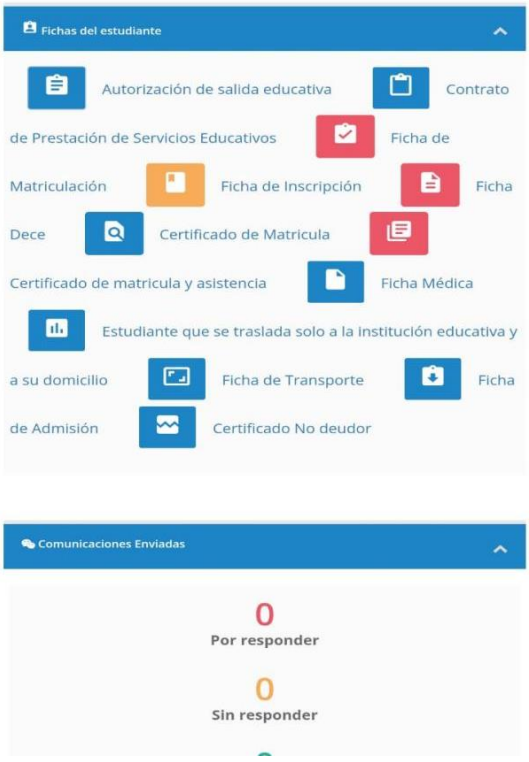


Figura 27: Diseño no responsivo

- Diseño de tabla no responsivo

Figura 28: Tabla de contenido no responsivo

Accesos al aplicativo según el tipo de usuario

Usuario	Nivel de prioridad al aplicativo	Acceso al aplicativo
Administrativo	**Alto (100%)**	• Ingreso de usuarios. • Ingreso de pagos. • Ingreso de notas. • Estadísticas (Dashboard). • Consultas. • Reportes. • Configuración de cursos. • Configuración de materias. • Asignación de maestros. • Vista de estudiantes. • Comunicación. • Activación de parciales. • Configuración de horarios. • Aulas virtuales. • Encuestas y evaluaciones.

Docente	**Medio Alto (45%)**	• Ingreso de notas. • Ingreso de evaluaciones. • Vista de horarios. • Aula virtual. • Envíos de comunicados.
Representante	**Medio (20%)**	• Ingreso de pagos. • Vista de notas • Comunicados • Recepción de comunicado. • Aula virtual. • Vista de Horarios
Estudiantes	**Medio Bajo (10 %)**	• Aula virtual. • Encuestas y evaluaciones. • Vista de Horarios

Tabla 30. Tabla de accesos al aplicativo según el usuario

Anexo 8. Mapeo Con Nmap

Se realizó el escaneo de la página web a través de la herramienta NMAP virtualizado en el sistema operativo Kali Linux con el código **nmap arboldevida.runacode.com**

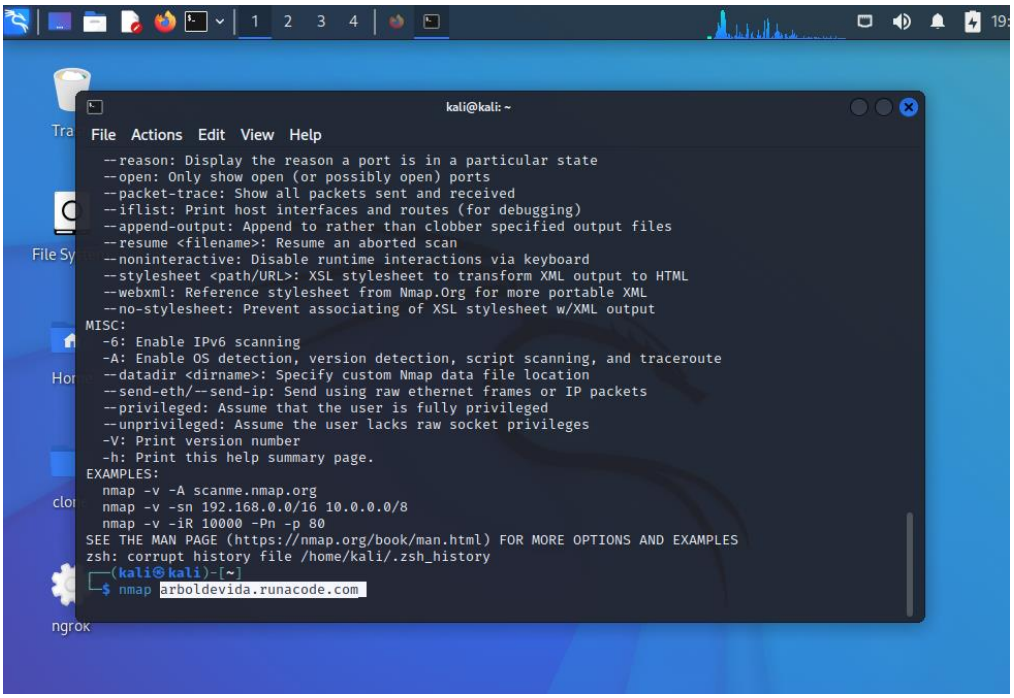


Figura 29: Escaneo con NMAP

Se procedió a ver los puertos abierto para realizar los escaneos determinados en el estudio dándonos como resultados 4 puertos abiertos y 996 puertos que están filtrados.

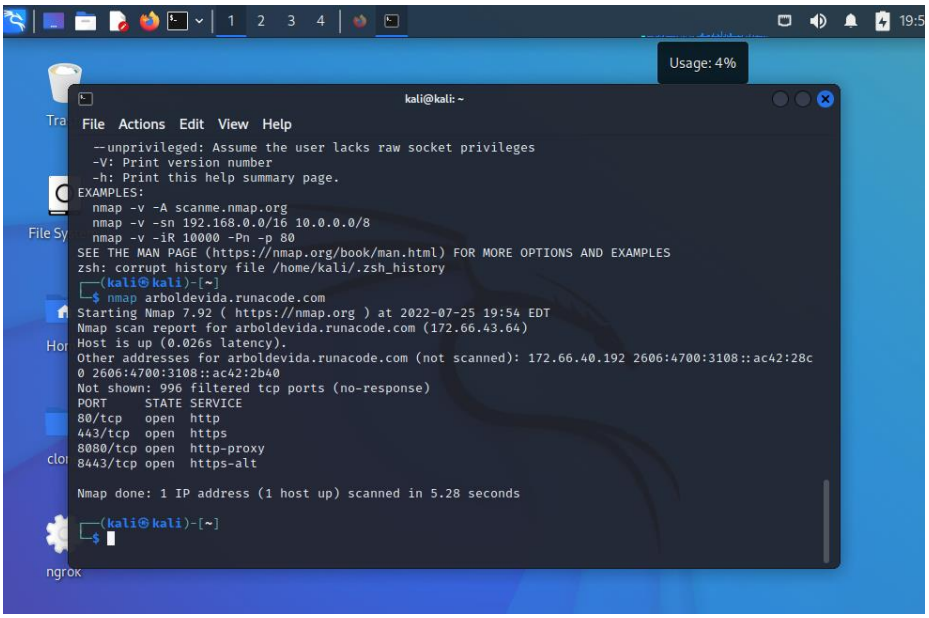


Figura 30: Escaneo de puertos abiertos

Al revisar los datos de los puertos se observó que el aplicativo web entra por medio de dos IP, esto nos permite analizar estas dos IP.

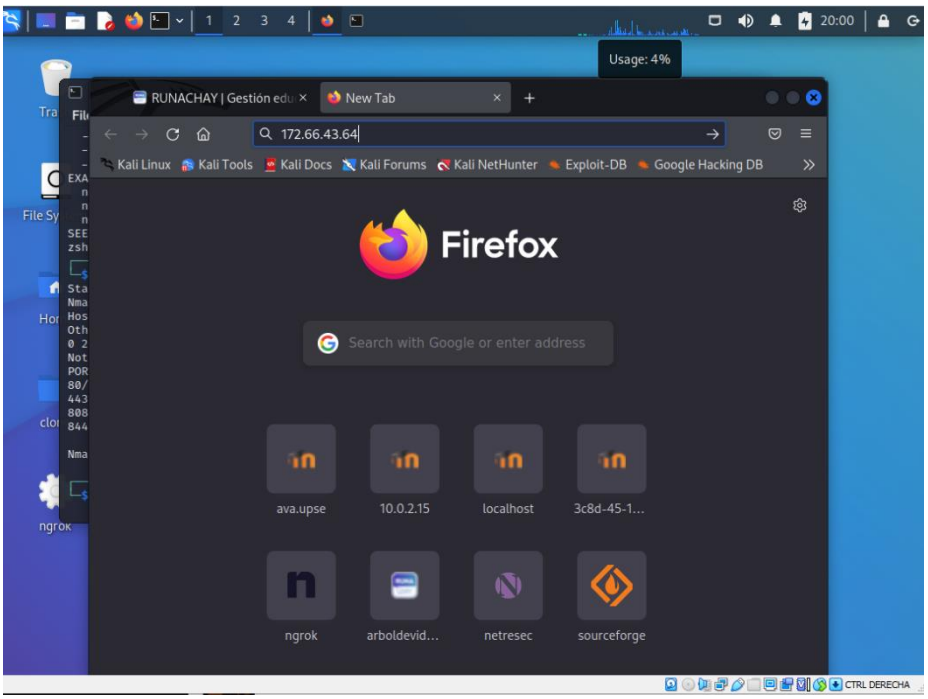


Figura 31: Determinación de IP encontradas

Se procedió a conectarse a las dos IP encontradas para inspeccionar su contenido el cual nos marcó un error al tratar de ingresar debido al servido donde se encuentra alojado.

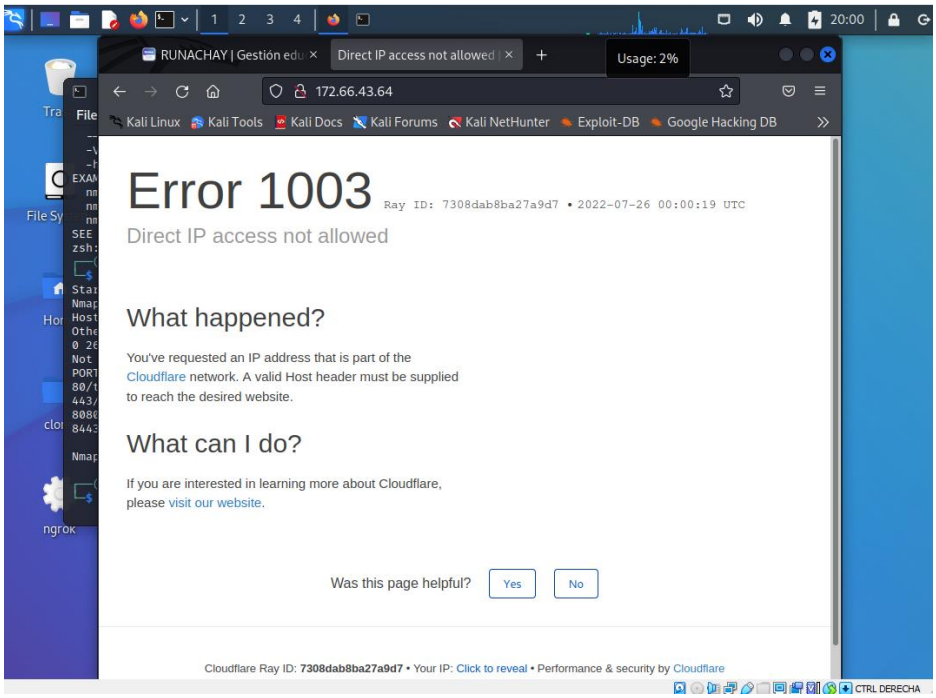


Figura 32: Resultados de la navegación de la IP 172.66.43.64

Los mismos resultados se presentaron en la otra IP dándonos un error 1003 que se referencia al servidor.

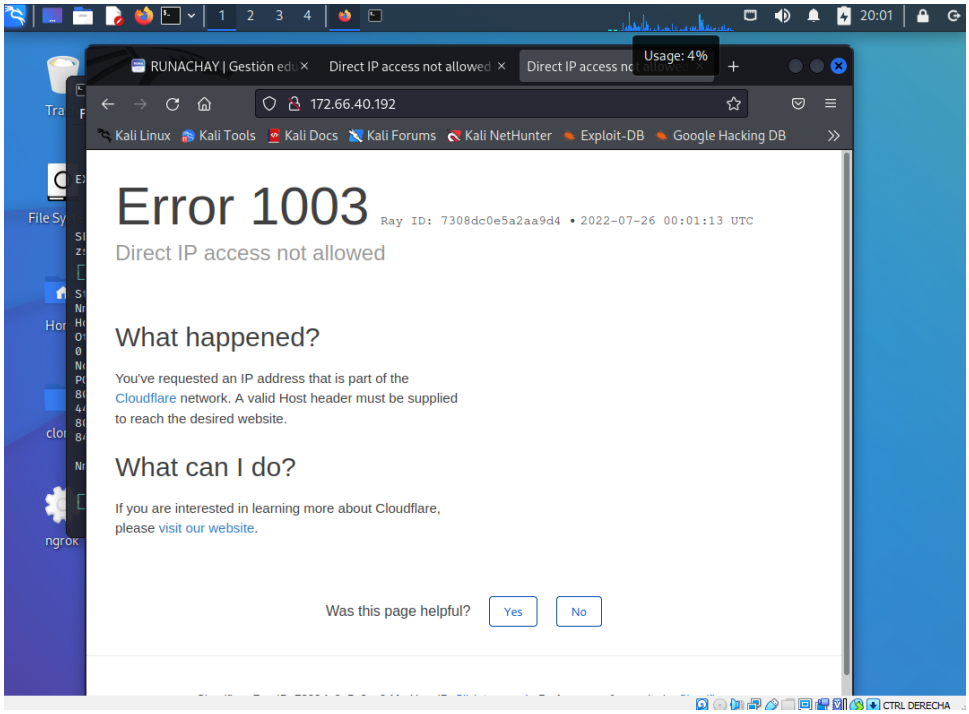


Figura 33: Resultados de la navegación de la IP 172.66.40.192

Se realizó también un NMAP de la misma manera a las IP para reafirmar si los datos obtenidos nos redirigen a los datos de origen mostrándonos de forma positiva esta confirmación.

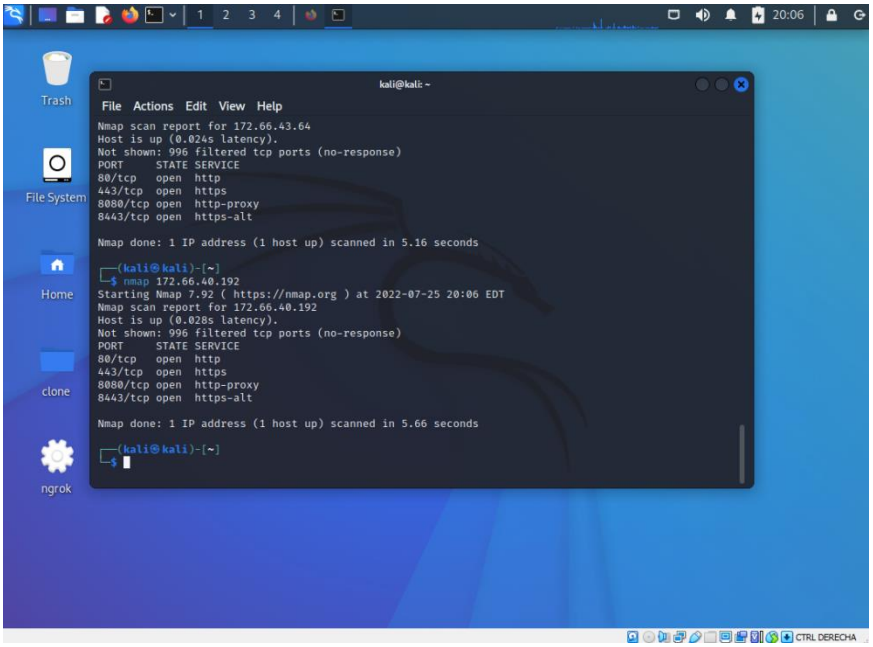


Figura 34: Resultados de NMAP en las IP encontradas

Se determinó el análisis de puertos específicos para poder observar sus especificaciones en cada una.

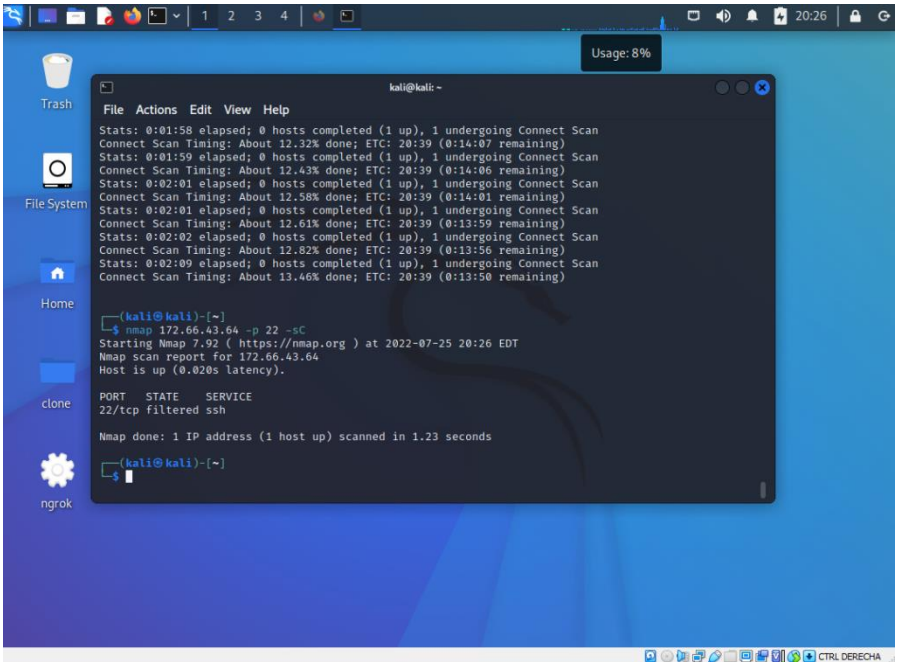


Figura 35: Resultados del puerto 22

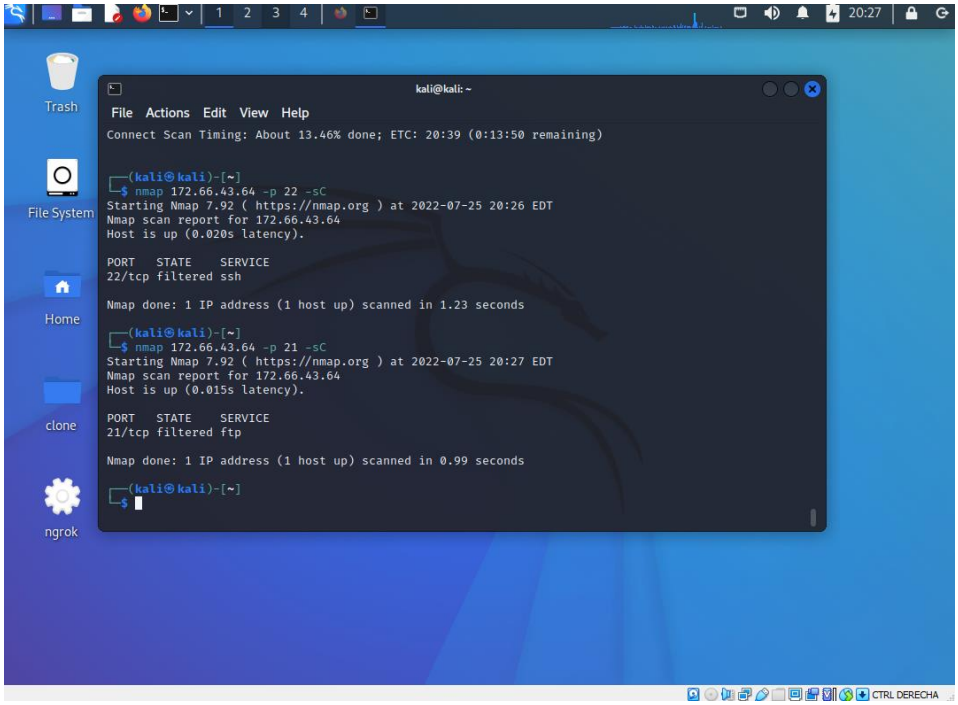


Figura 36: Resultados del puerto 21

Por último con el NMAP se usó el código -SV al puerto 80 que es uno de los puertos abierto para poder determinar con que servidor trabaja el aplicativo web dándonos como resultado que trabaja con un servidor Cloudflare.

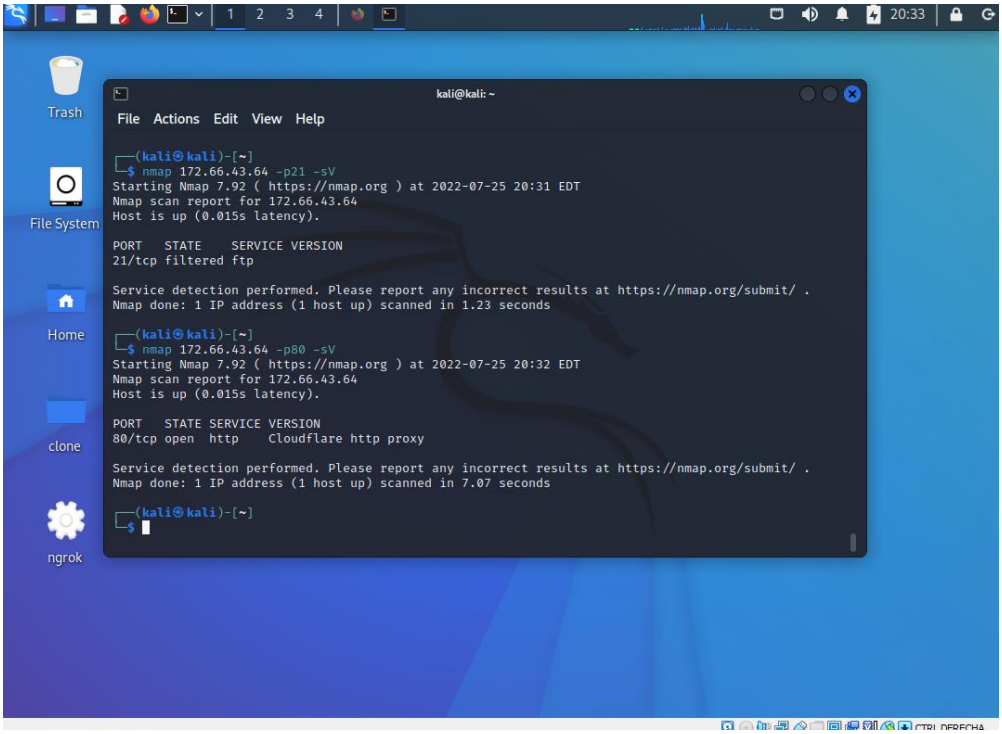


Figura 37: Determinar servidor con NMAP

Por último se usó el código -A que es considerado como un análisis agresivo o más profundo, alias para -O -sV -sC –traceroute, obteniendo, la detección de sistema operativo, la detección de versiones, la ejecución de scripts de seguridad y la determinación de la ruta hacia el objetivo. Esta opción es útil para obtener una visión general de la información de seguridad y la configuración de un sistema en una sola ejecución.

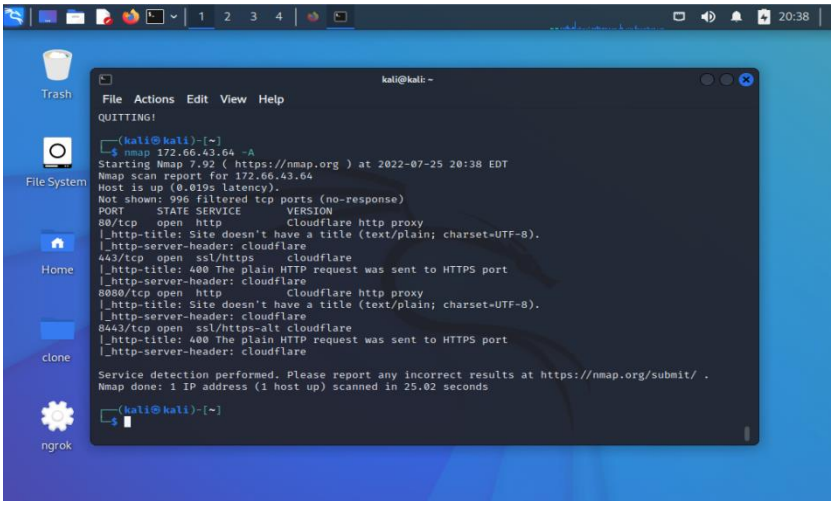


Figura 38: Resultados completo del NMAP

Anexo 9. Mapeo Con Nikto

Con la herramienta nikto haremos un escaneo al aplicativo web con el comando **nikto -h arboldevida.runacode.com** el cual nos mostrará datos como: direcciones ip, el servidor web que usa y vulnerabilidades en caso de que hayan.

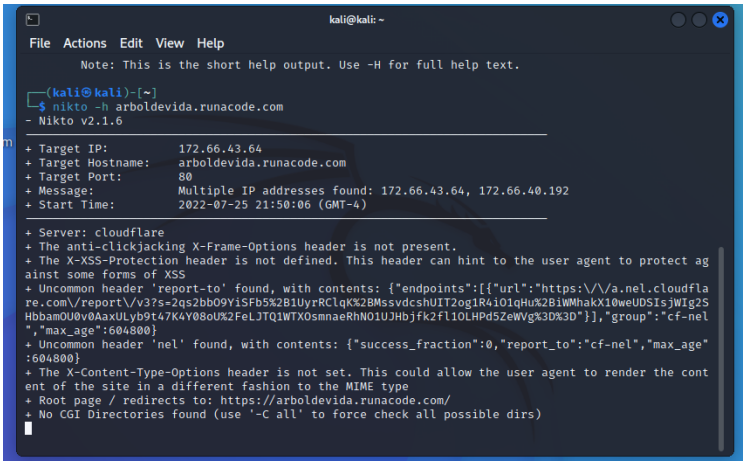


Figura 39: Resultados del escaneo con NIKTO

Se realizó un escaneo hacia un puerto en específico con el comando nikto –h 172.66.43.64 p 80

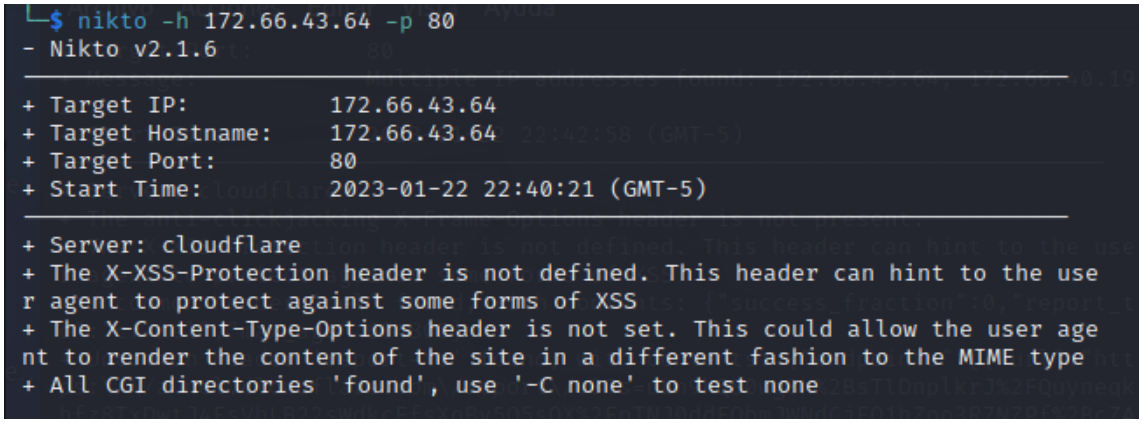


Figura 40. Escaneo hacia un puerto especifico con NIKTO

A continuación escanearemos la integridad de archivos utilizando los siguientes parámetros:

d = modo de depuración

v = mostrar detalles

h = host a escanear

nikto -D v -h arboldevida.runacode.com

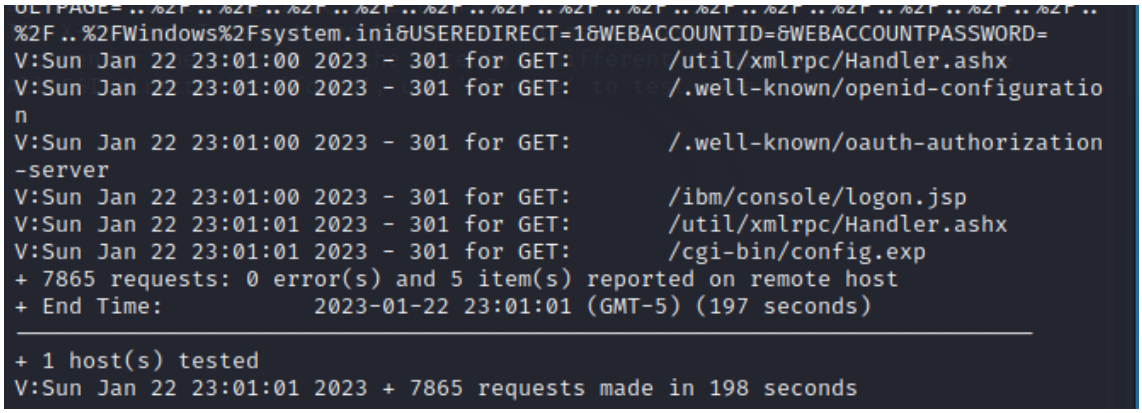


Figura 41: Resultados del escaneo con NIKTO

Después del escaneo, no se encontraron errores en archivos o enlaces.

También se realizó un análisis ssl con el comando nikto –h 172.66.43.64 –ssl

```
┌──(kali㉿kali)-[~]
└─$ nikto -h arboldevida.runacode.com -ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.66.40.192
+ Target Hostname:    arboldevida.runacode.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Francisco/O=Cloudflare
, Inc./CN=sni.cloudflaressl.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Cloudflare, Inc./CN=Cloudflare Inc ECC C
A-3
+ Message:         Multiple IP addresses found: 172.66.40.192, 172.66.43.6
4
+ Start Time:      2023-01-22 23:35:08 (GMT-5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'nel' found, with contents: {"success_fraction":0,"report_t
o":"cf-nel","max_age":604800}
+ Uncommon header 'report-to' found, with contents: {"endpoints":[{"url":"htt
ps:\/\/a.nel.cloudflare.com\/report\/v3?s=yyX26VAfpD1u4CDWtsB9g2Zusp%2FG2LM0p
bOYzIq5pkEIqgxn0v%2Bis43%2Bw0sJ7YKBaTyo55SSAtekMtnm%2BnN5j%2BjkyYKV7mhUnodoJ3
fqcaJelKfsVJHIx5z22QcSIPer9z4LFEDUjfO66Q%3D%3D"}],"group":"cf-nel","max_age":
604800}
```

Figura 42: Análisis SSL con NIKTO

Se obtuvo que la sesión de laravel de cookies es creada sin bandera segura

```
+ The site uses SSL and Expect-CT header is not present.
+ Root page / redirects to: public
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved access-control-allow-origin header: *
+ Cookie laravel_session created without the secure flag
+ Cookie 7079186a6d90f1f0e6ab13dcc7305ebc91c6f0bd created without the secure
flag
+ Entry '/public/' in robots.txt returned a non-forbidden or redirect HTTP co
de (302)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening st
ream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl
v3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
 at /var/lib/nikto/plugins/LW2.pm line 5157.
;  at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated:  20 error(s) and 9 item(s) reported on remote host
+ End Time:           2023-01-22 23:36:18 (GMT-5) (70 seconds)
```

Figura 43: Resultados de SSL con NIKTO

Anexo 10. Escaneo de vulnerabilidades con la herramienta owasp zap

OWASP cuenta con herramientas realizar escaneos y verificar si existe vulnerabilidad en las aplicaciones que se desean analizar para mostrar el entorno.

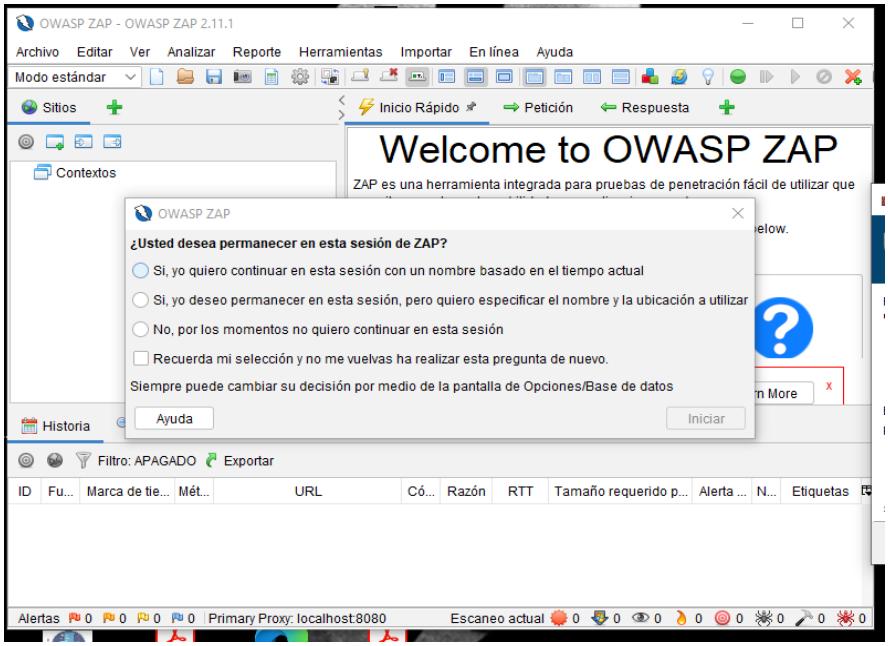


Figura 44: Herramienta OWASP

Entre las opciones se determinará si se desea hacer un escaneo y un ataque, para poder determinar varios puntos vulnerables.

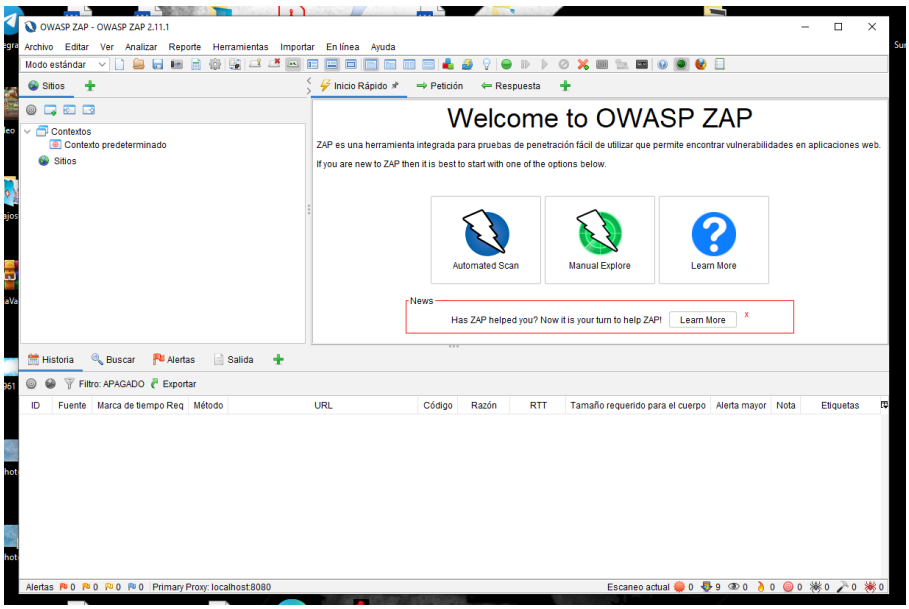


Figura 45: Opciones de la herramienta OWASP

Para comenzar con esta técnica, se procede escribiendo la URL que se solicita hacer el ataque, como es un sistema OWASP, determinará por defecto lo que sea necesario para iniciar el navegador.

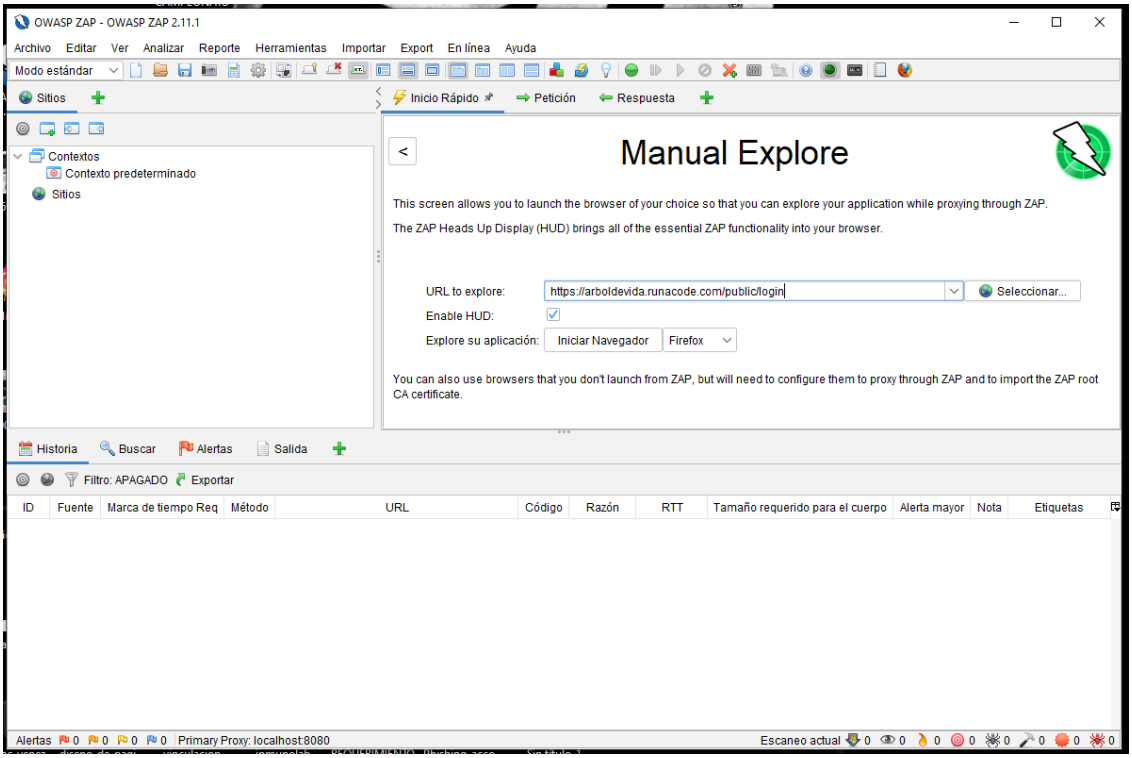


Figura 46: URL que se solicita realizar el ataque

Se comenzará a determinar los GET y los POST de entrada y salida para buscar las vulnerabilidades que recorren durante el proceso, dando como resultados, diferentes banderas de bajo, medio y alto.

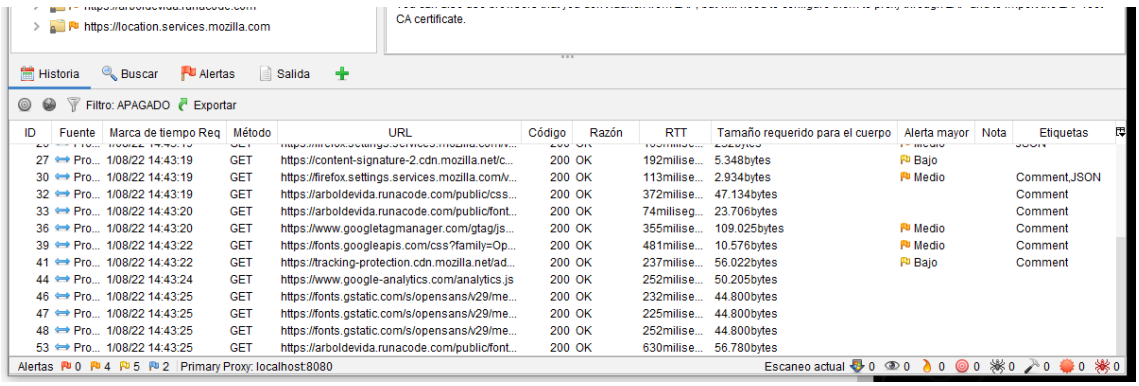


Figura 47: Determinación de los GET y POST de entrada y salida

En el mismo instante, también se abre un navegador, el cual fue seleccionado en el iniciador del programa, se puede encontrar vulnerabilidad dependiendo del navegador. Se diferencia a un navegador por la franja roja que aparece en la dirección.

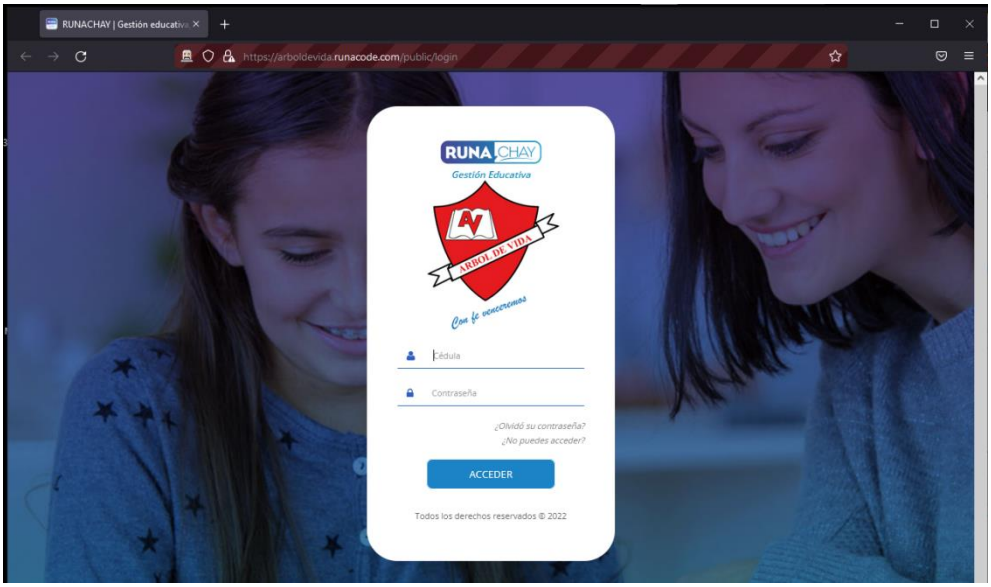


Figura 48: Abrir el navegador

Se pudo determinar que, en el navegador Firefox no se logró obtener un enfoque del programa, así que se procedió al escaneo por medio de navegador Google Chrome, para obtener información a través de ella.

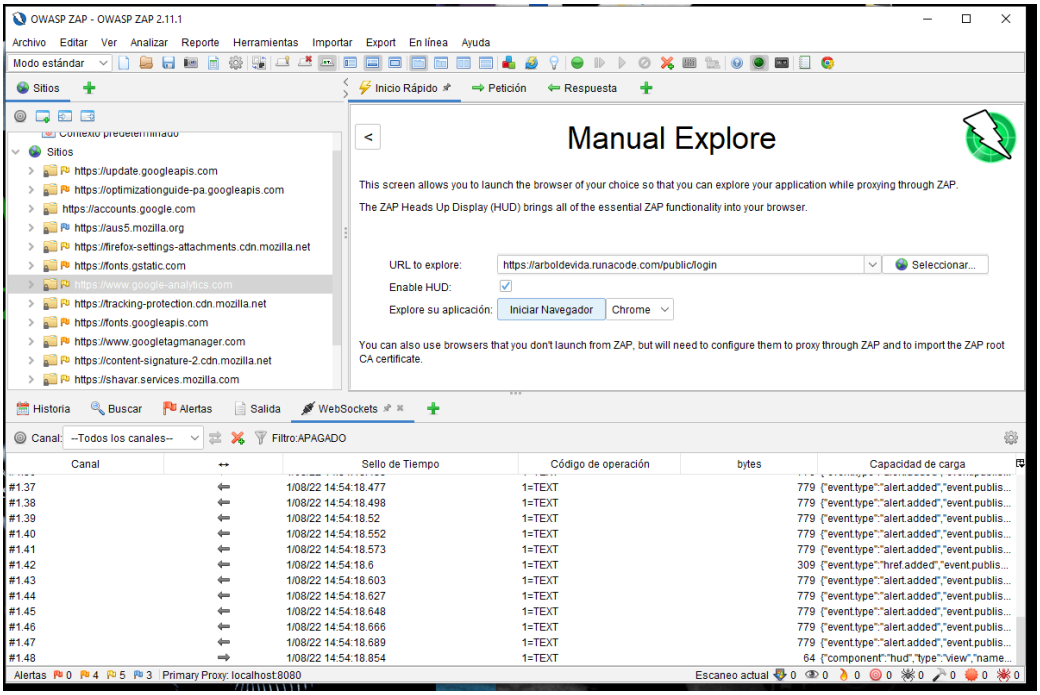


Figura 49: Escaneo por medio de navegador Google Chrome

La ventana obtenida en el navegador Chrome, se ilustró de una manera distinta a Firefox, indicando el emparejamiento óptimo que se dió con el Zap, mostrando una guía del manejo.

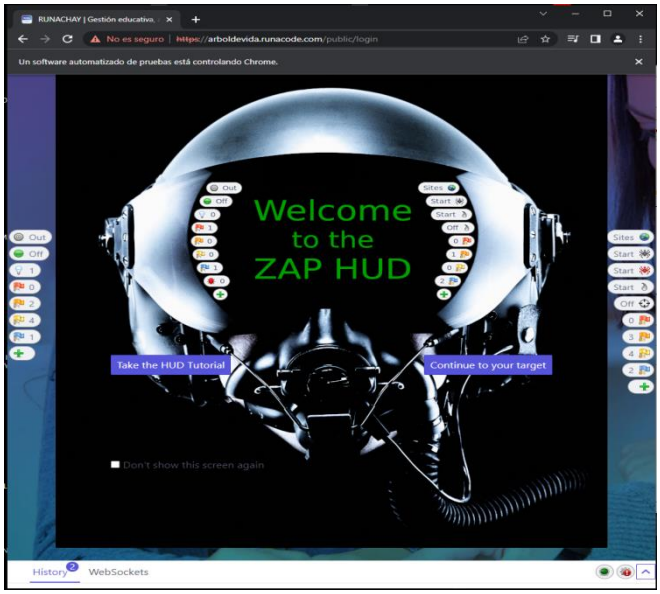


Figura 50: Ventana obtenida en el navegador Chrome

Luego de un lapso de tiempo, esta pantalla de introducción desaparece y aparecerá la pantalla del aplicativo web mostrando todas las vulnerabilidades, las cuales se detallarán en cada imagen.

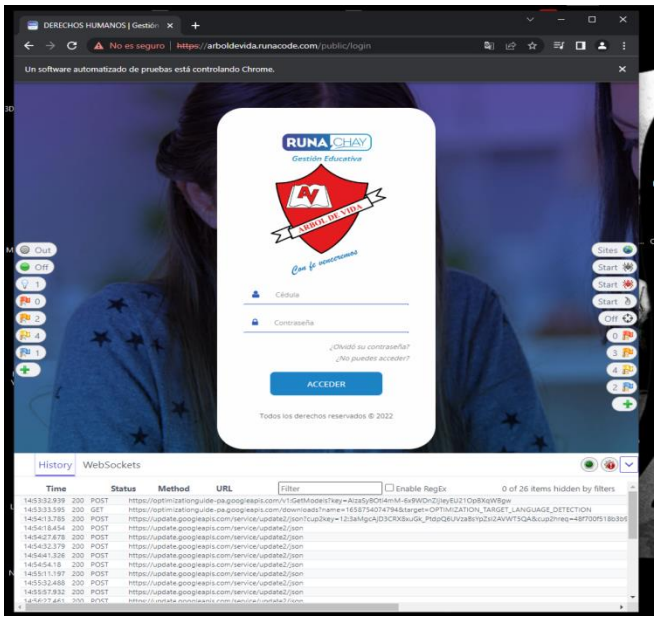


Figura 51: Pantalla del aplicativo web con las vulnerabilidades

En las banderas de la derecha, se encontrarán los riesgos de las páginas desde lo peligroso, medio y bajo. Entre los ataques medios se encuentran:

Content security policy (CSP) header not set: Es una capa adicional de seguridad que permite detectar y mitigar diversos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos.

Missing anti-clickjacking header: La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options, protegiendo contra los ataques de 'ClickJacking'.

Vulnerable JS library: Utiliza una o más bibliotecas de JavaScript que son vulnerables.

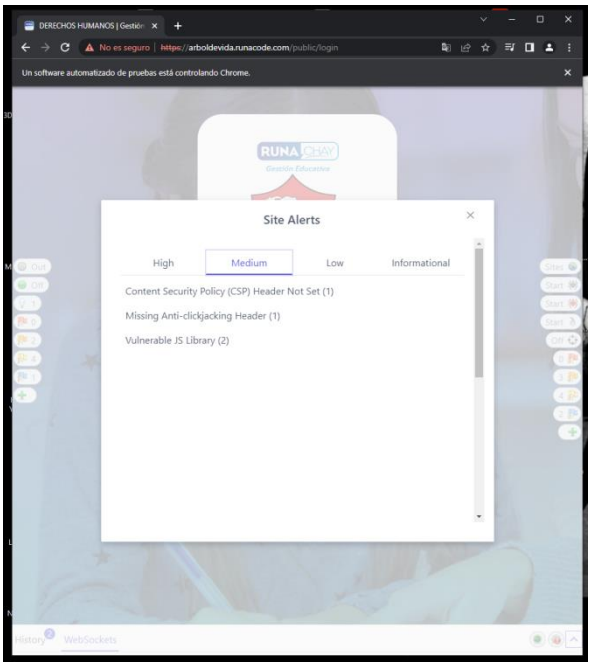


Figura 52: Tipos de ataques medios

Entre los ataques bajos se puede encontrar:

Cookie without Secure flag: Se ha configurado una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la misma, mediante conexiones no cifradas.

Cookie without samesite attribute: Se ha configurado una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud de 'entre sitios'.

Cross-domain JavaScript Source file inclusion: La página incluye uno o más archivos de script de un dominio de terceros.

Divulgación de la marca de hora – Unix: Una marca o sello es un tiempo registrado en un archivo, registro o notificación que ingresa cuándo se agregan, eliminan, cambian o transmiten los datos.

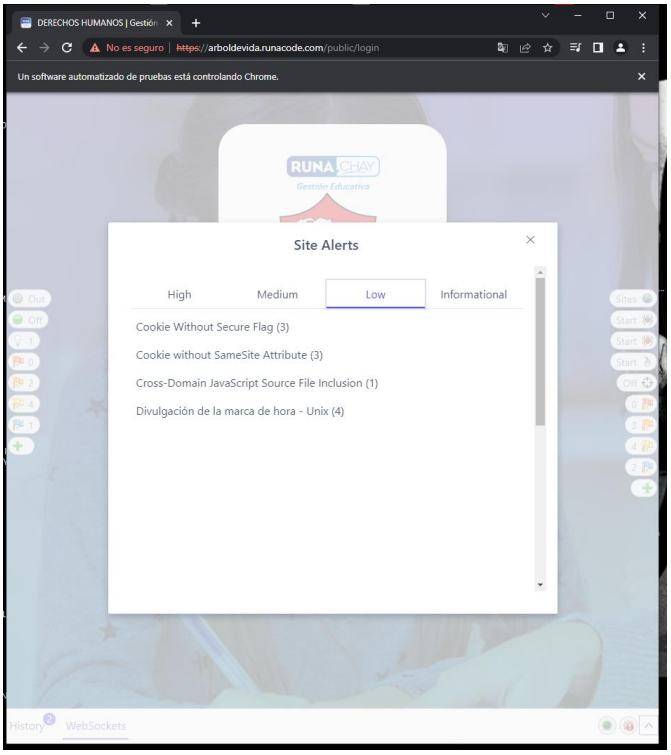


Figura 53: Tipos de ataques bajos

En la pestaña informacional, se determinó lo siguiente:

Divulgación de información - comentarios sospechosos

Re-examine cache-control directives: El encabezado de control de caché no se ha configurado correctamente o falta

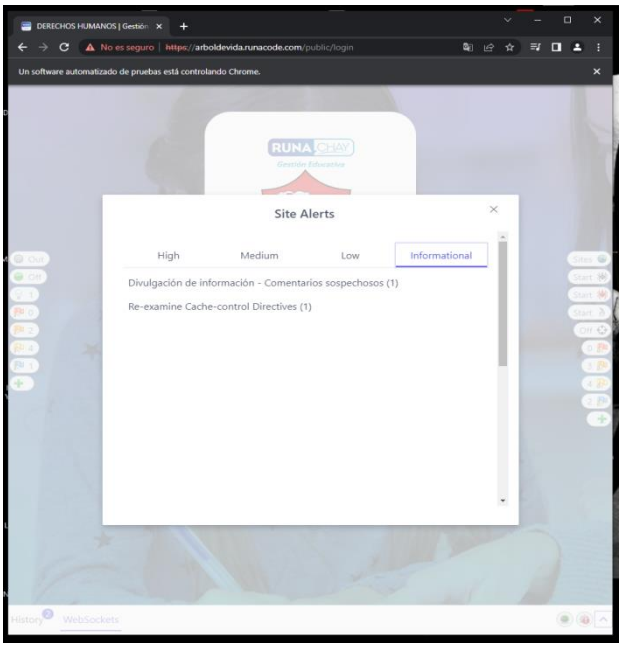


Figura 54: Pestaña informacional

En la siguiente imagen, se inició un escaneo para determinar los fallos ya encontrados.

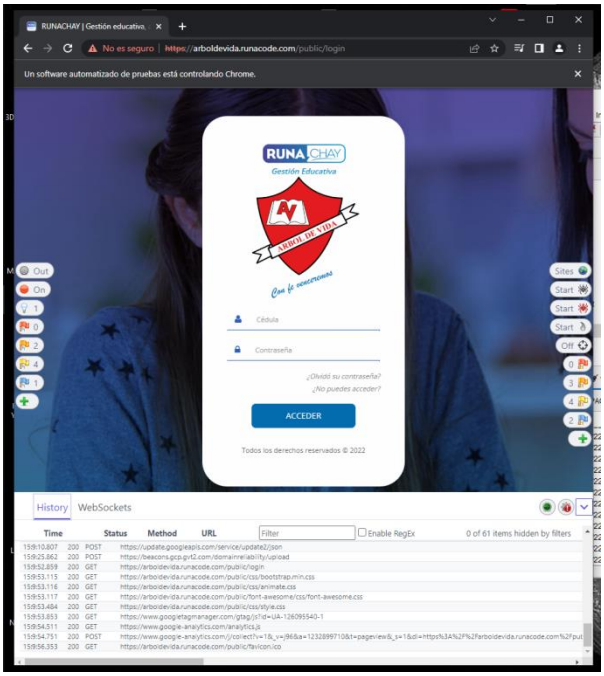


Figura 55: Inicio de escaneo

Entre los primeros escaneos que se realizaron, se encontraron componentes ocultos, por ejemplo, el text box que se ve a continuación con un código descriptivo.

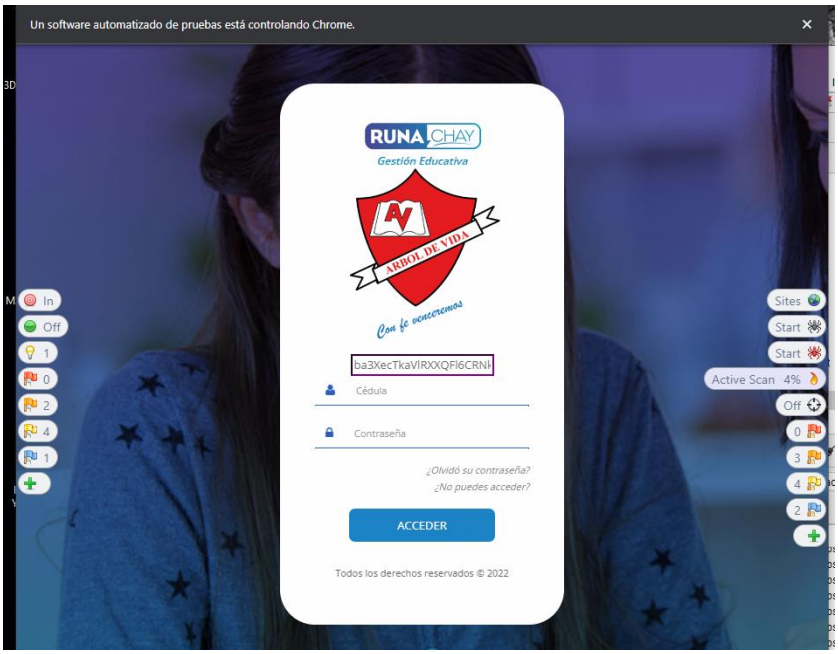


Figura 56: Componentes ocultos en el aplicativo web

Después, se procede a ejecutar un spider, que determina contenidos masivos dentro de todo el aplicativo web, el cual se mantiene un tiempo establecido.

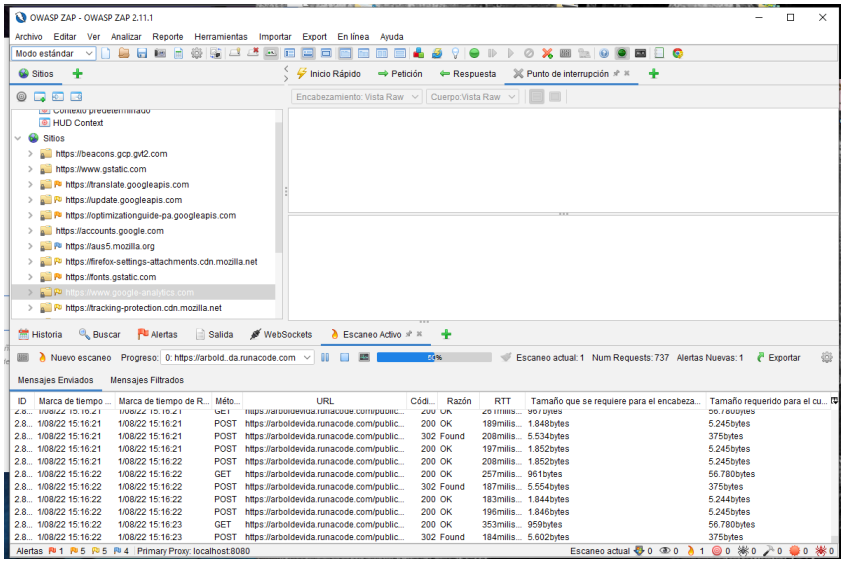


Figura 57: Spider

SEGUNDO ESCANEO REALIZADO

En el segundo apartado del Zap, se encuentra el Auto Scanner, el cual explora el sitio web en busca de posibles vulnerabilidades de seguridad. En esta acción, también se elegirá el tipo de navegador para el ataque.

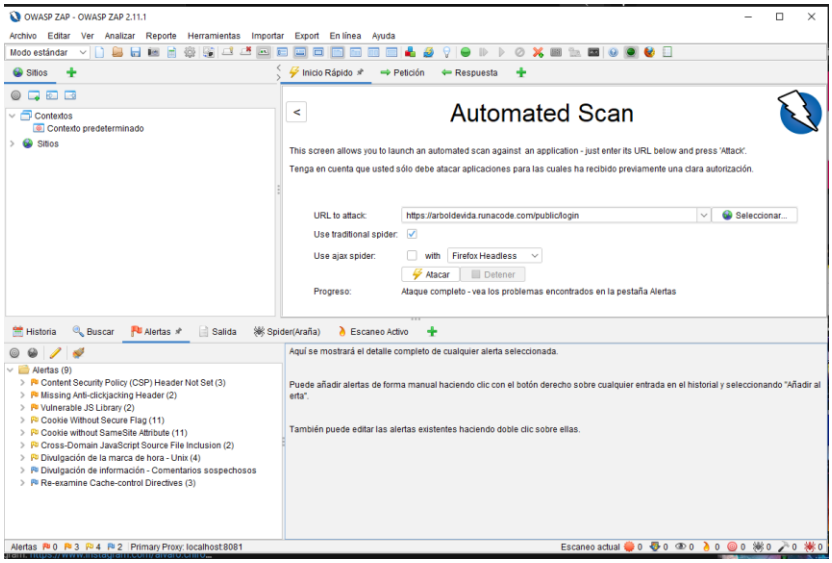


Figura 58: Auto Scanner

Una vez terminado el escaneo, mostrará un informe del ataque más recurrente, brindando datos del mismo.

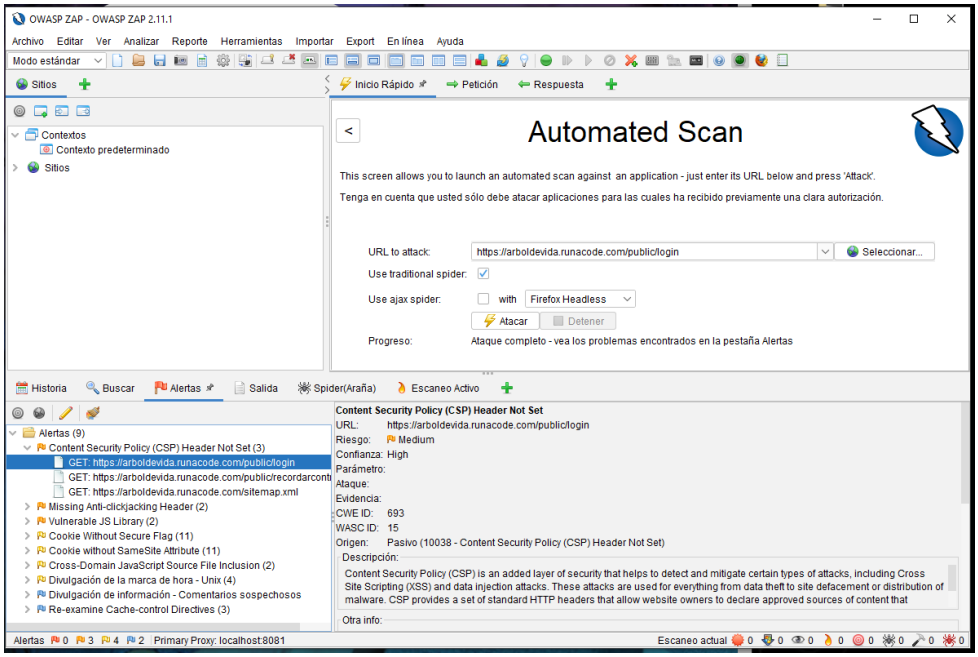


Figura 59: Informe del ataque más recurrente

Una vez terminado el escaneo, mostrará un informe del ataque más recurrente, brindando datos del mismo.

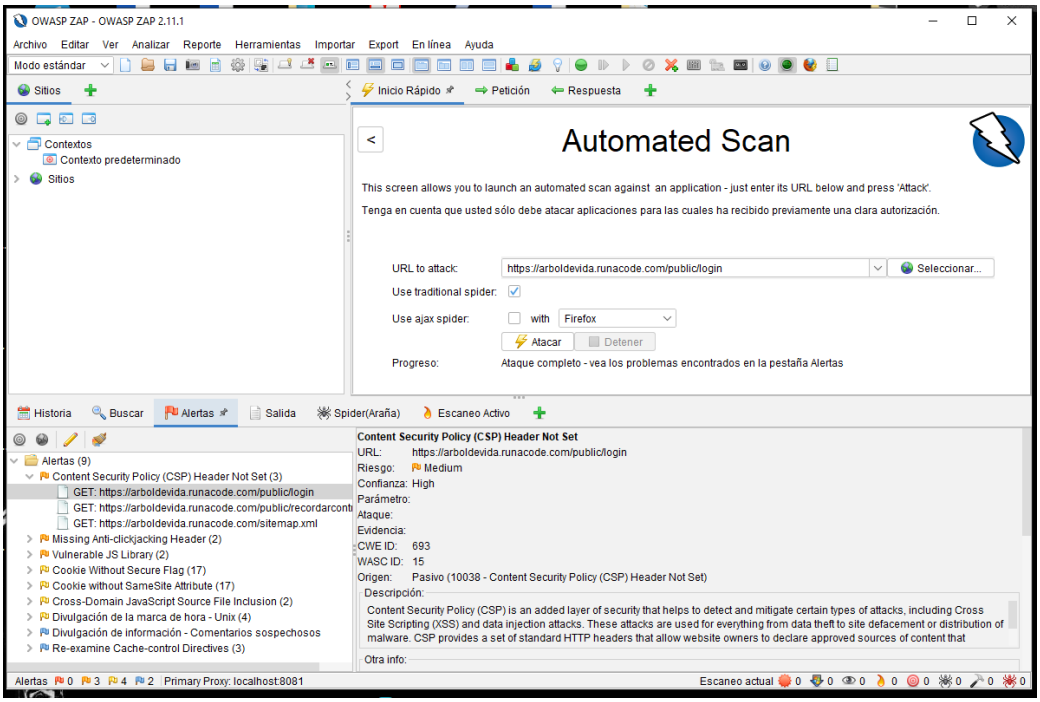


Figura 60: Informe del ataque más recurrente

Las siguientes ventanas son demostrativas del programa, donde arroja datos del ataque, que proviene de la entrada más vulnerable para su protección.

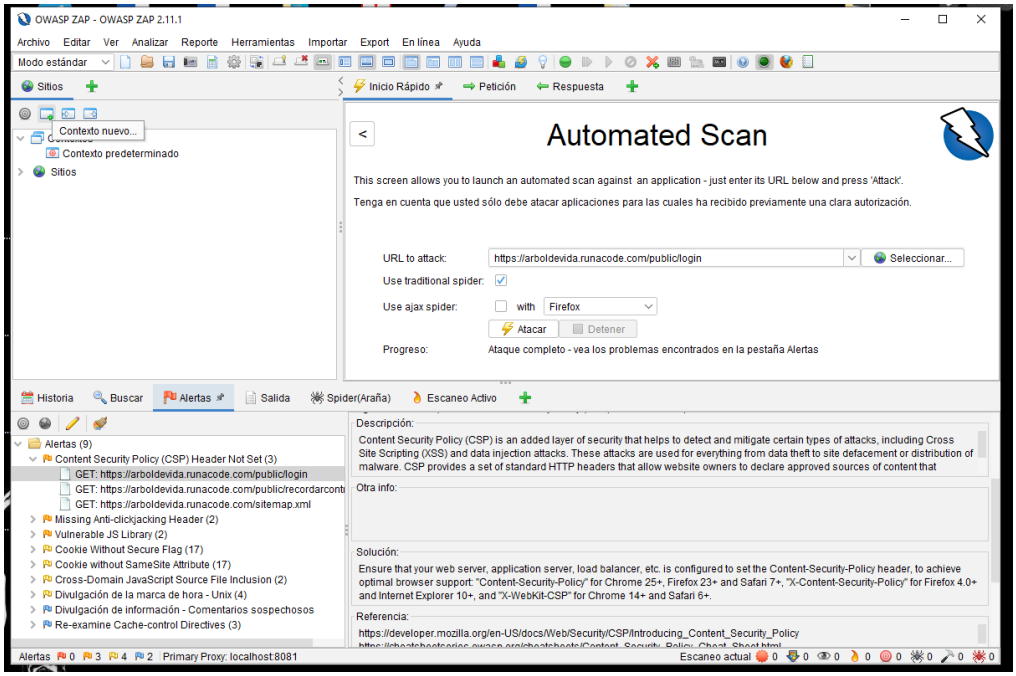


Figura 61: Información obtenida

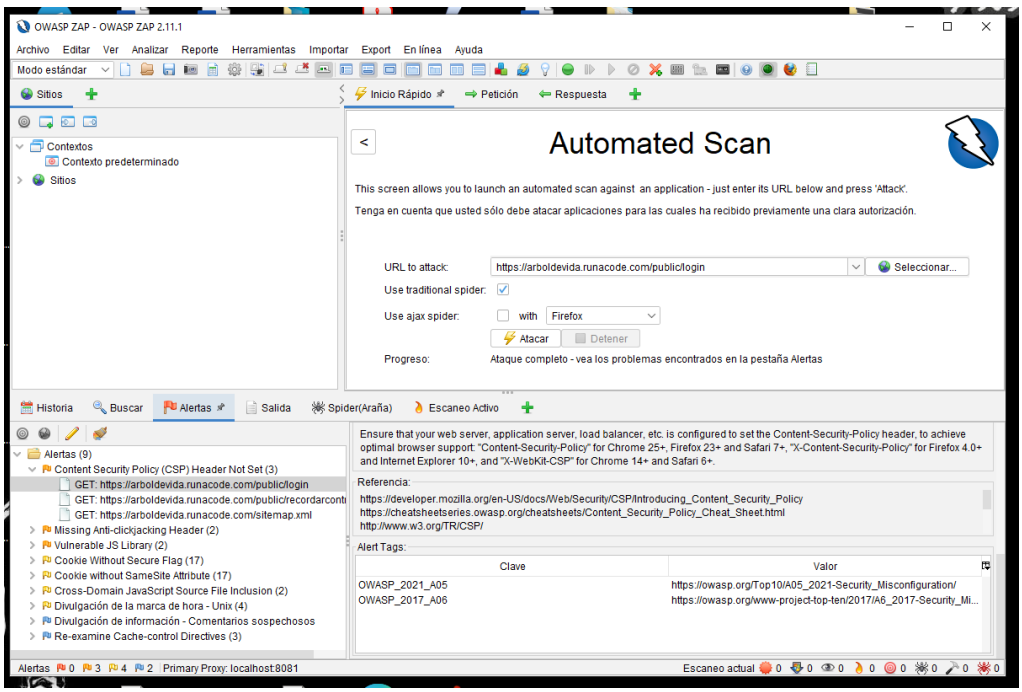


Figura 62: Información obtenida

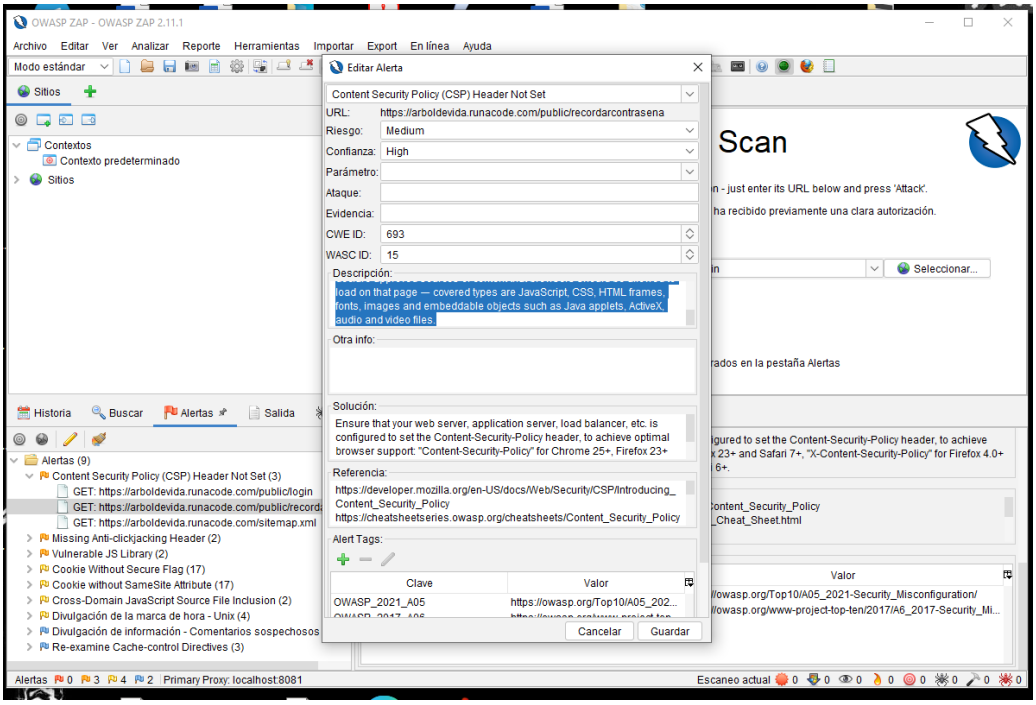


Figura 63: Información obtenida

La herramienta brinda un reporte de cada una de las alertas que fueron encontradas en cada escaneo ejecutado, como un informe en HTML, detallando el riesgo y la confianza.

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medio	4 (44,4%)
Missing Anti-clickjacking Header	Medio	2 (22,2%)
Vulnerable JS Library	Medio	2 (22,2%)
Cookie Without Secure Flag	Bajo	44 (488,9%)
Cookie without SameSite Attribute	Bajo	44 (488,9%)
Cross-Domain JavaScript Source File Inclusion	Bajo	2 (22,2%)
Divulgación de la marca de hora - Unix	Bajo	4 (44,4%)
Divulgación de información - Comentarios sospechosos	Informativo	1 (11,1%)
Re-examine Cache-control Directives	Informativo	3 (33,3%)
Total		9

Figura 64: Reporte de las acciones ejecutadas

Anexo 11. Prueba funcionamiento de interfaz en módulo matriculación

Objetivo: evaluar el funcionamiento del módulo de matriculación

Condiciones de formulario de matriculación (campos obligatorios)

- Sección de datos principales de estudiante

Dato	**Condición**
Fecha de solicitud	Fecha actual
Cedula	Numero de diez dígitos
Apellidos	Cadena de caracteres <=2 o >=30
Nombres	Cadena de caracteres <=2 o >=30
Dirección	Cadena de caracteres
Fecha de nacimiento	Formato dd/mm/aaaa y en un rango de edad valida

Tabla 31. Condiciones de formulario de matriculación en la sección de estudiante.

- Sección datos del representante

Dato	**Condición**
Cedula	Numero de 10 dígitos
Apellidos	Cadena de caracteres <=2 o >=30
Nombres	Cadena de caracteres <=2 o >=30
Email	Formato usuario@example.com
Celular	Numero de 10 dígitos

Tabla 32. Condiciones de formulario de matriculación en la sección de representante

Prueba 1: Verificar/validar el ingreso correcto de datos en el formulario de matriculación.

Entradas	Salidas esperadas	Salidas obtenidas	Nivel de complejidad
Llenar todo el formulario con datos incorrectos/inválidas	Que el sistema valide cada dato, sino cumple con las condiciones mostrar mensaje de error, no permitir la matricula	Matrícula procesada	Bajo
No llenar todos los campos obligatorios.	Mostrar mensaje que debe llenar campos faltantes, no permitir seguir con el proceso	No permite seguir con el proceso de matriculación	Bajo
Ingreso de fecha con formato y fuera de rango de edad adecuado para estudiantes.	Mensaje de error: ingrese fecha de nacimiento en un rango de edad valida, no permitir matriculación	No hay validación de fecha, Matricula igual sigue su proceso	Bajo

Tabla 33. Prueba de validación de ingreso de datos en el formulario de matriculación

Procese:

Al estar en el apartado matriculación de estudiantes, se llena todos los campos de texto y de selección con datos incorrectos, inválidos, inexistentes en la sección datos principales del estudiante

Figura 65: Interfaz de registro

Permite el ingreso de fechas actuales como fecha de nacimiento

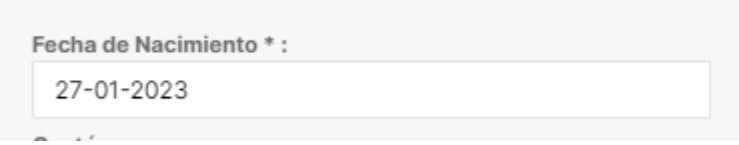


Figura 66: Fecha de nacimiento no valida

Luego se llena todos los campos de texto y de selección con datos incorrectos, inválidos, inexistentes en la sección datos principales del representante

Figura 67: Interfaz de datos de representante

En la parte inferior de la sección de datos del representante se puede observar una nota

NOTA IMPORTANTE: Los datos como número celular y correo eléctronico del representante serán utilizados para comunicar la información generada por Runachay.

Figura 68: Nota importante en la sección de ingreso de datos del representante

En la última sección de este apartado, hay datos de facturación que se llenan automáticamente con los datos del representante ingresados anteriormente

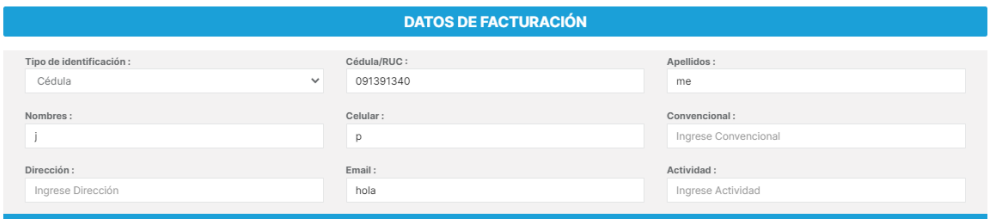


Figura 69: Validación de datos de ingreso

Al presionar el botón grabar, se guardan los datos y aparece una pantalla de registro exitoso con los datos del estudiante matriculado

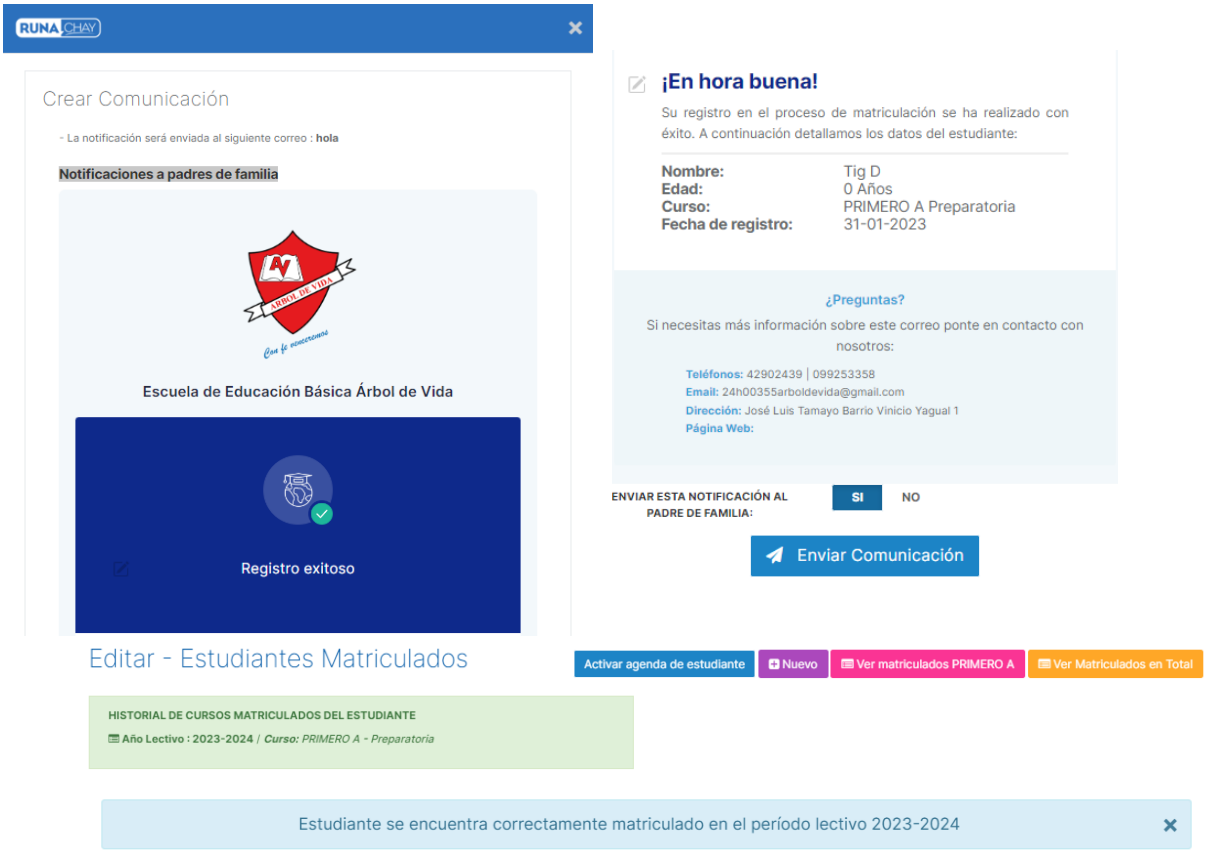


Figura 70: Imágenes de registro exitoso

Se observa que la matrícula fue procesada con datos incorrectos, genera ficha de estudiante.

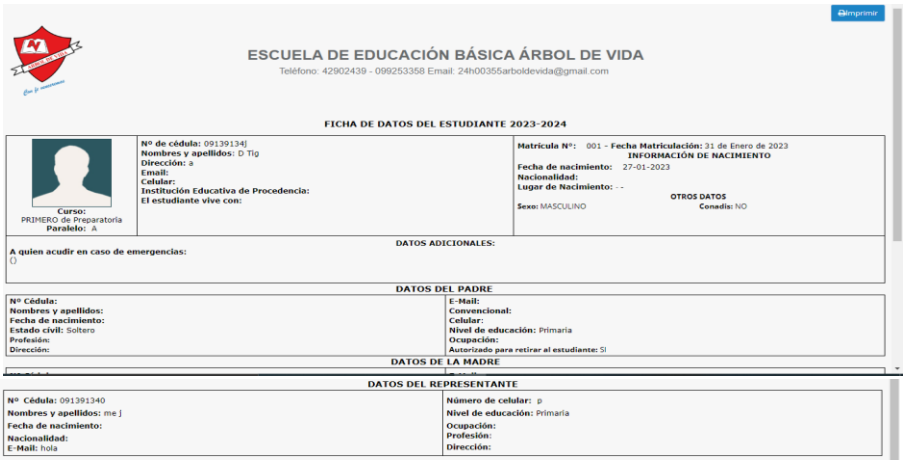


Figura 71: Ficha de estudiante matriculado con datos erróneos

Genera certificado de matrícula.

Figura 72: Certificado de matrícula con datos erróneos

Se dejaron campos obligatorios vacíos y procesar la matrícula, el sistema no dejó seguir con el proceso, mostrando mensajes en los campos requeridos.

Figura 73: Campos requeridos en el ingreso de datos

Prueba 2: Verificar la no duplicación de registros de estudiantes.

Entradas	Salidas esperadas	Salidas obtenidas	Nivel de complejidad
Duplicación de datos (cedula)	Mensaje de estudiante ya matriculado, no permitir matriculación	Se carga la página para editar datos de la matrícula	Bajo

Tabla 34. Verificación de duplicación de registro de estudiantes.

Al ingresar cédula de estudiante matriculado, se cargan automáticamente los datos registrados, por ende, no permite la duplicación de matrícula de estudiante, envía a la edición de datos de estudiante

Figura 74: ingreso de número de cédula

Figura 75: Validación en el campo de cedula

Prueba 3: Verificar el envío de correo de validación en el registro del estudiante

Entradas controladas	**Salidas esperadas**	**Salidas obtenidas**	**Nivel de complejidad**
Ingresar correo sin el formato requerido	Mensaje de error, formato invalido; no permitir guardar datos	Matricula procesada, no muestra mensaje de error, envío de mensaje de matrícula exitosa.	Bajo
Ingreso de correos inexistentes	Mensaje de error: correo inexistente/inválido	Matricula procesada, no muestra mensaje de error, envío de mensaje de matrícula exitosa.	Bajo
Ingreso de correo con formato adecuado	Antes de procesar la matricula, debe enviar un correo de verificación. Posteriormente a la verificación, procesar y enviar el estado de la matricula	No hay verificación del correo electrónico, al procesar la matrícula se envía mensaje de registro exitoso	Bajo

Tabla 35. Validaciones correo electrónico en el registro de estudiantes.

Al ser matriculación, el monitoreo del estado del estudiante lo realizan los padres, en este caso piden como dato obligatorio el ingreso de correo electrónico para enviar comunicaciones de las actividades académicas, el aplicativo permite el ingreso de cualquier dato.

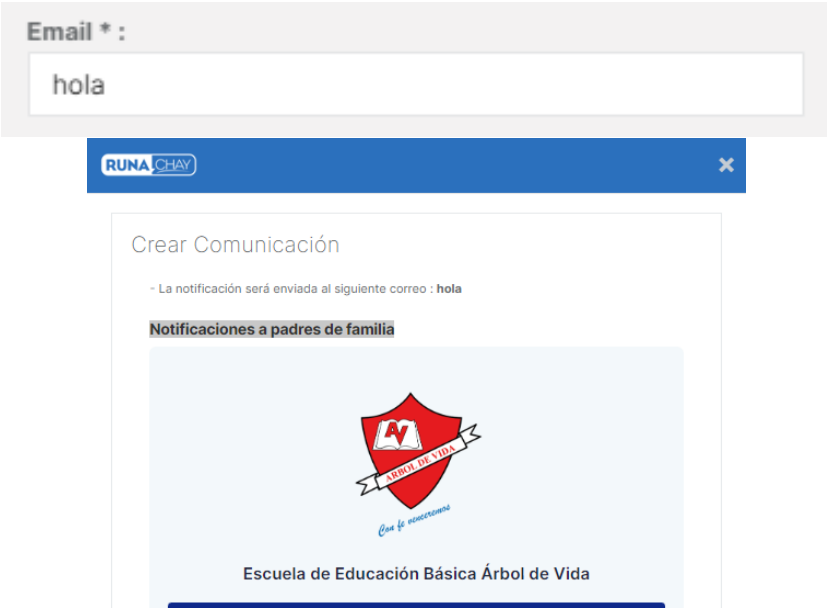


Figura 76: Validación de ingreso de correo electrónico

Se ingresa un correo existente para verificar que envíen el mensaje

Figura 77: ingreso de correo existente

El mensaje llega al correo registrado.

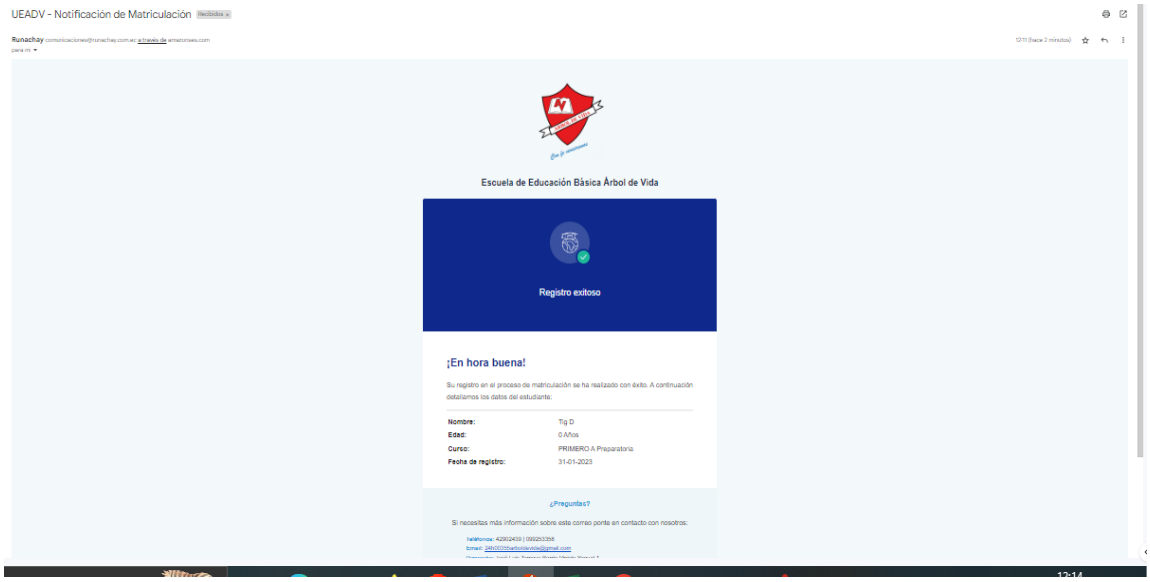


Figura 78: Verificación de recibimiento de correo

Prueba 4: Verificar el proceso de los estados de solicitud de matrícula.

Entradas	Salidas esperadas	Salidas obtenidas	Nivel de complejidad
Selección de estado de solicitud de matrícula(aprobado, aprobado con nivelación y reprobado)	Enviar mensaje al correo del representante del estado de matrícula	Se envía el mensaje al correo del representante	Bajo

Tabla 36. Verificación de los estados de solicitud de matricula

Evidencia

Selección de aprobación de solicitud de cupo

Figura 79: Sección de aprobación de cupo

Al estar haciendo pruebas, la página dejó de responder

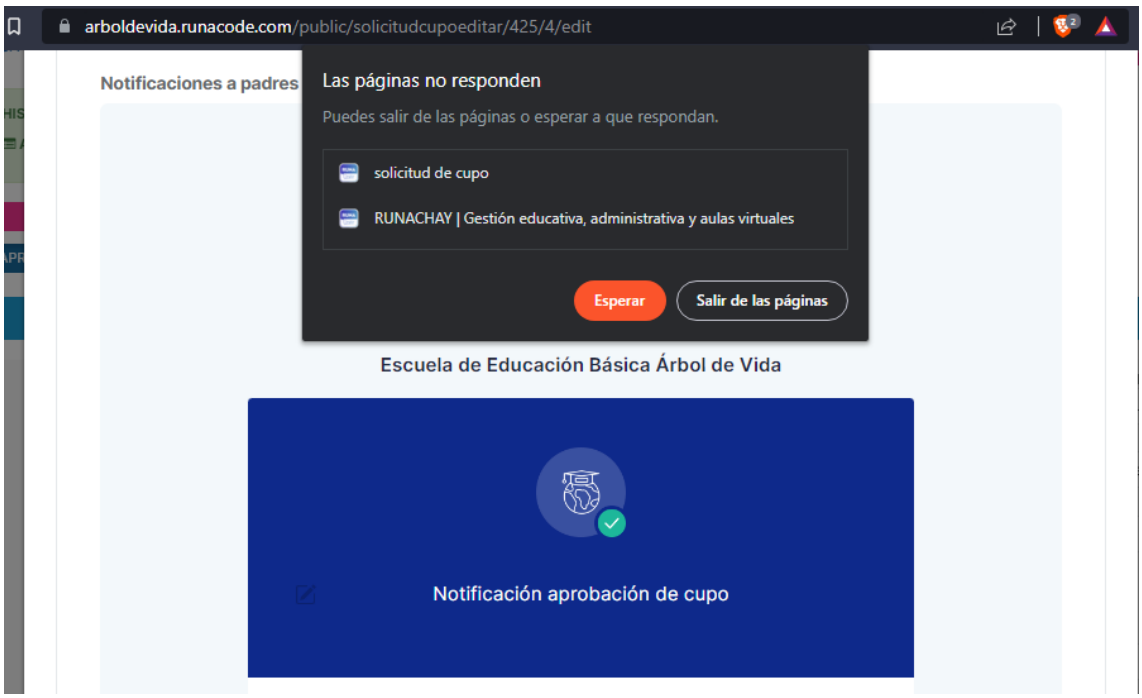


Figura 80: Error al probar el aplicativo

El mensaje llegó correctamente al correo ingresado en la solicitud de cupo

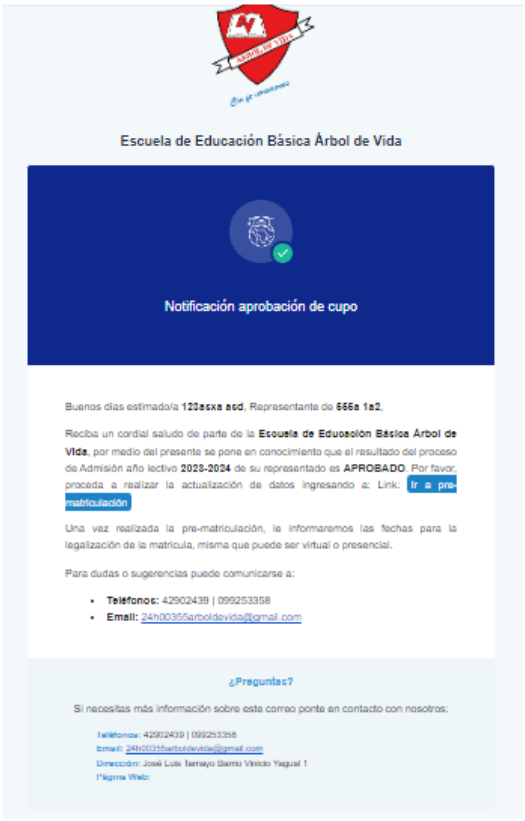


Figura 81: Mensaje de solicitud de cupo

Facilita un link para la pre matriculación, donde pide el ingreso de cedula de representante o representado, al encontrar datos registrados los muestra en la pantalla y tiene habilitado botón para registrarlo en matrícula.

Figura 82: prueba del link de pre matriculación

Se cambia el estado de solicitud de cupo para matricula a reprobado y se verificó que llegue el mensaje al correo

Figura 83: Notificación de Reprobado

Luego de haber cambiado el estado de la solicitud se comprueba que el link de pre-matriculación aún funciona

Figura 84: Interfaz de búsqueda por cedula

Se puede seguir interactuando pero no presenta el botón registrar

Figura 85: Link de pre matriculación no muestra el botón de registrar cuando el estado es reprobado.

Estudiante con estado de solicitud de cupo para matrícula de reprobado

Acciones	Cédula	Nombres	Curso	Teléfono	Correo	Fecha de nacimiento	Nº Matrícula	Fecha de solicitud	Estado solicitud	Estado matrícula	Cédula	Nombres	Correo	Celular
Acciones	a13da	123asxa asd	INICIAL A - Inicial	celular	1234	2030-04-08	2	2026-02-05	REPROBADO		12345	1a2 555a	kenyamejillon18@gmail.com	1

Figura 86: Estado de solicitud de matrícula como reprobado

Permite generar la ficha de matrícula

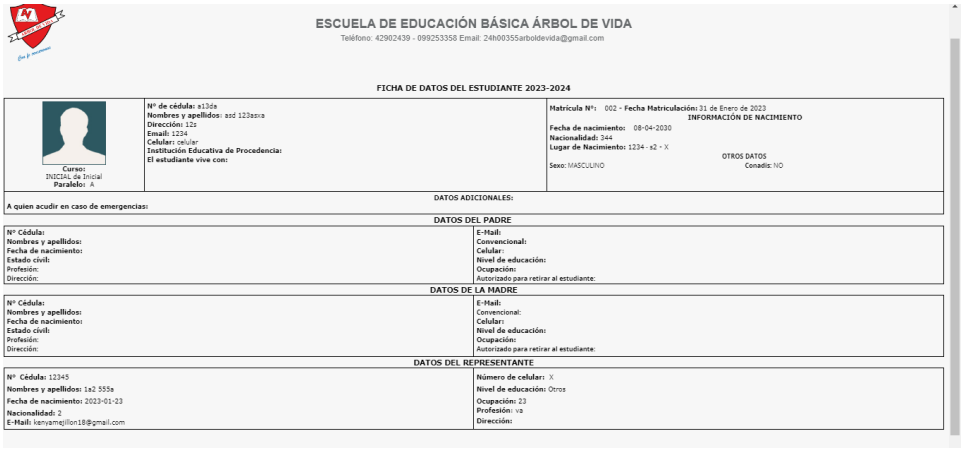


Figura 87: Generación de ficha de matrícula de una solicitud de cupo como reprobado

Permite generar el certificado de matrícula

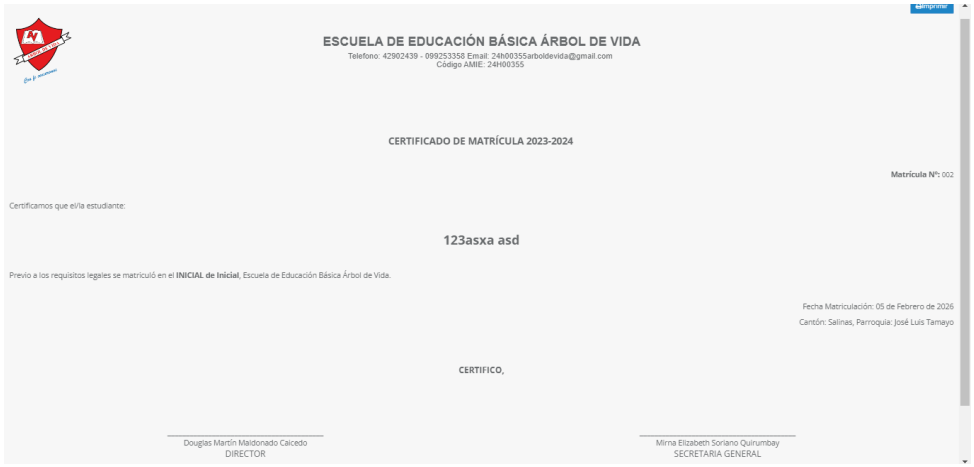


Figura 88: Certificado de matrícula de una solicitud de cupo como reprobado

Anexo 12. Prueba de funcionalidad en módulo Calificaciones

Objetivo: evaluar el funcionamiento del módulo de calificaciones

Descripción del proceso:

1. El docente debe seleccionar el curso donde va a ingresar notas
2. Escoge el parcial/periodo a calificar
3. Se ubica en el insumo/actividad a calificar
4. Ingresa notas

Condiciones en los campos

- Se permite el ingreso de numero positivos
- No debe ser mayor a 10
- No permite el ingreso de caracteres alfabéticos
- Permiten el ingreso del punto (.) en las calificaciones

Escenario de prueba 1: Modificaciones de notas en periodos no vigentes

Entradas	Salidas esperadas	Salidas obtenidas	Nivel de complejidad
Selección de parcial/ periodo a calificar	Si el periodo ya no está vigente, el icono de edición no debe estar habilitado, tampoco se puede añadir nuevas tareas	Las calificaciones no se pueden editar, la opción añadir actividad/insumo sigue activa.	Bajo

Tabla 37. Pruebas de modificación de notas en periodos no vigentes

Evidencias de la prueba

- Se escoge el periodo

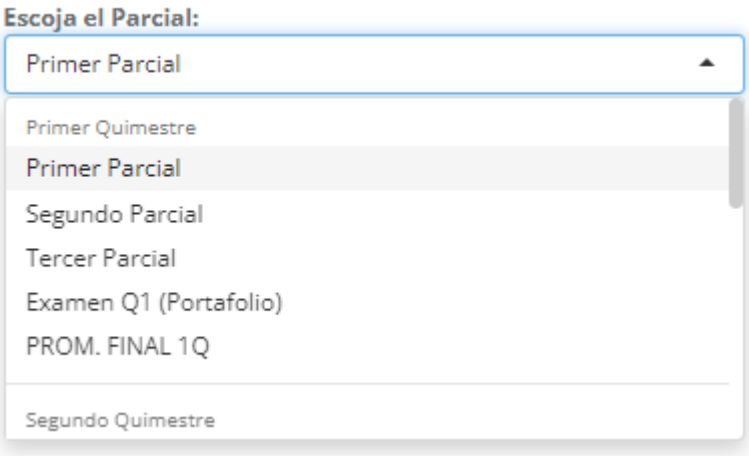


Figura 89: Selección de parciales

- Nos muestra el estado del periodo, si está vigente o finalizado

Figura 90: Estado del periodo académico

- En la parte inferior se encuentra el cuadro de notas, el cual ya no tiene habilitado la opción de edición de notas, debido a que el periodo está finalizado

Figura 91: Cuadro de notas

- Permite observar detalles de las calificaciones y agregar comentarios

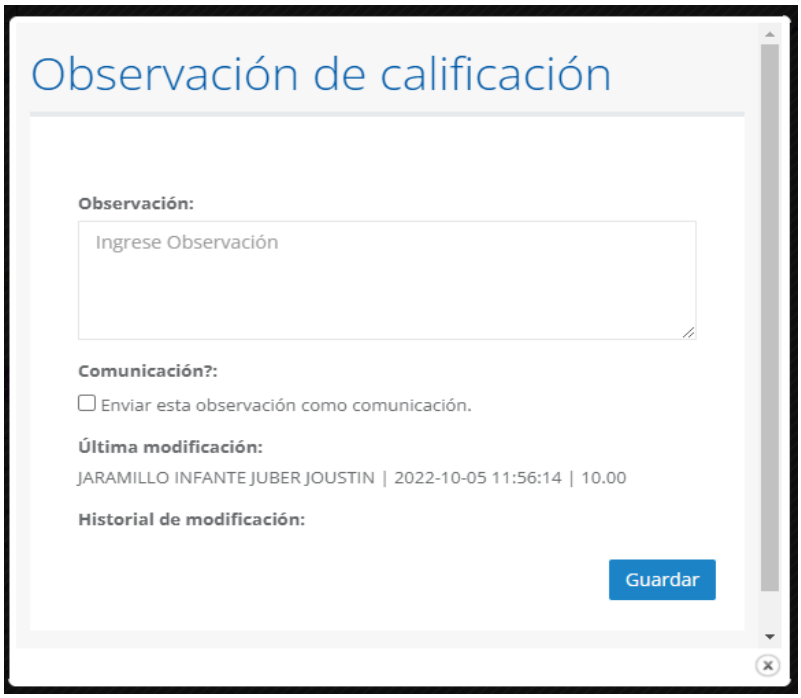


Figura 92: Observación de calificaciones

- El botón agregar insumo, sigue habilitado y permite añadir, pese a que el periodo ya finalizó

Figura 93: Interfaz de agregar insumo

Escenario de prueba 2: Validar el Ingreso correcto de números en el campo de notas.

Entradas	**Salidas esperadas**	**Salidas obtenidas**	**Nivel de complejidad**
Números mayores a 10	Mensaje de error, no permitir ingresar el valor	Muestra mensaje de error que no permite el ingreso mayor al número 10, queda 0 por defecto.	Bajo
0 =< Numero >=10	Permite el ingreso de nota	Ingreso de nota exitoso	Bajo

Tabla 38. Prueba de validación de ingreso de ingreso correcto de números en el campo de notas

Evidencias del proceso

- Se procede a intentar ingresar un número mayor a 10 en el casillero de un alumno

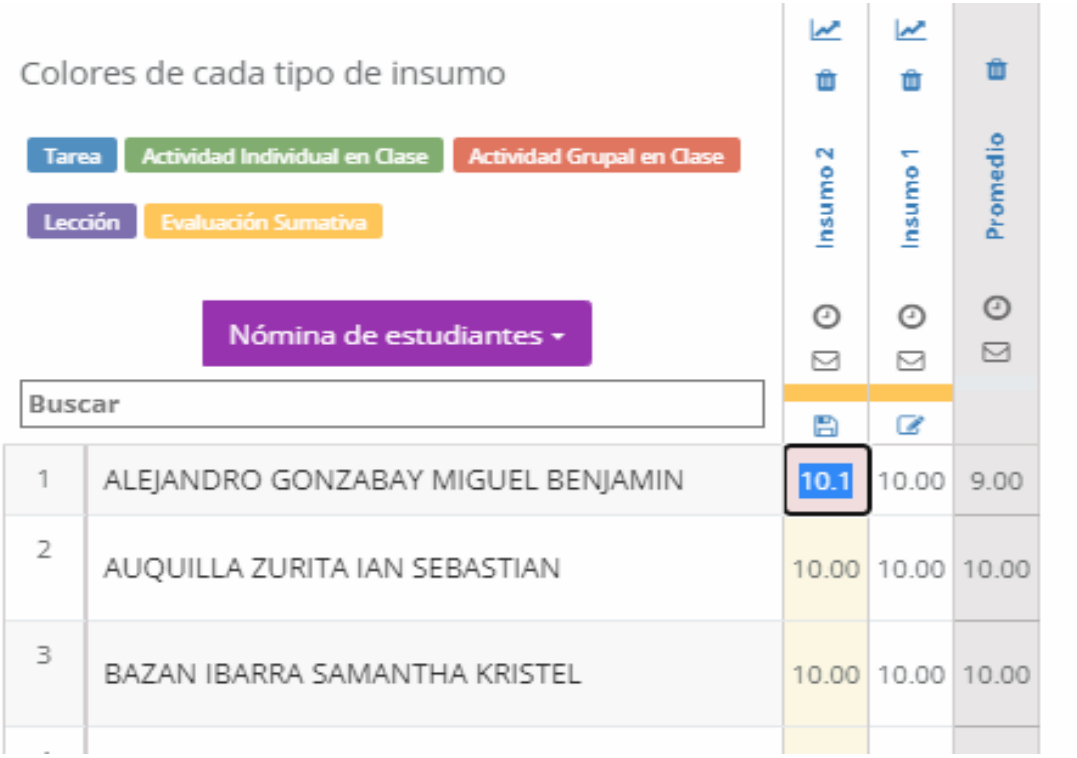


Figura 94: Ingreso de nota incorrecta en el cuadro de notas

- Se observa que inmediatamente aparece un mensaje flotante, donde se informa al docente que la calificación no debe ser mayor a 10.

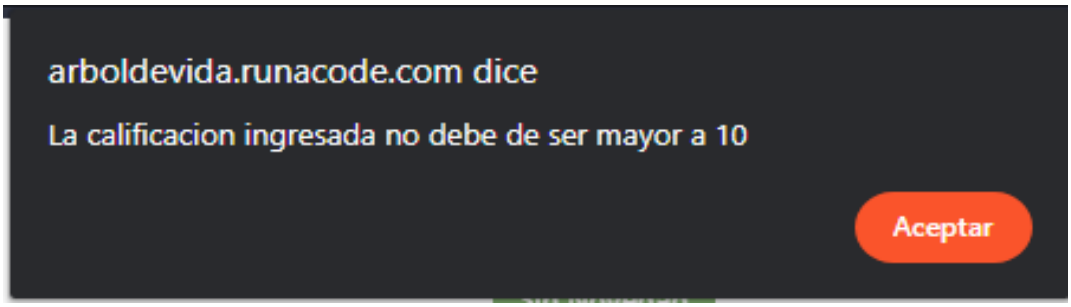


Figura 95: Alerta de error al ingresar notas

Escenario de prueba 3: Validaciones del tipo de dato numérico (positivos) en el campo de notas.

Entradas	Salidas esperadas	Salidas obtenidas	Nivel de complejidad
Ingreso de caracteres alfabéticos	No permitir el ingreso de caracteres	No mostrar nada en el campo mientras se presiona caracteres alfabéticos	Bajo
Ingreso de numero negativos	Bloquear el ingreso del signo negativo (-)	Bloqueo del sigo negativo (-)	Bajo
Ingreso del signo de puntuación (,)	No permitir el ingreso de la coma (,)	Bloqueo del signo de puntuación: la coma(,)	Bajo

Tabla 39. Prueba de validación de datos numéricos (positivos)

Nota: Sin evidencias, debido a que funcionó correctamente en este escenario de prueba.

Anexo 13. Prueba de funcionalidad en inicio de sesión

Descripción: en la página de inicio de sesión, hay dos campos de texto para usuario (número de cédula) y la contraseña, un botón de acceder y las opciones ¿Olvidó su contraseña? Y ¿No puedes acceder? El inicio de sesión exitoso lleva al usuario a la página de inicio del aplicativo de la unidad educativa.

Proceso

1. El usuario escribe su nombre y el password (Autenticación)
2. El sistema comprueba que existe una cuenta con ese nombre y password y, si los datos son correctos, se da permiso para entrar en el sistema.
3. Si existe el nombre de usuario pero el password es incorrecto, no permite el ingreso

Requisitos no funcionales del inicio de sesión.

- El password no debe ser visible

- Los nombres de usuarios es el número de cédula, por ende no se aceptan valores mayores/menores al rango de 10 dígitos.

Id. Caso	Entradas controladas		Salidas esperadas	Salidas obtenidas	Nivel de complejidad
	Usuario(cédula)	Contraseña			
1	chvjbjk	*******	Acceso denegado y mensaje, permitir solo el ingreso de numero en usuario	Datos incorrectos	Bajo
2		*******	Mensaje en el campo cédula(campo requerido) Ingrese datos	Ingrese usuario y contraseña por favor	
3	0913916340	*******	Acceso denegado, ingrese valores válidos	Datos incorrectos	
4	0913913406	*******	Acceso denegado, usuario no registrado	Tus datos son incorrectos	
5	0923311518	*******	Mensaje de acceso exitoso	Ingreso a la página	

Tabla 40. Escenario de prueba: Inicio de sesión validando campos requeridos.

Evidencias

- Ingreso de datos del id 1 de la tabla anterior, caracteres.

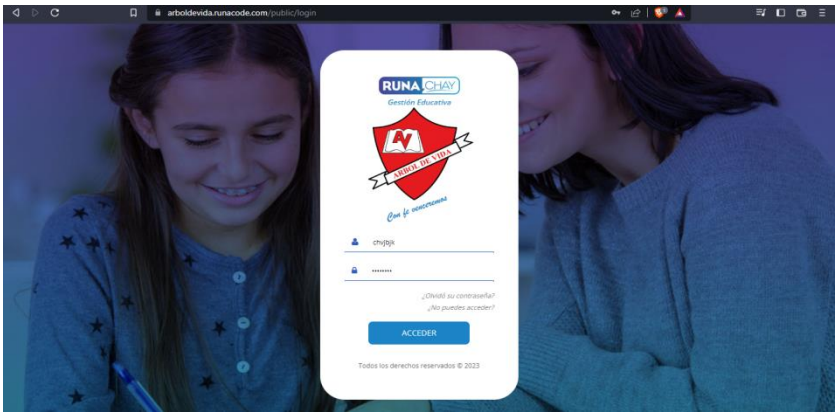


Figura 96: Inicio de sesión con datos incorrectos

- No permite el acceso, datos inválidos

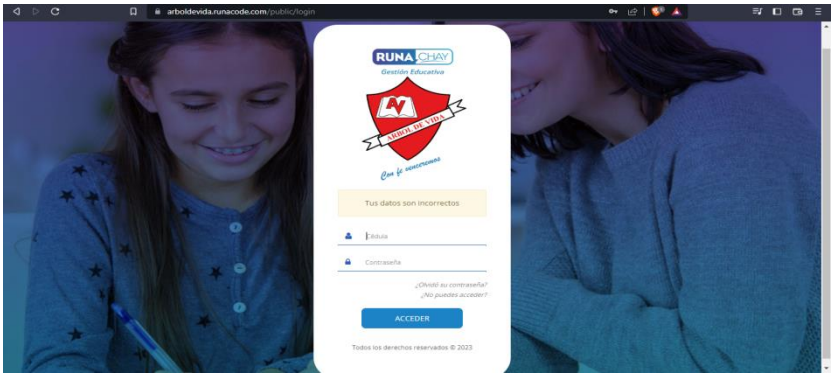


Figura 97: Inicio de sesión sin datos

- Ingreso de datos del id 2 de la tabla anterior, campo de cédula vacío.

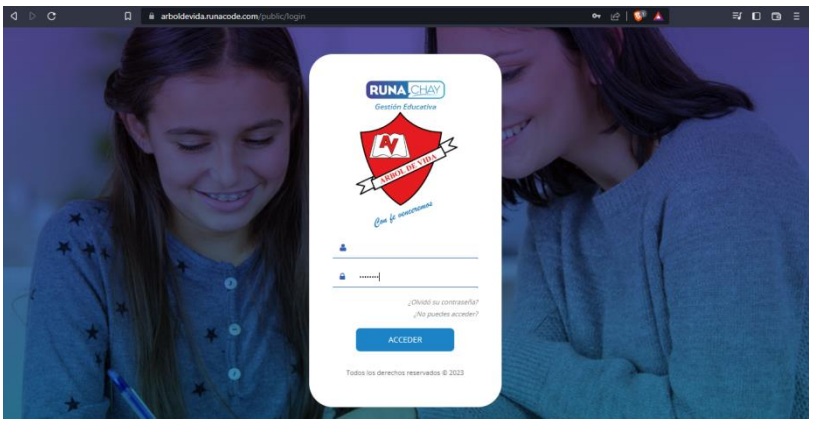


Figura 98: inicio de sesión solo con contraseña

- A pesar de dejar en blanco el campo cedula, el botón está habilitado

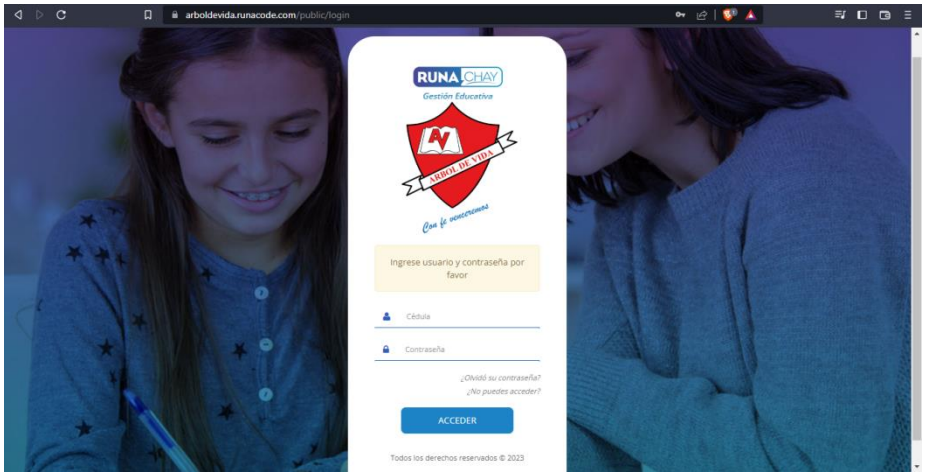


Figura 99: Validación del botón de ACCEDER

- Ingreso de datos del id 3 de la tabla anterior, número con 9 dígitos

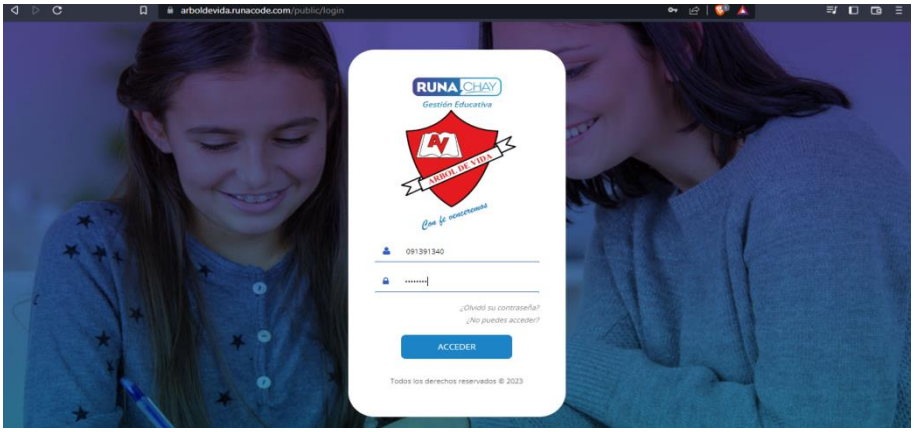


Figura 100: Inicio de sesión con cédula de 9 dígitos

- Permite el ingreso de números menos a 10 dígitos, no muestra mensaje

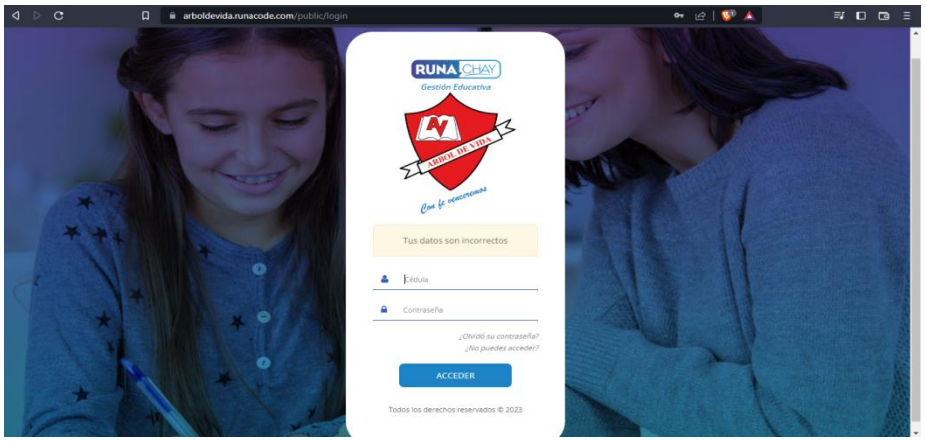


Figura 101: Inicio de sesión no muestra los mensajes correctos

- Ingreso de datos del id 4 de la tabla anterior.

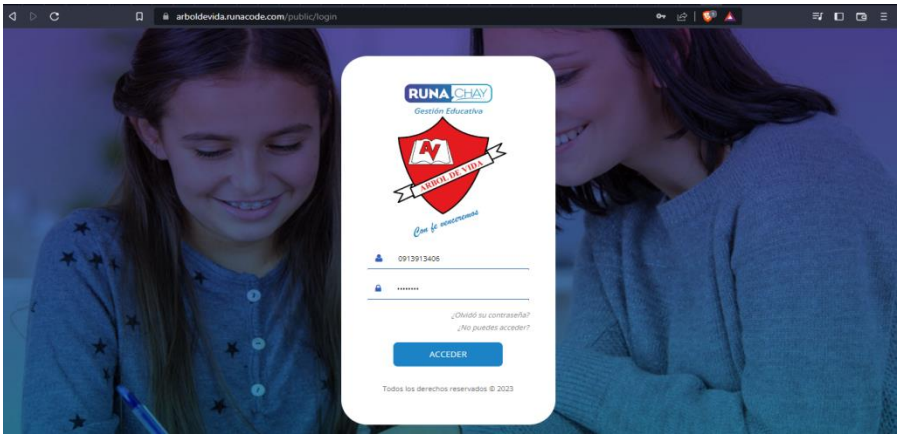


Figura 102: Ingreso de usuario no registrado

- Ingreso de un numero de cedula correcto pero no registrado, no emite mensaje de usuario no registrado.

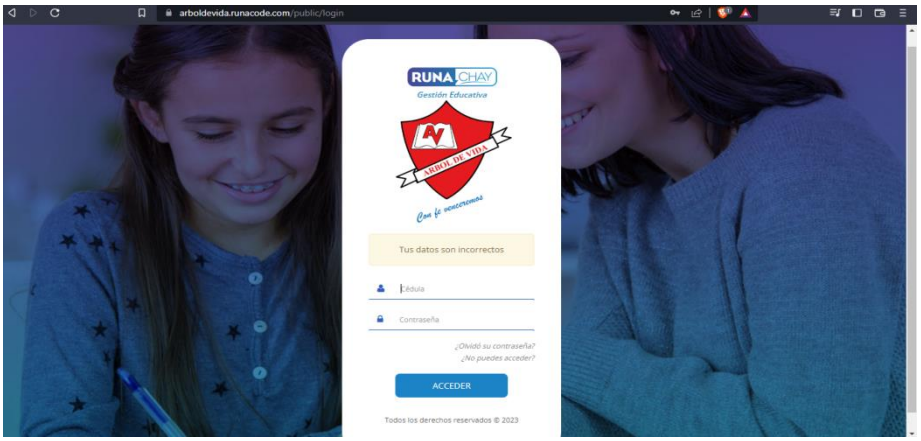


Figura 103: No muestra mensaje de usuario no registrado

- Ingreso de datos del id 5 de la tabla anterior, datos registrados

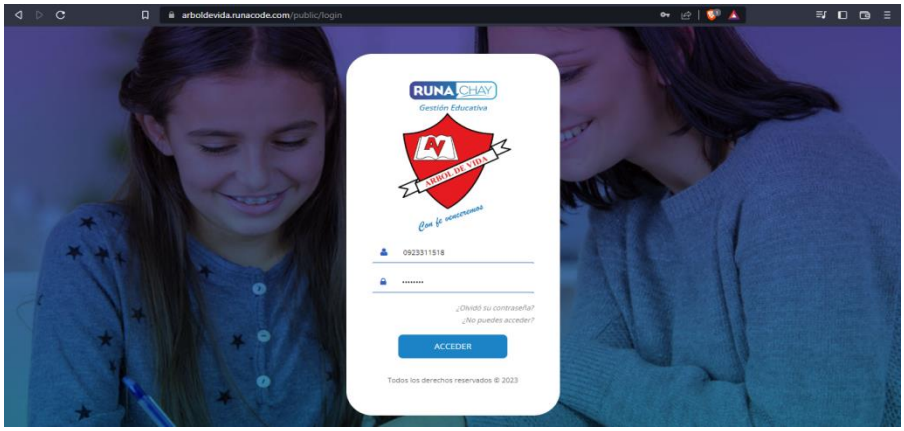


Figura 104: inicio de sesión valido

- Permite el ingreso a la página principal del aplicativo

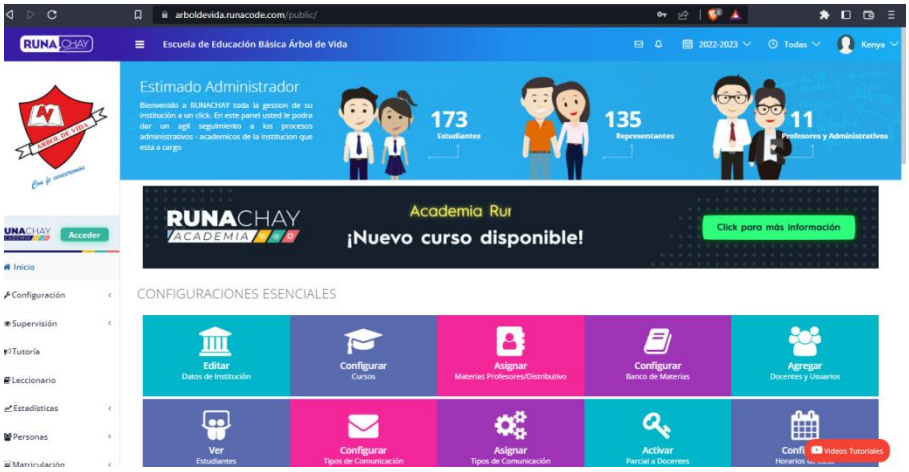


Figura 105: Acceso al aplicativo

Prueba 2: Verificar que la funcionalidad de cambio/recuperación de contraseña solicite la contraseña anterior, la nueva contraseña y una confirmación de la contraseña.

Entradas controladas	Salida esperada	Salida obtenida	Nivel de complejidad
Se ingresa cédula registrada	Proceso de restablecimiento de contraseña por correo electrónico	Muestra un mensaje que se envió un mensaje al correo electrónico para reestablecer la contraseña	Bajo

Tabla 41. Entradas y salidas del módulo de inicio de sesión

Proceso:

Se ingresa la cédula que se encuentra registrada

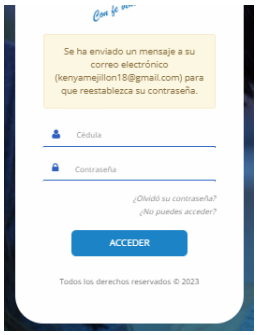


Figura 106: Solicitud de cambio de contraseña

Se verifica que haya llegado mensaje para restauración de contraseña en el correo electrónico registrado, mientras no se cumplan con los requisitos de la creación, ni coincida la nueva contraseña no se pueden guardar los cambios

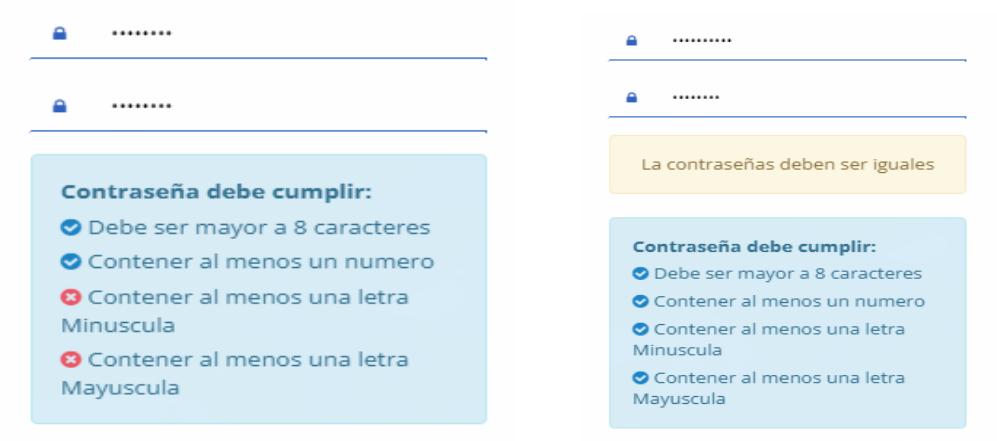


Figura 107: Interfaz de Cambio de contraseña

Se habilita el botón recuperar y se guardan los cambios

Figura 108: Recuperar contraseña

Anexo 14. Inserción de script malicioso en modulo matriculación - Xss Almacenado

En el aplicativo web, conectado por un perfil administrador, identificamos formulario de entrada del usuario que se almacena en el sistema para probar la inserción de script malicioso. La primera sección es un formulario para ingresar datos principales del estudiante.

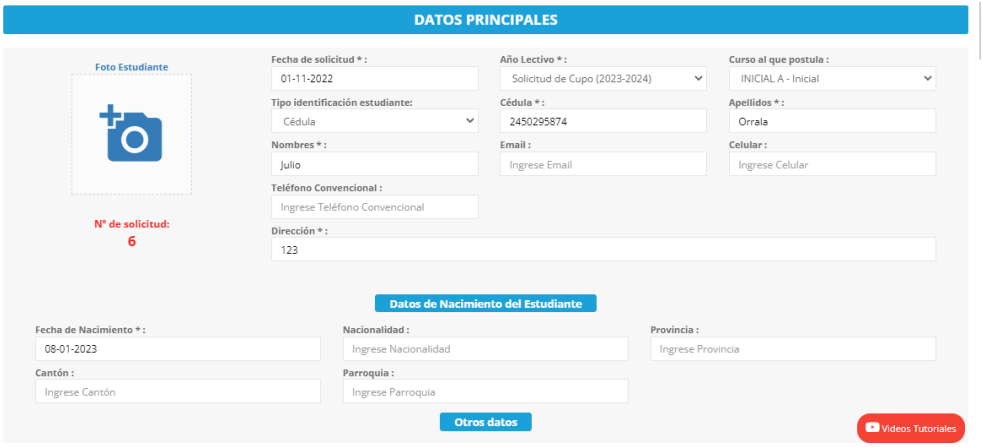


Figura 109: Interfaz de datos principales para registro de usuario

Se insertará script malicioso en todos los cuadros de texto <script>alert(‘XSS’)</script>

Figura 110: Inserción de código XSS en el campo Cédula

En el campo cédula no permite insertar el script, por ende que no se ejecute la alerta

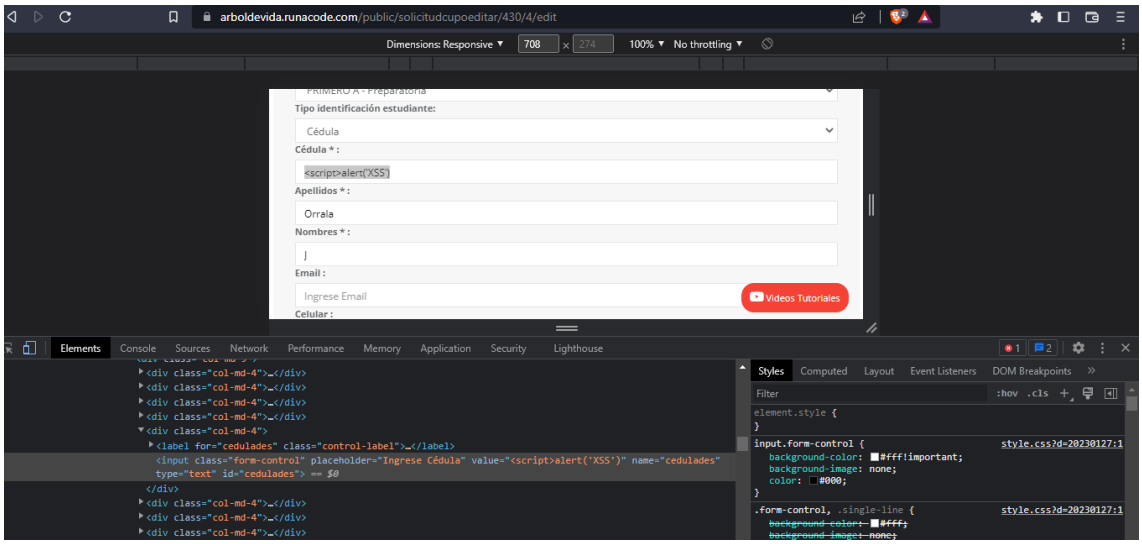


Figura 111: Respuesta de la página ante el código XSS en el campo cédula

En el campo apellido si permite la inserción del script malicioso

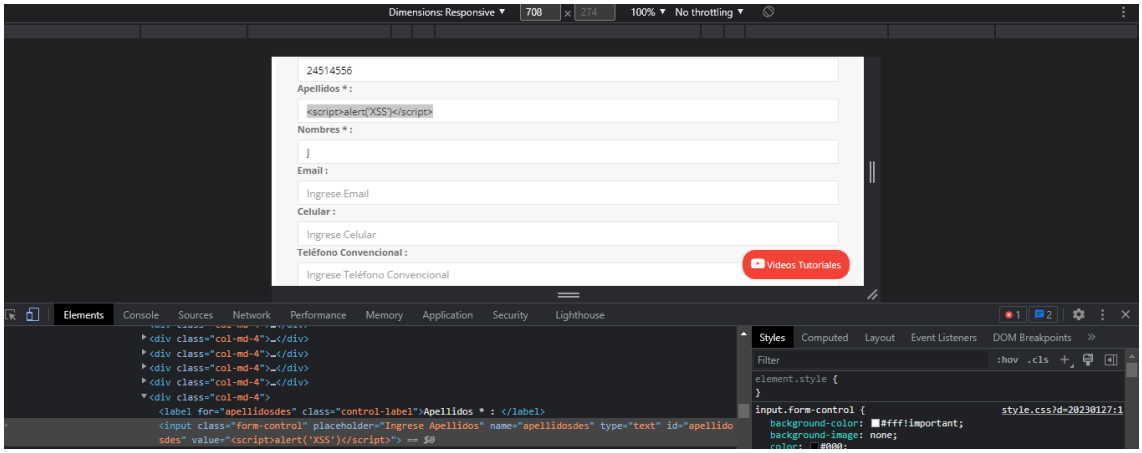


Figura 112: Inserción de script en el campo apellido

El script se ejecuta y aparece la alerta en la pantalla de la página

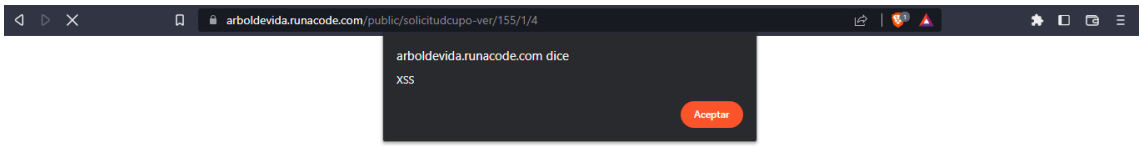


Figura 113: Resultado del Script insertado

Se realiza el mismo procedimiento en todos los campos, obteniendo como resultado que si permite insertar el script y no usa filtrado.

Se procede a editar el campo email, añadiendo el script y observar cómo actúa el sistema

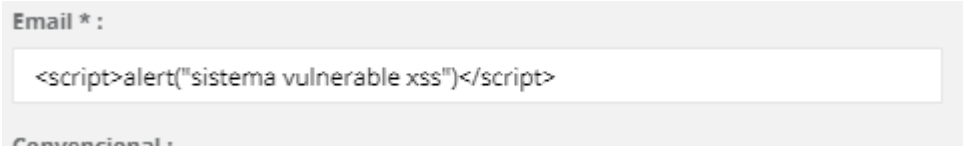


Figura 114: Script insertado en el campo Email

Se inspecciona el código para verificar si permite el ingreso del script o usa filtrado de datos.

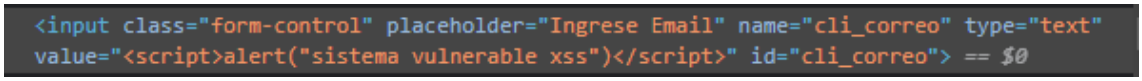


Figura 115: Verificación del Script insertado en el campo Email

Se vuelve a cargar la página y efectivamente en el campo de ingreso de email se puede realizar la inserción de script malicioso, se carga la alerta en el aplicativo web.

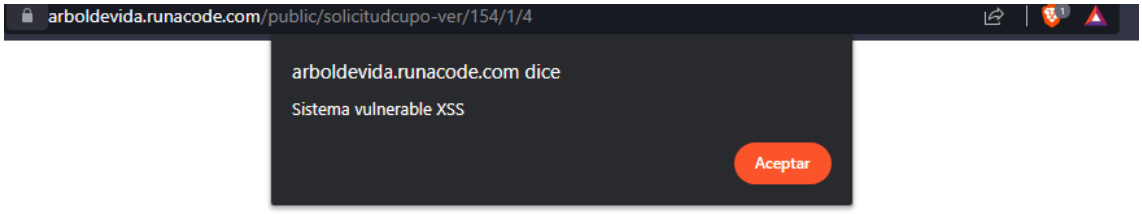


Figura 116: Resultado del Script insertado en el campo Email

Se empieza a evaluar los campos de la sección de ingreso de datos del representante, ingresando el <script>alert(“Hola has sido hackeado”)</script>

Figura 117: Evaluación de los campos de los datos del representante

Regresamos a la sección donde listan los estudiantes que están en el proceso de admisión

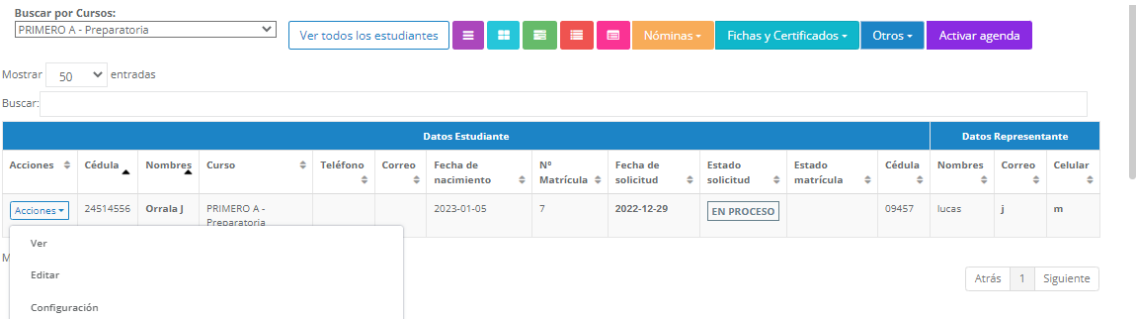


Figura 118: Interfaz de listado de estudiantes

Al presionar la opción ver datos del estudiante, se ejecuta la alerta en el sistema

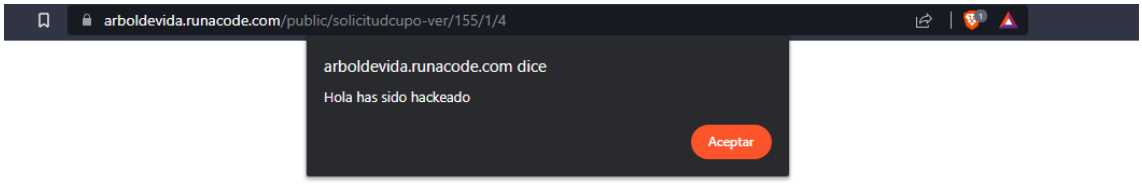


Figura 119: Resultado de las pruebas en la interfaz de matriculación – datos representante

Finalmente evaluamos la sección de datos facturación que está relacionado con los datos ingresados del representante y se obtiene el mismo resultado. Script insertado **<script>alert("Hola soy Kenya")</script>.**

Figura 120: Ingreso de script en el campo nombres de sección datos facturación

Se guardan los datos y se envía solicitud de visualizar datos del estudiante.

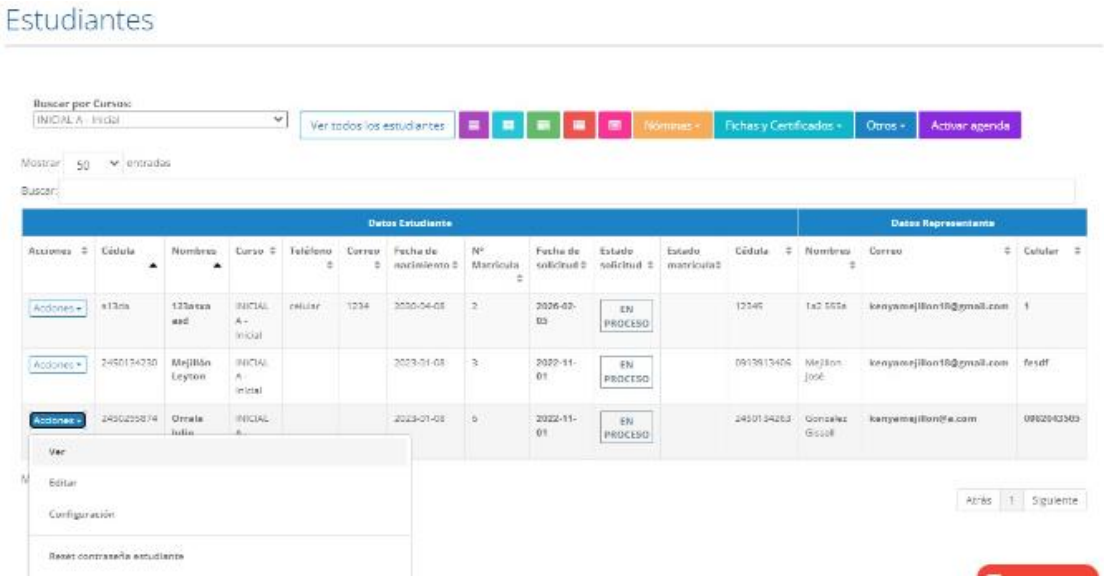


Figura 121: Solicitud de visualizar datos del estudiante

Nos aparece la alerta

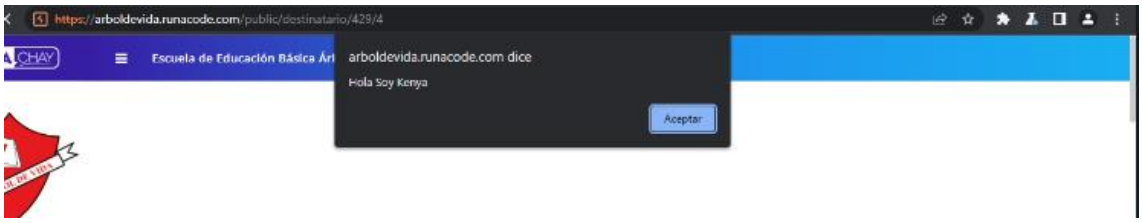


Figura 122: Resultado del Script insertado en el campo nombre

También se evaluó el formulario insertando un script diferente, usando el String. fromCharCode() que es un método estático que devuelve una cadena creada mediante el uso de una secuencia de valores Unicode especificada, que es el siguiente:

<script>alert(String.fromCharCode(88,83,83))</script>. El sistema debe mostrar la alerta con mensaje: **XSS**

Figura 123: Código XSS para cadena de caracteres

Se carga datos de estudiantes y muestra la alerta con el mensaje esperado.

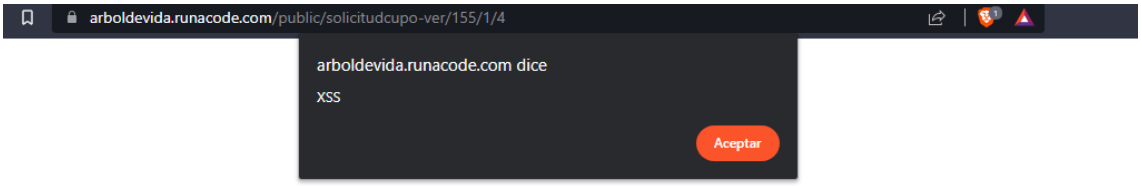


Figura 124: Resultado del Script

Finalmente se hizo la prueba con un script intentando capturar cookies para ello utilizamos el siguiente: <script>alert(document.cookie); </script>

Figura 125: Script para capturar cookies

Se guardan los datos y se solicita visualizar datos del estudiante. La prueba fue exitosa.

Figura 126: resultado de la captura de cookies

Anexo 15. Prueba de inyección SQL

Objetivo: Evaluar respuesta de la base de datos ante la inyección SQL.

Proceso

- Se identifica las entradas de datos que se envían a la base de datos, como formularios web o parámetros en la URL.

- Se prueba cada entrada para ver si es posible inyectar comandos SQL, ingresando caracteres especiales o secuencias de comandos SQL maliciosos en los campos de entrada.
- Se analiza los resultados de las pruebas de entrada para determinar si se produjo una respuesta anormal o inesperada, lo que indica una posible vulnerabilidad a la inyección SQL.

Pasos

Una forma de probar si un sitio está ejecutando comandos es enviar una comilla simple, es decir: ‘al final del dato ingresado.

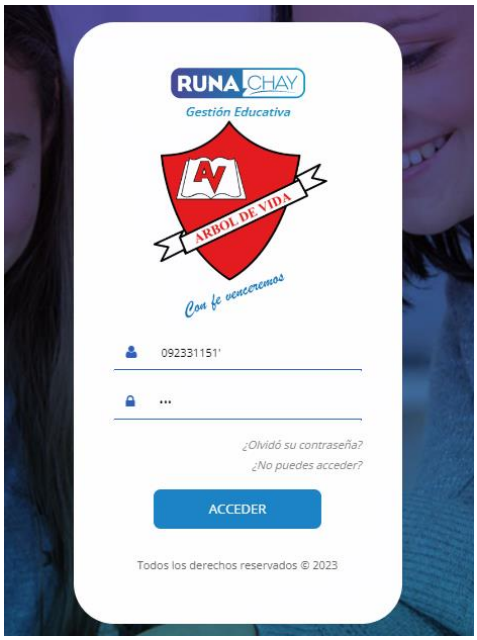


Figura 127: Envío de comilla simple en formulario de inicio de sesión

Al hacer esto, la página dará un error si es vulnerable a inyección SQL, por lo general aparece un mensaje de Database error o Internal Error, donde sería posible manipular su base de datos. En este caso, la página mostró que los datos son incorrectos.

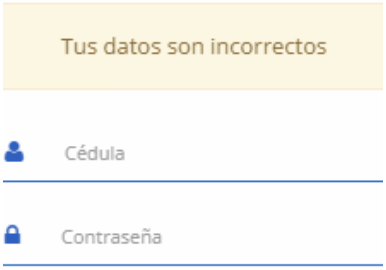


Figura 128: Respuesta de la aplicación ante el envío de comilla simple

También se puede verificar posibles ataques desde el enlace del sitio web. Al interactuar con funciones del aplicativo, se obtuvo un enlace que contiene un parámetro https://arboldevida.runacode.com/public/personas?filtro=1

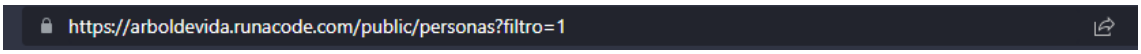


Figura 129: Url que contiene parámetro para prueba de inyección sql

En este caso, 'filtro'es un parámetro y '1' es su valor. Si en el enlace proporcionado se ingresa un 'signo en lugar de 1, verificaríamos la posible inyección.

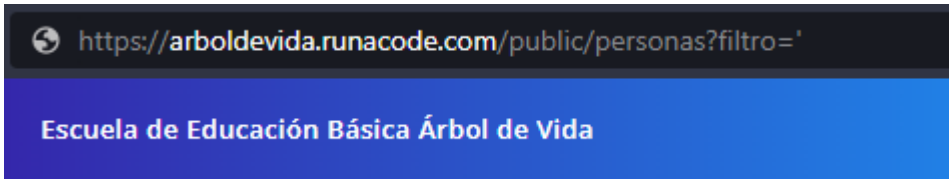


Figura 130: Ingreso de comilla simple en la url que contiene parámetro

No se obtuvo ningún error inesperado, pero se observó que hay codificación de caracteres especiales

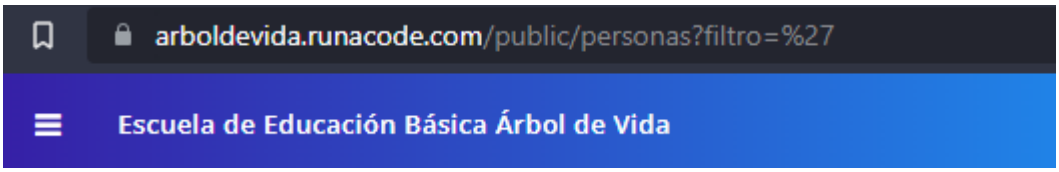


Figura 131: Existencia de codificación de caracteres especiales

También se hizo la prueba enviando un código como 'or 1 = 1; --' en la url.

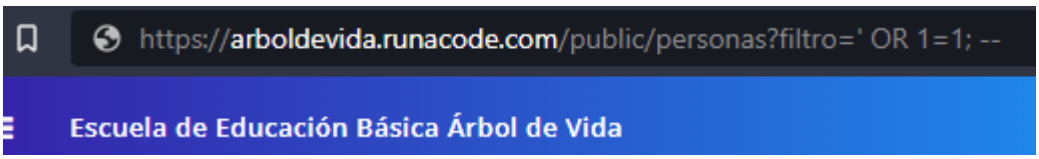


Figura 132: Envío de código sql en la url que contiene parámetro

Nuevamente se observó que hay codificación de caracteres especiales al enviar la Url

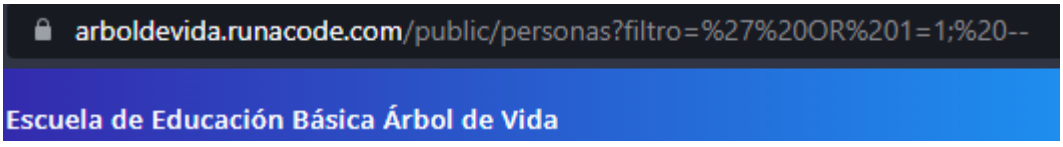


Figura 133: codificación de caracteres especiales

Otra forma de verificar si existe vulnerabilidad de inyección sql es ejecutando herramientas o escáneres enfocadas en vulnerabilidades, para ello ejecutamos la

herramienta sqlmap previamente instalada, con el siguiente comando python sqlmap.py -u [URL].

Figura 134: Ejecución de herramienta sqlmap

Empieza la búsqueda de vulnerabilidades con la url ingresada que enviaba un parámetro.

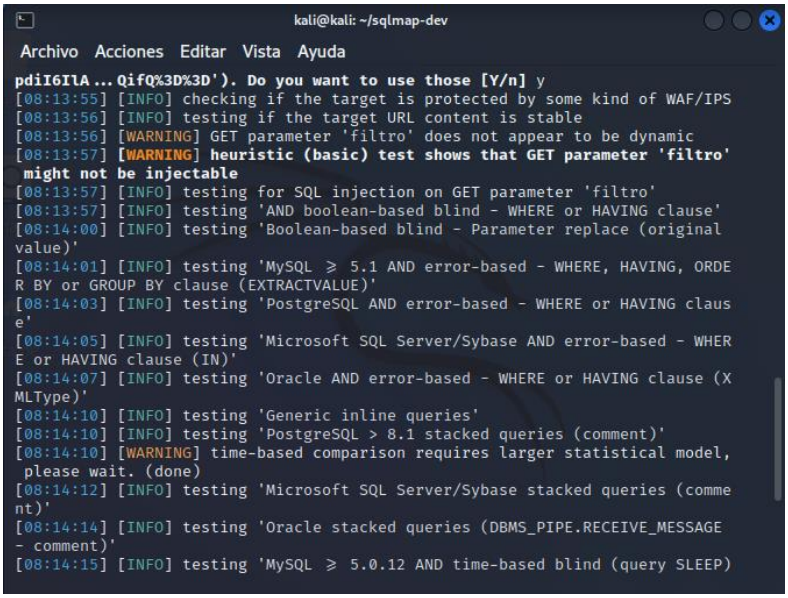


Figura 134: Búsqueda de vulnerabilidades sqli en el aplicativo con sqlmap

No se obtuvo información de la base de datos y un mensaje que el parámetro de la URL no es inyectable, también se detectó un retraso considerable en la respuesta de conexión.

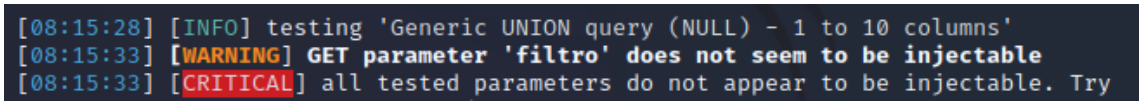


Figura 135: URL ingresada en el escaneo no es inyectable

Se usó una herramienta de escaneo de vulnerabilidades online - SQL Injection Scanner, donde nuevamente no se obtuvo alguna alerta. Al inicio de la ejecución del trabajo se realizaron escaneo y no mostró vulnerabilidad de SQLI.

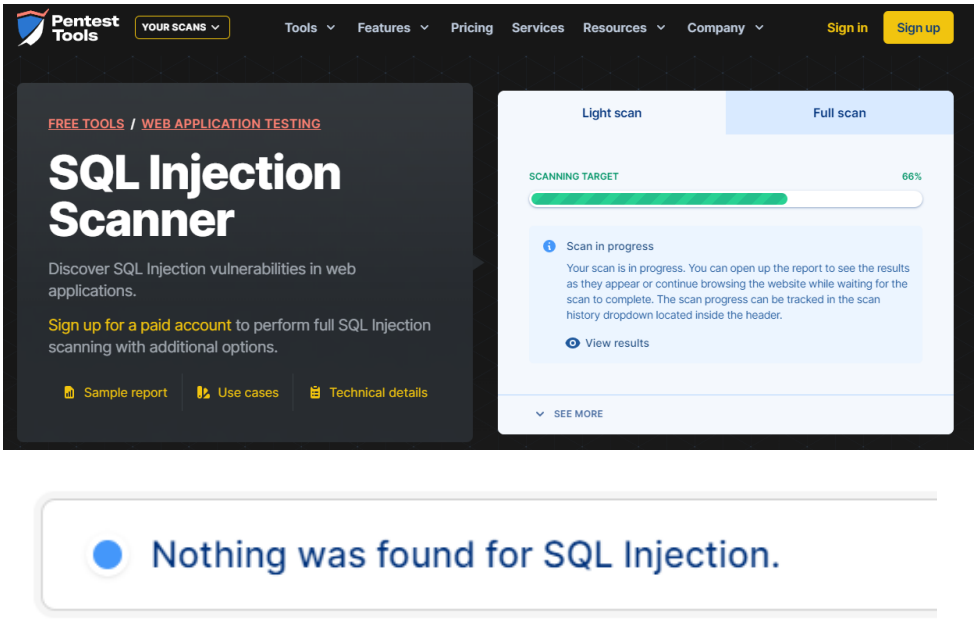


Figura 136: Escaneo de vulnerabilidades sqli online

Anexo 16. Denegación de servicio

Objetivo: Comprobar la disponibilidad del aplicativo web mediante pruebas de stress. Descripción: preparar la herramienta que se usará para el envío de múltiples solicitudes al aplicativo, ejecutar el ataque de denegación de servicios (Ddos) cambiando el número de solicitudes, evidenciar tiempos de respuestas.

Tiempo mínimo	Tiempo máximo	Tiempo medio
5ms	10ms	6ms

Tabla 42. Tiempo de respuesta antes de la prueba

Número de solicitudes	Tiempo mínimo	Tiempo máximo	Media de tiempo	% paquetes perdidos	Complejidad
150	4ms	153 ms	9ms	0	Media
500	4ms	132ms	12ms	1	
3000	4ms	558ms	11ms	10	

Tabla 43. Comparativa de tiempos de respuestas durante el ataque.

Al aumentar la cantidad de solicitudes enviadas, se evidencia que aumenta el tiempo máximo de respuesta y la perdida de paquetes, sin embargo la estabilidad y disponibilidad de los servicios del aplicativo continuaron con normalidad.

Proceso:

1. Abrir terminal en nuestra maquina kali Linux, se crea un directorio Escritorio con el nombre slowloris, con el comando mkdir slowloris.

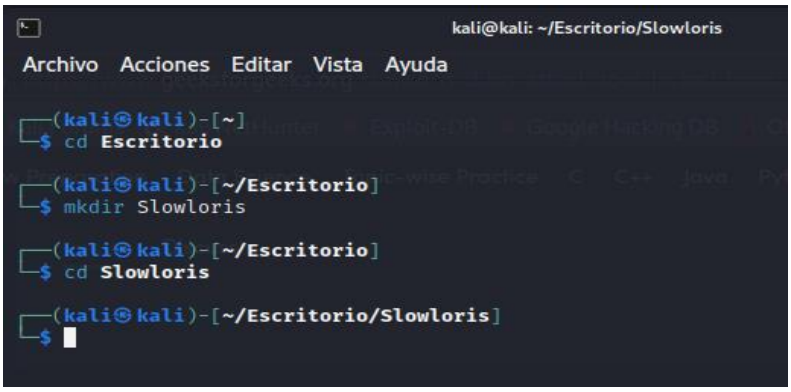


Figura 137: Creación de carpeta de instalación de la herramienta SlowIoris

2. Se debe hacer la clonación de la herramienta slowloris disponible en github con el siguiente comando: git clone

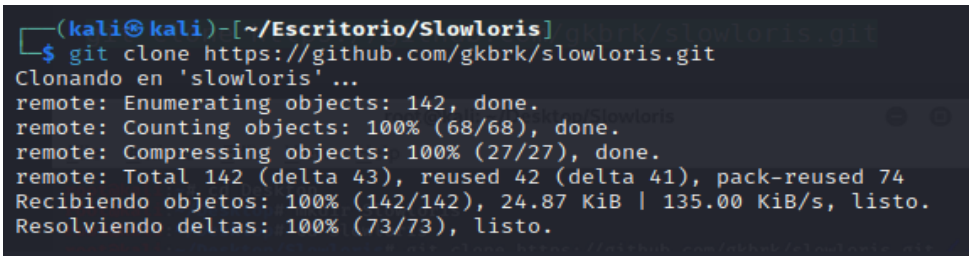


Figura 138: Clonación de la herramienta en el repositorio de GitHub en kali linux

3. Una vez instalada la herramienta, revisamos los archivos que contiene

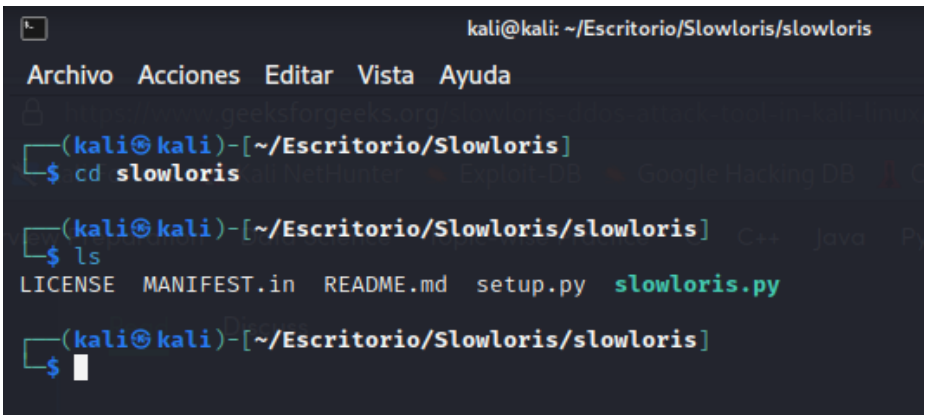


Figura 139: Herramienta instalada exitosamente

4. Antes de iniciar con el ataque de Ddos, se realiza ping a la url de la página para ver los tiempos de respuesta.

```
C:\Users\Kenya Mejillón>ping arboldevida.runacode.com

Haciendo ping a arboldevida.runacode.com [172.66.43.64] con 32 bytes de datos:
Respuesta desde 172.66.43.64: bytes=32 tiempo=6ms TTL=54
Respuesta desde 172.66.43.64: bytes=32 tiempo=6ms TTL=54
Respuesta desde 172.66.43.64: bytes=32 tiempo=5ms TTL=54
Respuesta desde 172.66.43.64: bytes=32 tiempo=10ms TTL=54

Estadísticas de ping para 172.66.43.64:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 5ms, Máximo = 10ms, Media = 6ms
```

Figura 140: tiempos de respuesta de la página antes del ataque DDOS

5. Se ejecuta el archivo slowloris.py se especifica nuestro objetivo y el número de solicitudes, se empiezan a crear y enviar las 150 solicitudes.

```
┌──(root㉿kali)-[/home/kali/Escritorio/Slowloris/slowloris]
└─# python3 slowloris.py 172.66.43.64 -s 150
[27-01-2023 12:07:23] Attacking 172.66.43.64 with 150 sockets.
[27-01-2023 12:07:23] Creating sockets...
[27-01-2023 12:07:24] Sending keep-alive headers...
[27-01-2023 12:07:24] Socket count: 150
[27-01-2023 12:07:39] Sending keep-alive headers...
[27-01-2023 12:07:39] Socket count: 150
[27-01-2023 12:07:39] Creating 150 new sockets...
```

Figura 141: ataque DDOS con 150 solicitudes

Se vuelve a realizar ping hacia el aplicativo, durante el ataque.

```
Estadísticas de ping para 172.66.43.64:
    Paquetes: enviados = 186, recibidos = 186, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 4ms, Máximo = 153ms, Media = 9ms
```

Figura 142: tiempo de respuesta durante el ataque DDOS

Ahora ejecutamos otra vez slowloris.py pero aumentando el número de solicitudes, 500 solicitudes.

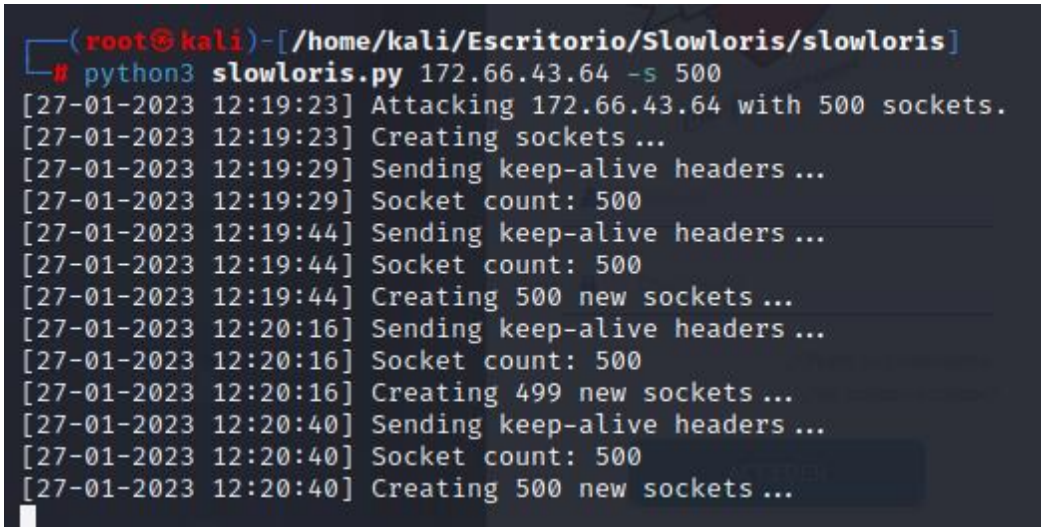


Figura 143: segundo ataque DDOS con 500 solicitudes

Se realiza ping durante el ataque

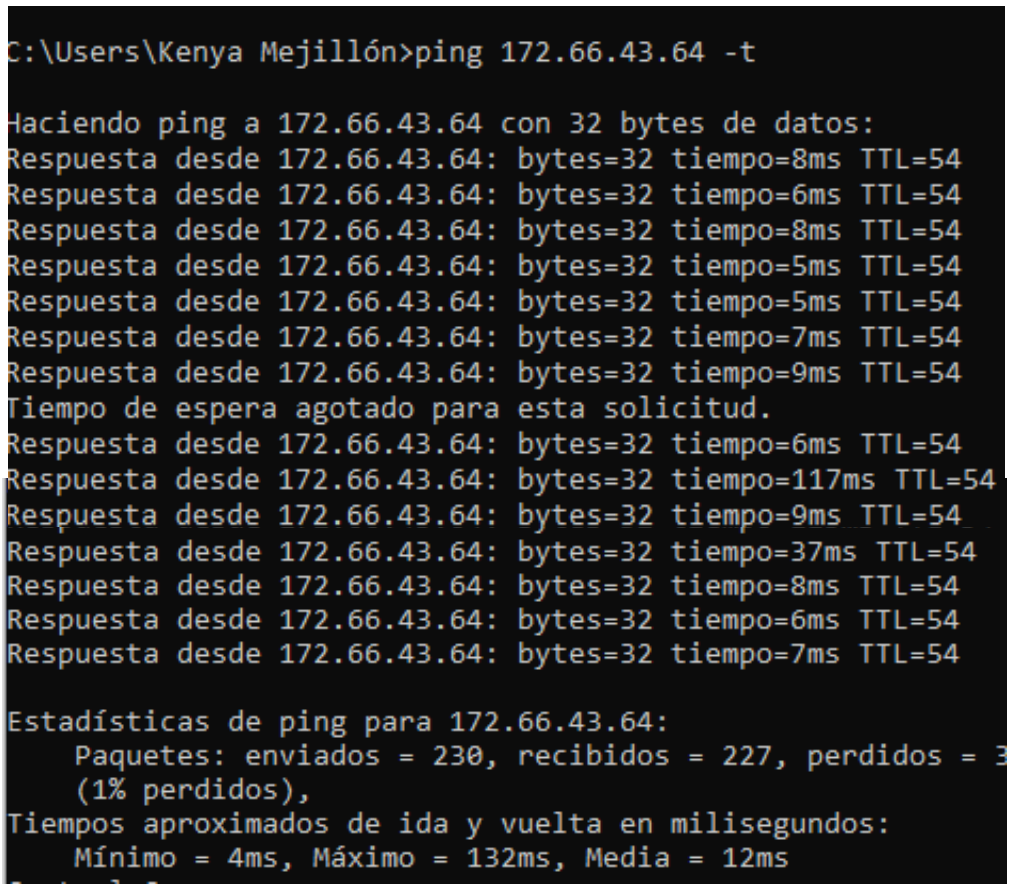


Figura 144: tiempo de respuesta durante el segundo ataque

Ping luego del ataque

```
C:\Users\Kenya Mejillón>ping 172.66.43.64

Haciendo ping a 172.66.43.64 con 32 bytes de datos:
Respuesta desde 172.66.43.64: bytes=32 tiempo=8ms TTL=54
Respuesta desde 172.66.43.64: bytes=32 tiempo=8ms TTL=54
Respuesta desde 172.66.43.64: bytes=32 tiempo=27ms TTL=54
Respuesta desde 172.66.43.64: bytes=32 tiempo=15ms TTL=54

Estadísticas de ping para 172.66.43.64:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 8ms, Máximo = 27ms, Media = 14ms
```

Figura 145: Tiempo de respuesta después del ataque

Se procede a hacer otra prueba con 3000 solicitudes

```
┌──(root㉿kali)-[/home/kali/Escritorio/Slowloris/slowloris]
└─# python3 slowloris.py 172.66.43.64 -s 3000
[27-01-2023 12:27:51] Attacking 172.66.43.64 with 3000 sockets.
[27-01-2023 12:27:51] Creating sockets...
[27-01-2023 12:28:09] Sending keep-alive headers...
[27-01-2023 12:28:09] Socket count: 1021
[27-01-2023 12:28:09] Creating 2193 new sockets...
```

Figura 146: tercer ataque DDOS con 3000 solicitudes

Se termina el envío de solicitudes

```
[27-01-2023 12:33:42] Sending keep-alive headers...
[27-01-2023 12:33:42] Socket count: 142
[27-01-2023 12:33:42] Creating 2858 new sockets...
[27-01-2023 12:33:57] Sending keep-alive headers...
[27-01-2023 12:33:57] Socket count: 142
[27-01-2023 12:33:57] Creating 2996 new sockets...
[27-01-2023 12:34:12] Sending keep-alive headers...
[27-01-2023 12:34:12] Socket count: 4
[27-01-2023 12:34:12] Creating 2999 new sockets...
[27-01-2023 12:34:27] Sending keep-alive headers...
[27-01-2023 12:34:27] Socket count: 1
[27-01-2023 12:34:27] Creating 3000 new sockets...
[27-01-2023 12:34:42] Sending keep-alive headers...
[27-01-2023 12:34:42] Socket count: 0
[27-01-2023 12:34:42] Creating 3000 new sockets...
[27-01-2023 12:34:57] Sending keep-alive headers...
[27-01-2023 12:34:57] Socket count: 0
[27-01-2023 12:34:57] Creating 3000 new sockets...
```

Figura 147: ejecución del tercer ataque

Ping durante la ejecución del envío de 3000 solicitudes

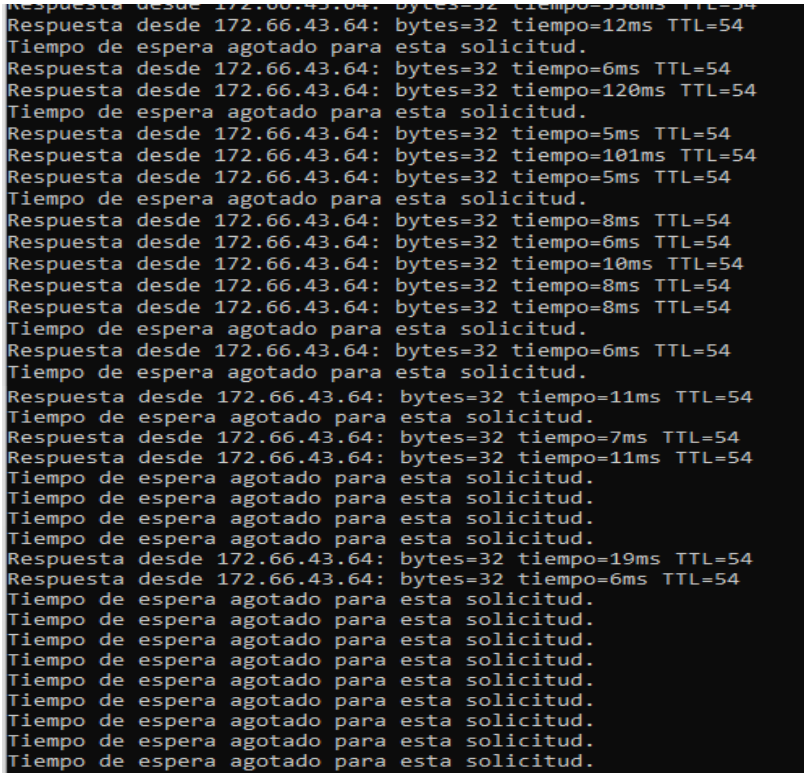


Figura 148: Tiempo de respuesta durante el tercer ataque

La página tuvo retardos, pero si respondió bien antes una cantidad alta de solicitudes

Para verificar que no es vulnerable a este ataque, se ejecutó desde la terminal de kali Linux y otra herramienta como Ddos ripper, obteniendo los mismos resultados.

1. Se verifico el escaneo de los puertos para conocer los servicios impartido por el entorno web y la ejecución de ping de la dirección para conocer la ip que maneja

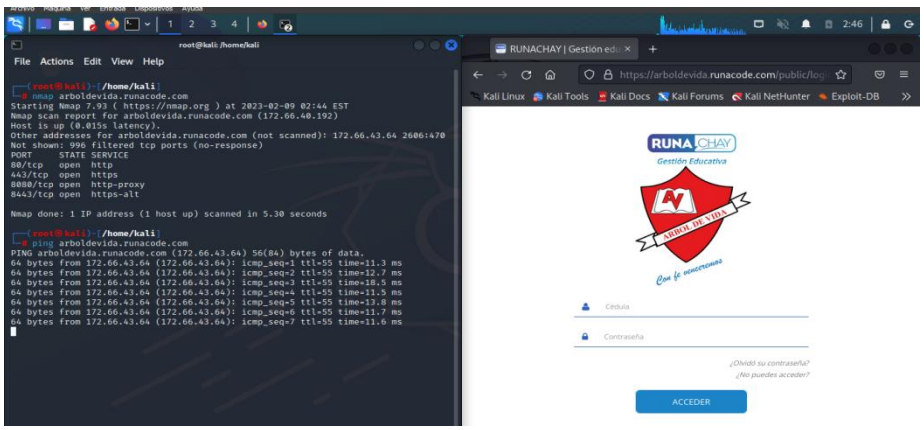


Figura 149: Ping hacia el aplicativo

2. Ejecución del ping de la ip hallada, y se observa los paquetes de envió

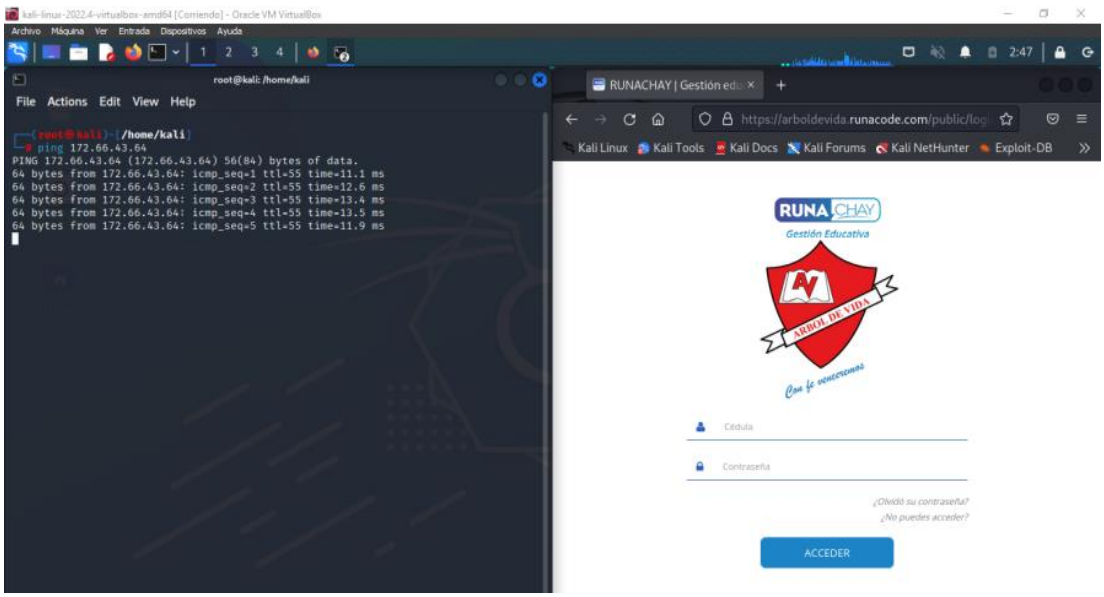


Figura 150: Ping hacia la ip hallada

3. Con el siguiente comando realizamos las solicitudes de envió de solicitud, insertando un tamaño de cada petición de 8192 KB que es el resultado de 8MB y el parámetro de interval de 0.001 se va enviar mil paquetes por segundos

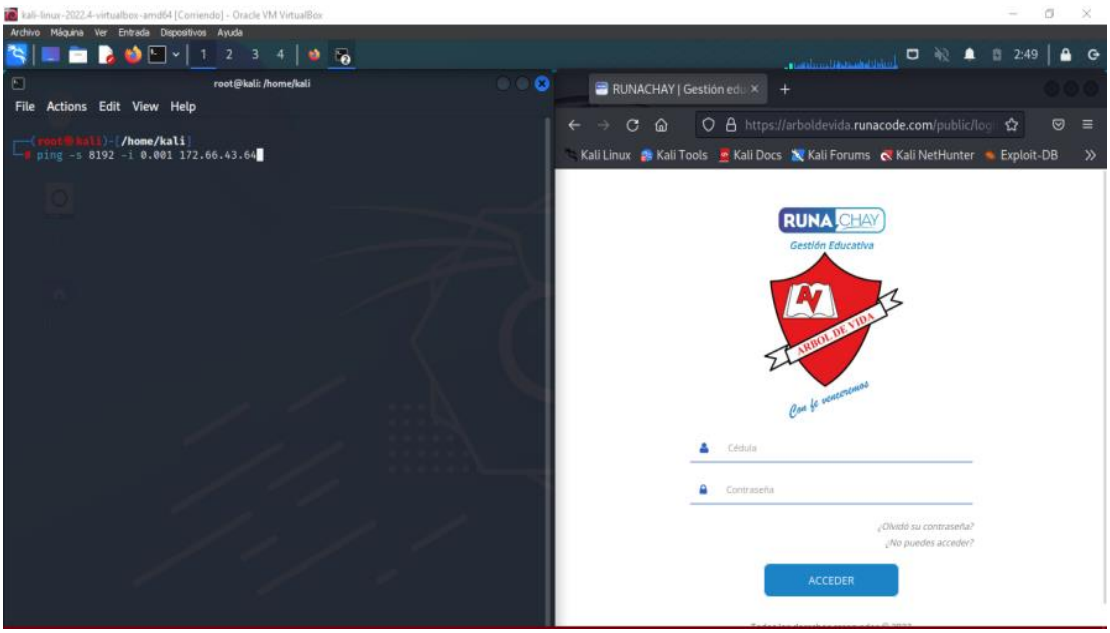


Figura 151: envío de 8MB solicitudes desde terminal kali linux

4. Aquí se enviará 10 mil paquetes de segundos

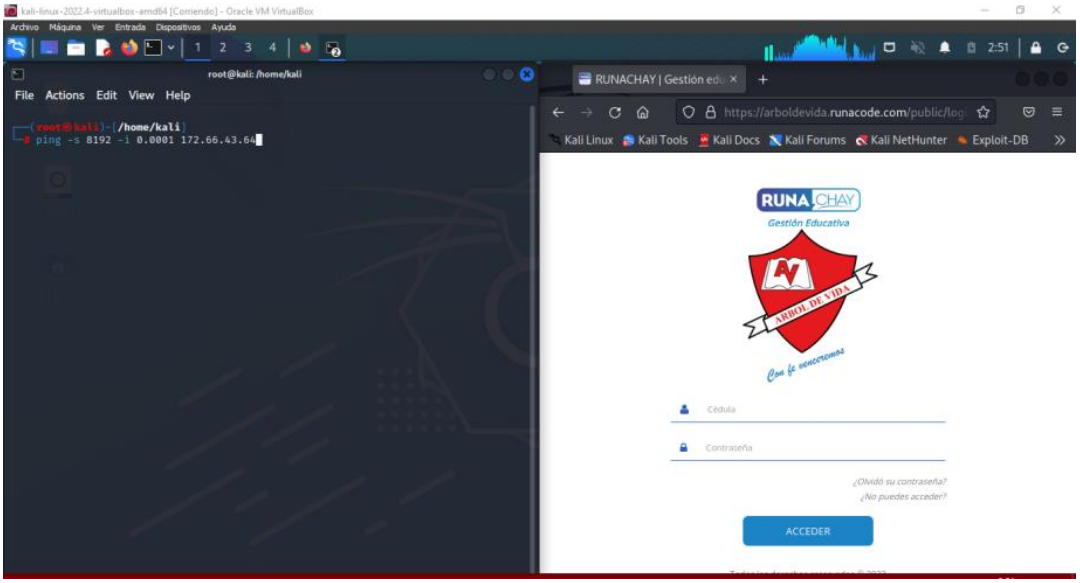


Figura 152: envío de 10 mil solicitudes

5. Las peticiones son ejecutadas, pero el aplicativo se mantiene estable, sin cambio alguno.

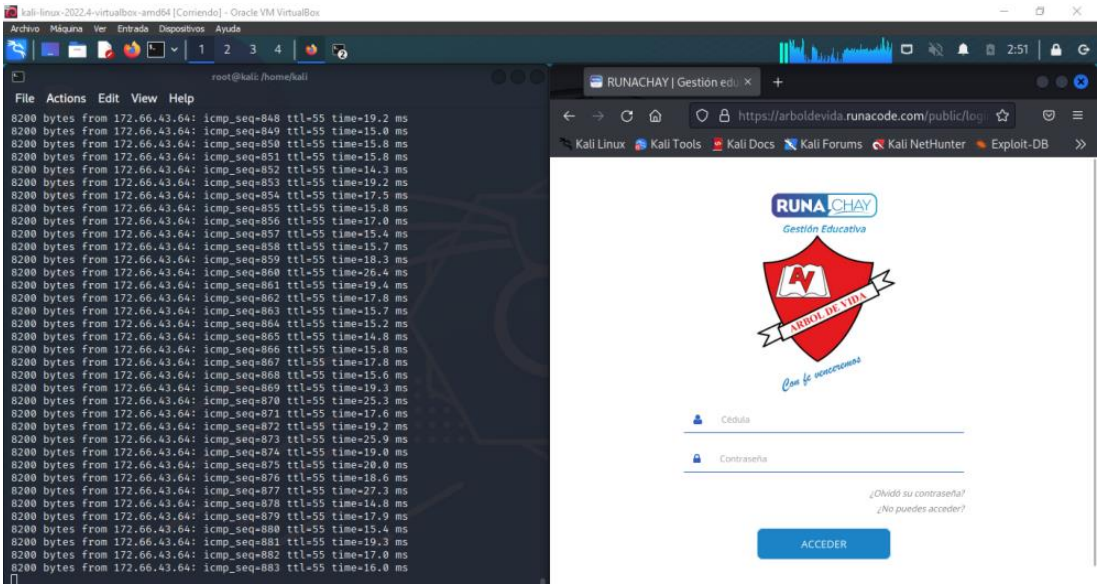


Figura 153: Correcta respuesta del aplicativo

6. Se descarga el script DDos-RRiper en la dirección de git en formato zip

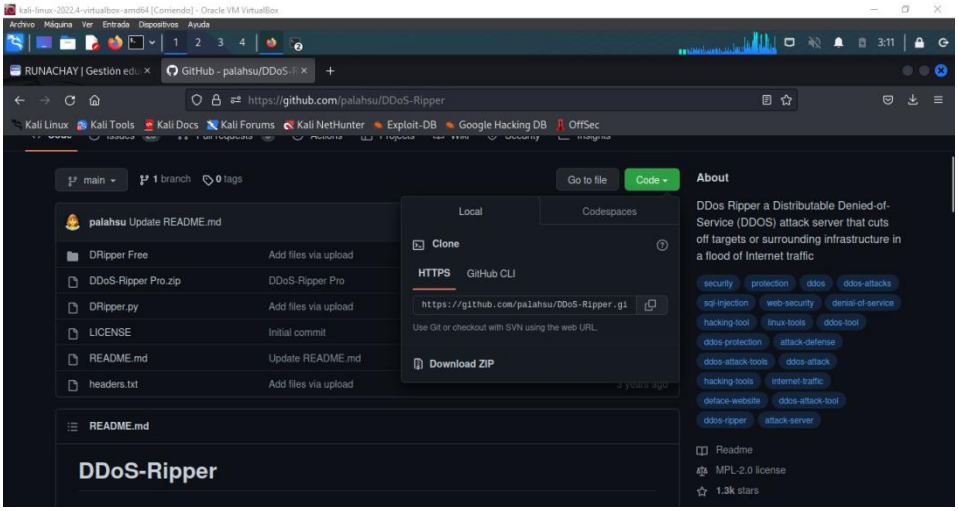


Figura 154: Descarga de Ddos RRiper

7. Con unzip descomprimir el archivo

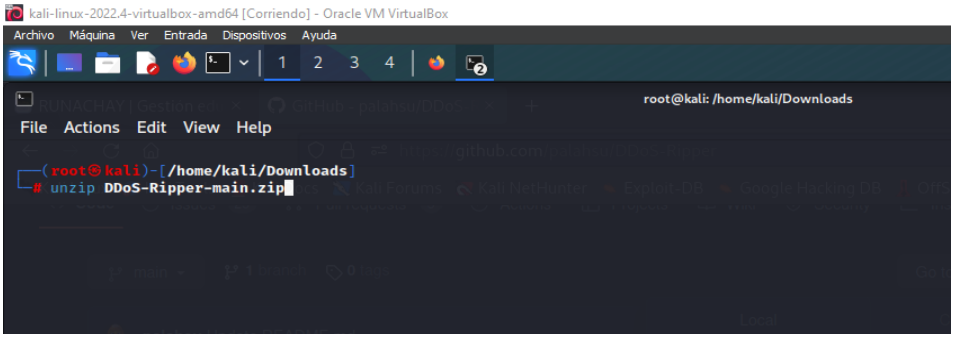


Figura 155: Unzip del archivo descargado

8. Ingresar a la carpeta donde se aloja el script

Figura 156: Ingreso a carpeta de archivo descargado

9. Ejecutar la herramienta dripper de Python con el siguiente comando, asignado el parámetro –s para la dirección –p para el puerto que este caso es 80

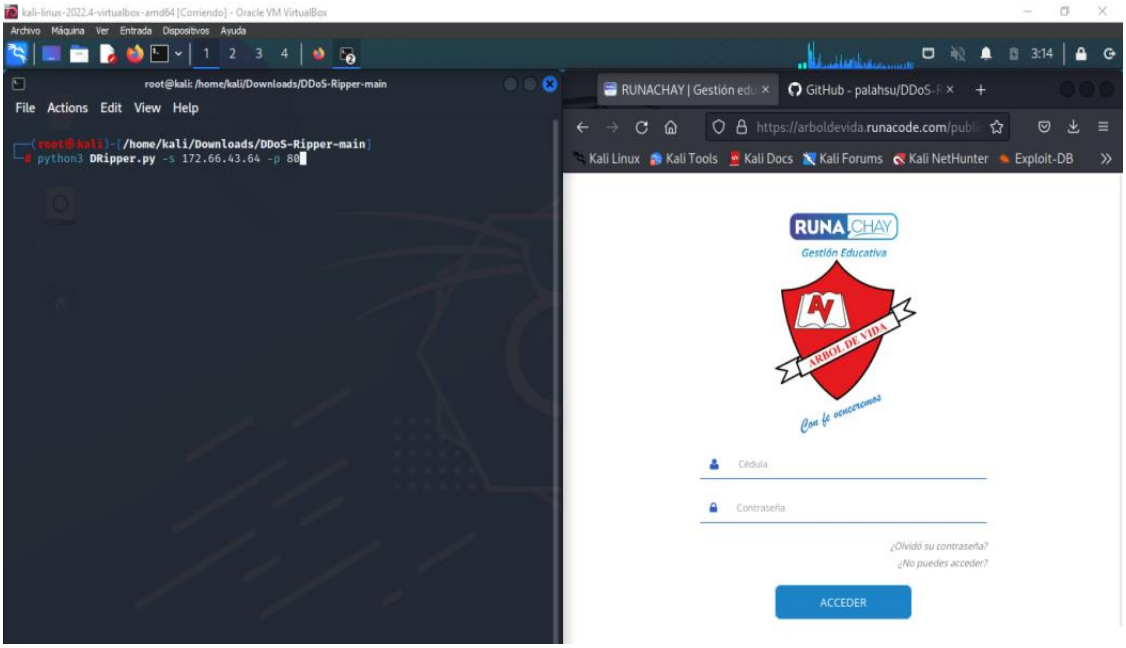


Figura 157: Ejecución de la herramienta DDOS RIPPER

10. Se comienza a ejecutar la herramienta para enviar las cargas al aplicativo

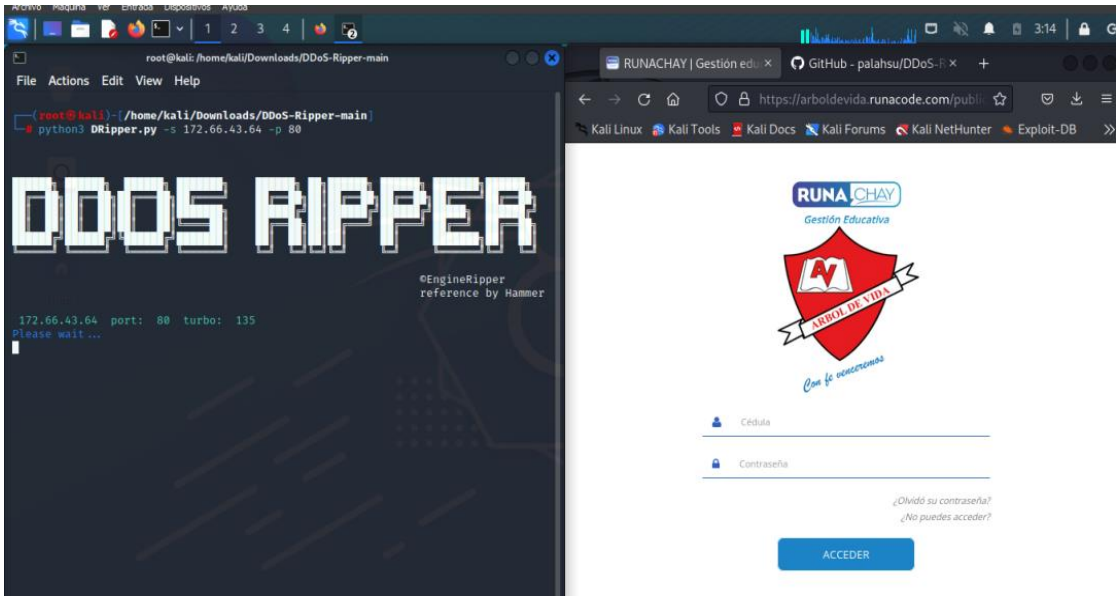


Figura 158: Envío de solicitudes al aplicativo

11. Se comienza el envío masivo de las solicitudes para saturar el aplicativo

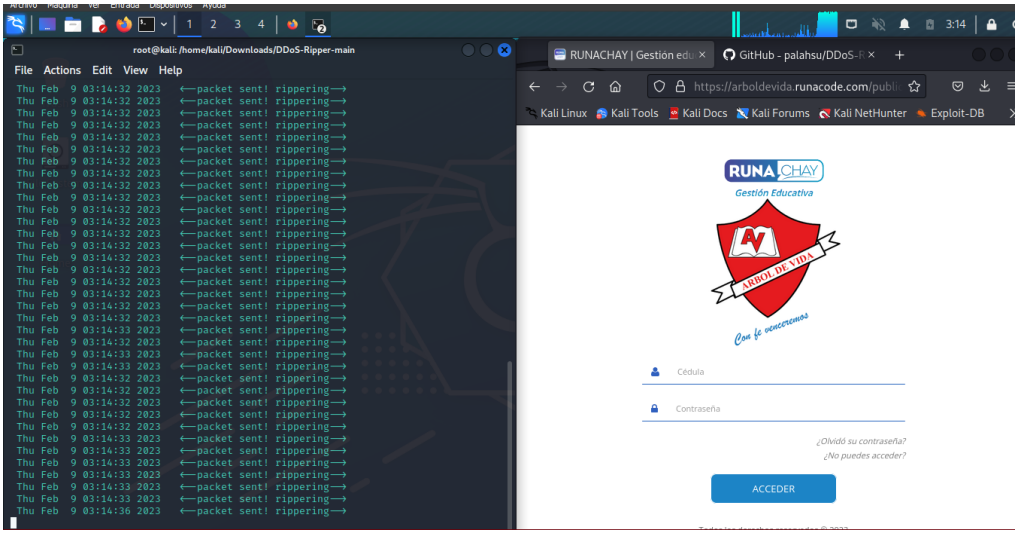


Figura 159: Envío masivo de solicitudes al aplicativo

12. Al observar, se identifica que en intervalos se observa la destrucción del bots, identificando que el aplicativo contiene una herramienta ante denegación de servicio y esta actúa contra el ataque

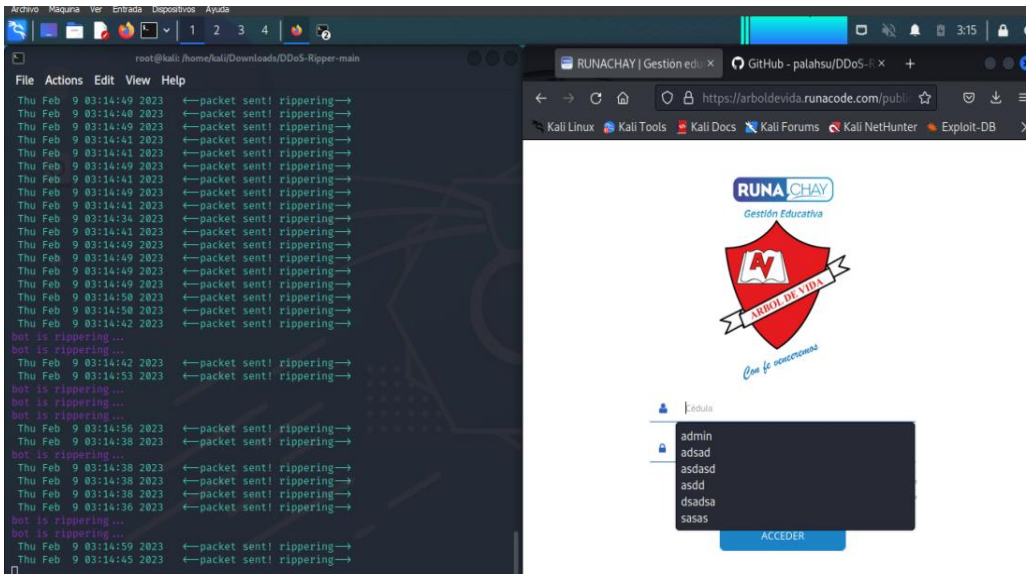


Figura 160: Destrucción de bots en el envío de solicitudes al aplicativo

13. La saturación del aplicativo no es ejecutada, sigue intacto, pero la destrucción delos bots es más continuo sobre el ataque

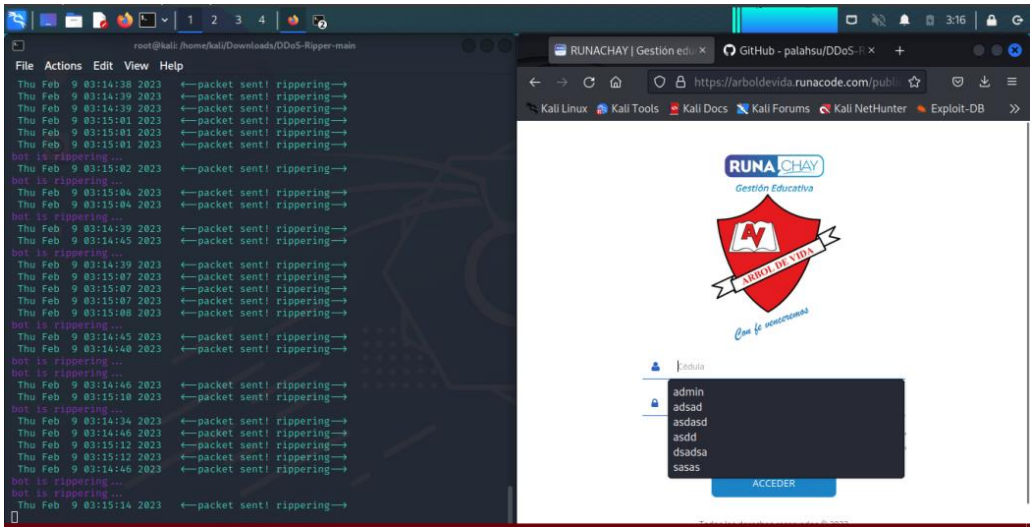


Figura 161: Destrucción más continua de bots en el envío de solicitudes al aplicativo

Anexo 17. Comprobación de vulnerabilidad clickjacking

Para comprobar que existe la vulnerabilidad de clickjacking, se usará la herramienta Jack master clickjacking disponible en github

Primero nos ubicamos en la carpeta descargas y luego iniciamos la clonación de la herramienta con el comando

Git clone https://github.com/sensepost/jack

Figura 162: Clonación de la herramienta Jack sensepost en kali linux

Con el comando ls, listamos todo el contenido de la carpeta descargas, luego ingresamos a la carpeta Jack y revisamos su contenido

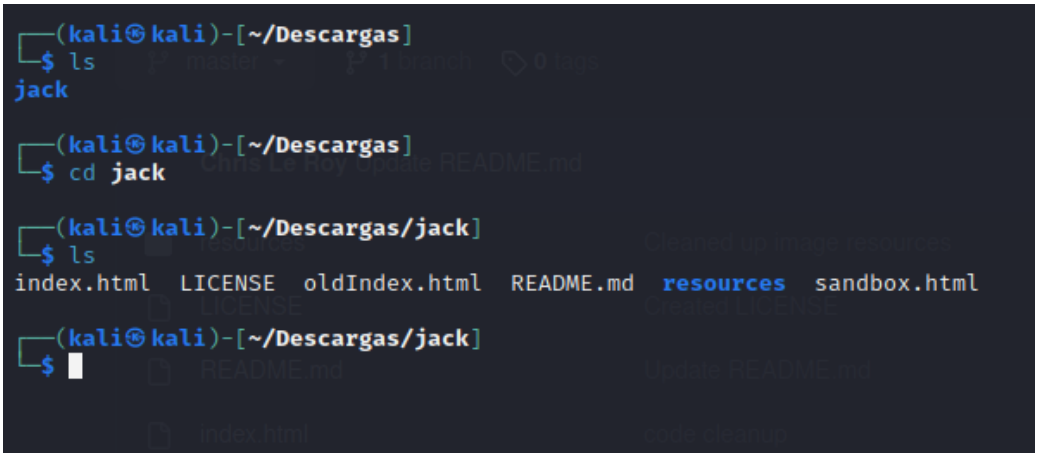


Figura 163: verificación de instalación de la herramienta JACK sensepost

Se ejecuta el index.html para empezar a interactuar con la herramienta

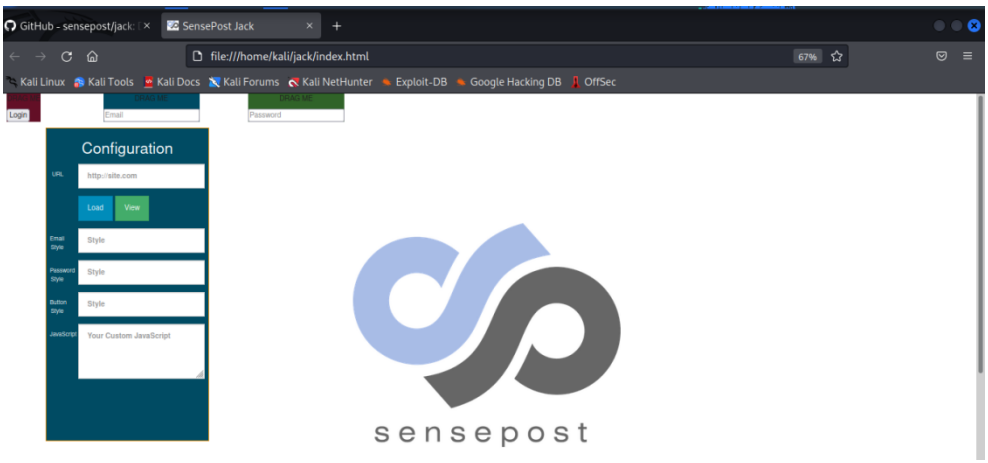


Figura 164: Interfaz de SensePost Jack

Para comprobar si el aplicativo de la institución educativa es vulnerable al ataque clickjacking, se ingresa la url y hacemos click en load.

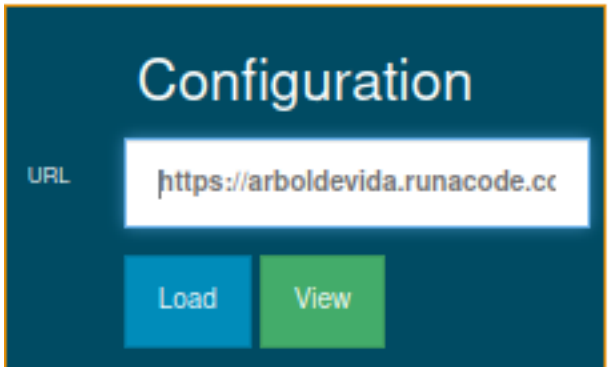


Figura 165: Ingreso de URL para comprobar si es vulnerable al clickjacking

Efectivamente la página es vulnerable al ataque clickjacking, porque cargó correctamente en la pantalla de la herramienta.

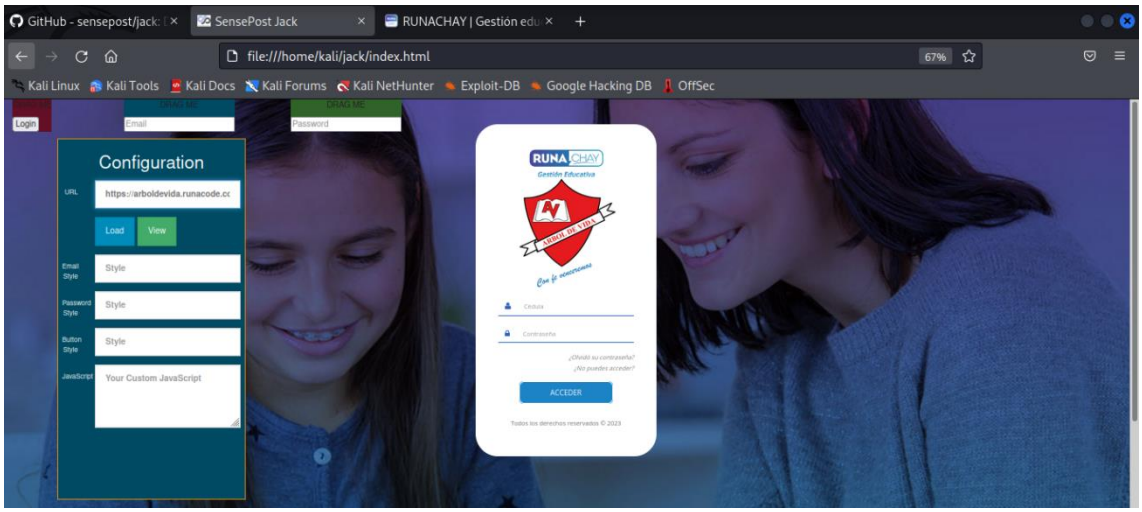


Figura 166: Verificación de vulnerabilidad

La herramienta nos da la opción de añadir campos de ingresos de datos en alguna parte de la página que estamos comprobando, en este caso, se añade en el formulario de inicio de sesión.

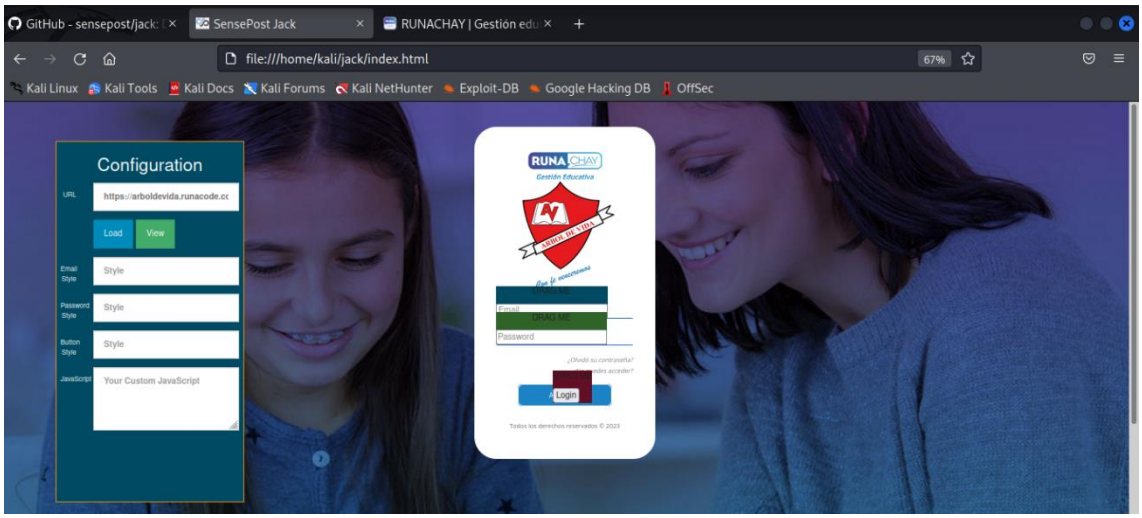


Figura 167: Clonación de la página e ingreso de campos de texto

Una vez colocado los campos de ingreso de datos, se hace click en el botón view y nos muestra la clonación de la página con esos campos

Figura 168: Interfaz con clickjacking

Llenamos el formulario y hacemos click en ingresar

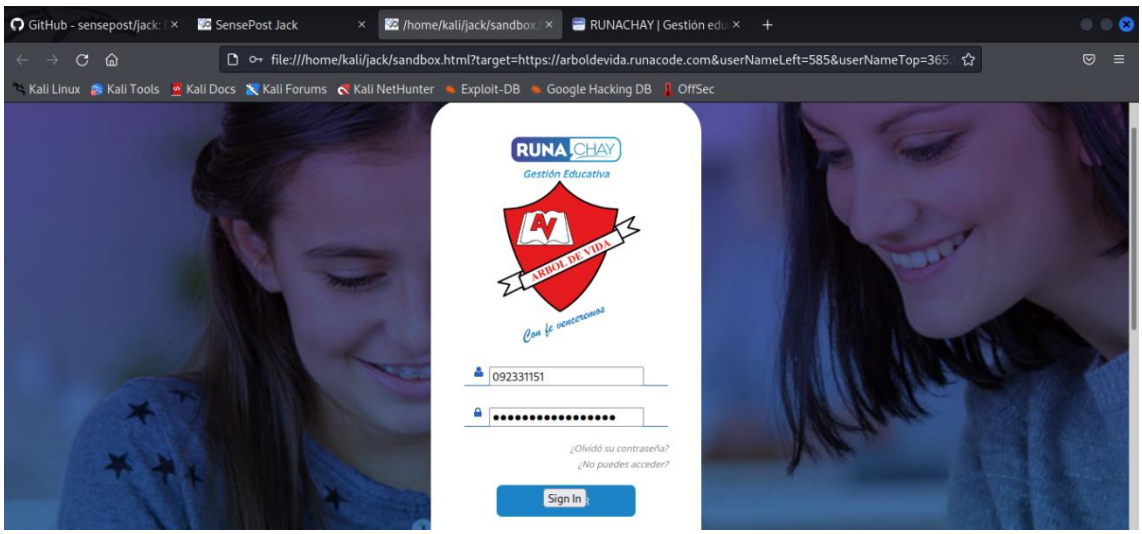


Figura 169: Ingreso de datos en la página con clickjacking

Al hacer dicha acción, la herramienta muestra una alerta con el usuario y contraseña que ingresamos, es decir permite capturar los datos de inicio de sesión.

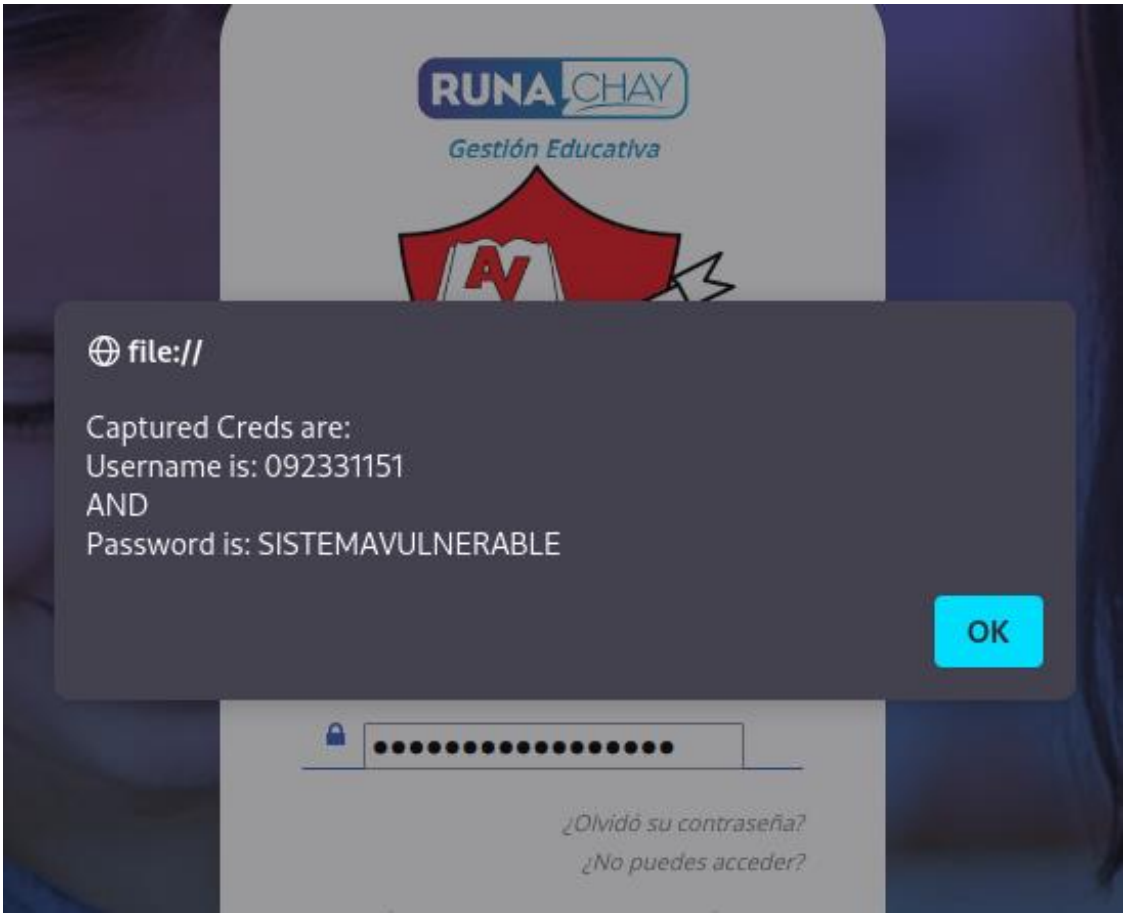


Figura 170: Datos capturados con SensePost Jack

Cuando una página o sitio web no tiene esta vulnerabilidad de clickjacking, se muestra así

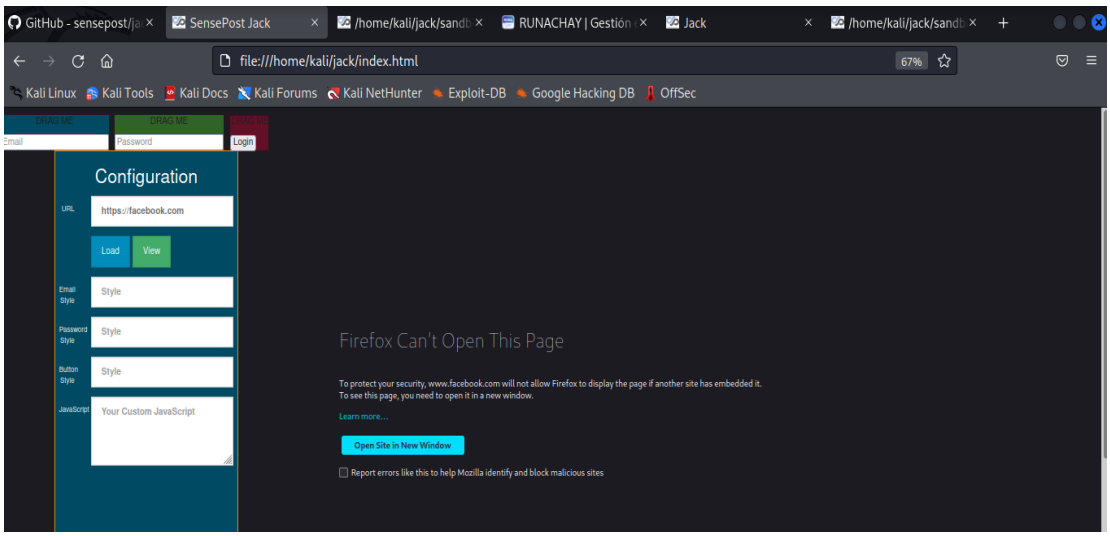


Figura 171: Muestra de página protegida contra clickjacking

Anexo 18. Ataque de ingeniería social mediante QR por via Whatsapp.

Iniciamos la herramienta Social Engineering toolkit desde un sistema operativo virtualizado (Kali Linux), la cual mostrará este entorno de inicio. Seleccionamos la opción de ataque, en este caso ingeniería social que es la opción 1.

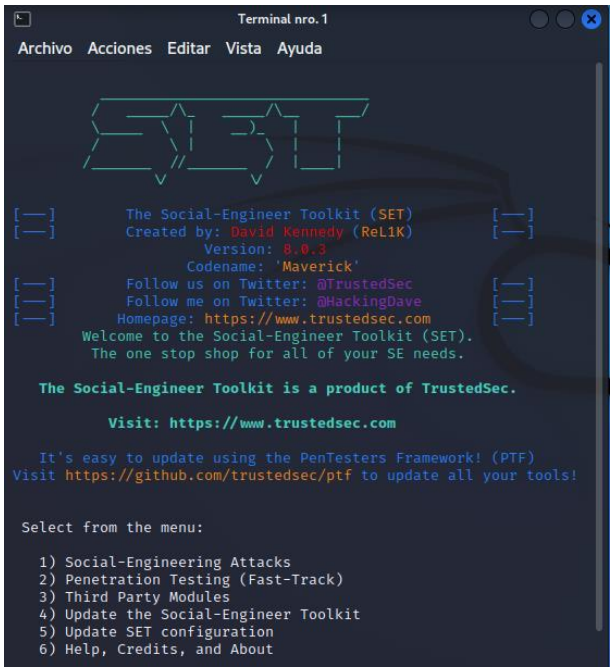


Figura 172: Interfaz de Social Engineering toolkit

Se despliega otro menú de opciones, donde seleccionamos nuestro ataque, la opción 2: Website attack vector.

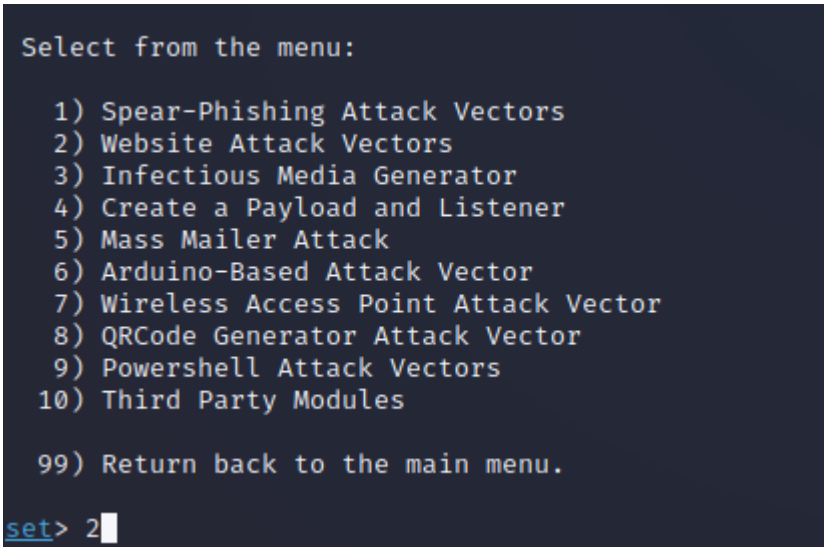


Figura 173: Menú de Social Engineering toolkit

En el siguiente menú, se seleccionará la opción 3: Credential harvester, attack metol, permitiendo clonar una página web que será subida a un servidor.

Figura 174: Ejecución de la opción 3 Credential Harvester Attack Method

En el menú que se muestra a continuación, se encuentran 3 opciones, de las cuales, la primera es una web que viene por defecto, la segunda es una clonación de página, que es poner el link para el sitio a clonar y la tercera es custom import, que es una página creada por autoría propia, en este caso se seleccionará la opción 2.

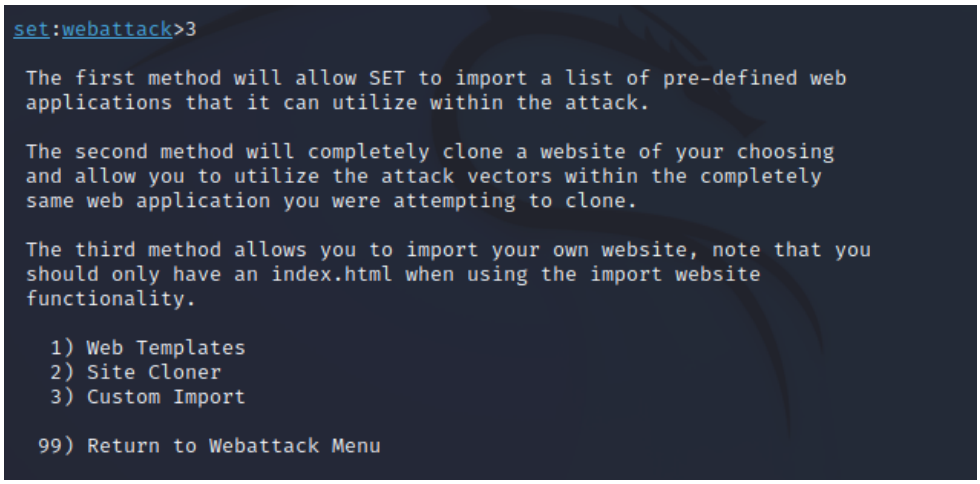


Figura 175: Selección de opción 2, clonación de página

A continuacion, se debe ingresar la ip que recogerá los datos ingresados por las víctimas, comúnmente es la ip de la máquina creadora.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
```

Figura 176: IP que recogerá los datos de las victimas

Finalmente debemos ingresar la dirección de la página a clonar

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://arboldevida.runacode.com
```

Figura 177: Dirección de la página a clonar

Se mostrará información que afirma la creación de la página, encontrándose lista para agregarla a un servidor web y comenzar a enviar el link a las víctimas.

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://arboldevida.runacode.com

[*] Cloning the website: https://arboldevida.runacode.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardle
ss, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Figura 178: Confirmación de clonación de la página

Comprobamos la clonación de la página.

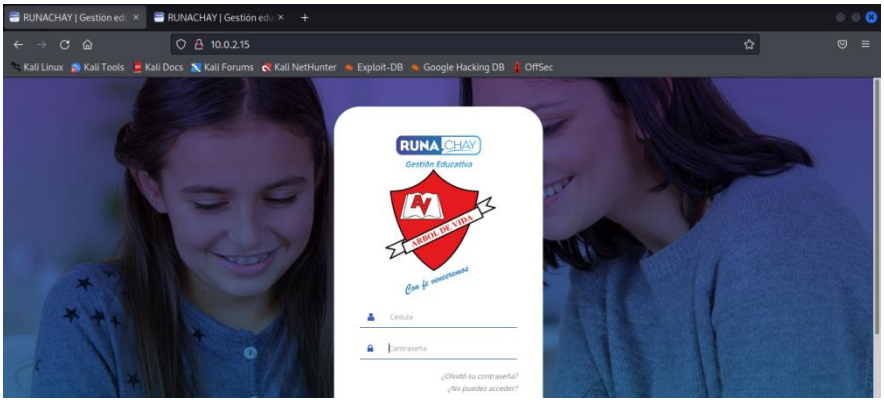


Figura 179: Pagina clonada

Luego se genera código qr con el enlace de la página clonada para enviar a nuestras victimas mediante la red social WhatsApp

Figura 180: Opción generador de código QR

Luego de haber generado mostrara la dirección en donde se guardó la imagen del QR para poder copiarlo, como esta en una carpeta Root necesita privilegios de administrador.

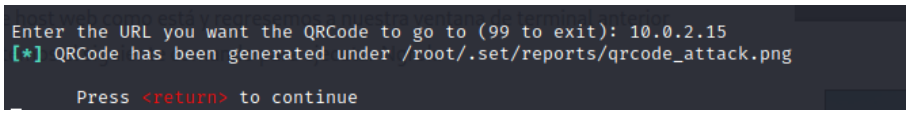


Figura 181. Dirección de ubicación del Código QR

No dirigiremos a la dirección donde se encuentra el código QR, usando comando CD para abrir carpetas y LS para mostrar los archivos.

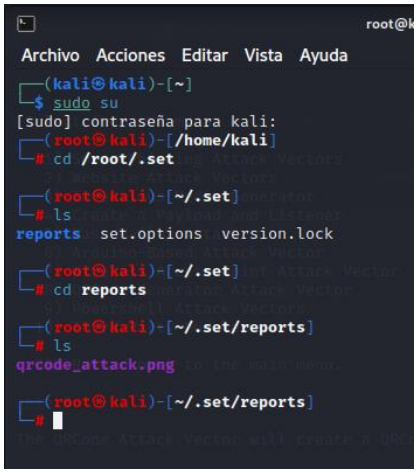


Figura 182. Ingreso a la carpeta Root

Se procede a copiar el archivo en una direccion donde podremos verla sin los privilegios de administrador usando el codigo MV que es para mover un archivo.

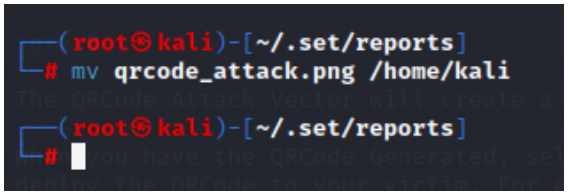


Figura 183: Re direccionar el archivo PNG

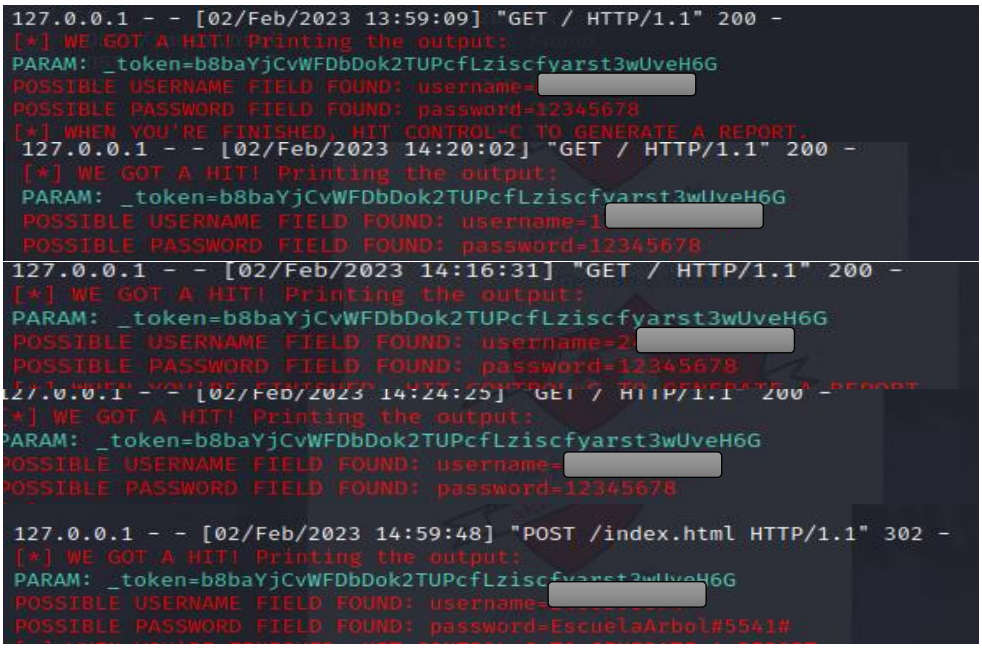
Una vez generado el código QR

Figura 184: Código QR

Se procede a usar la red social WhatsApp para poder enviar el código junto con un mensaje para la victima especificada.

Figura 185. Ataque por WhatsApp

Datos obtenidos de las victimas



Acceso al sistema con credenciales que ingresaron las víctimas del ataque

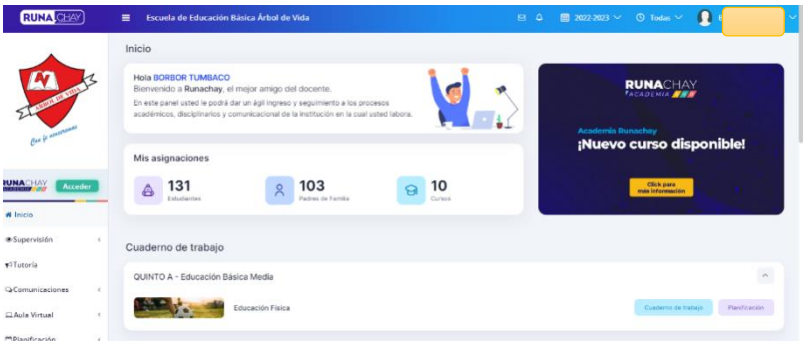


Figura 187: Acceso al sistema con credenciales de las victimas

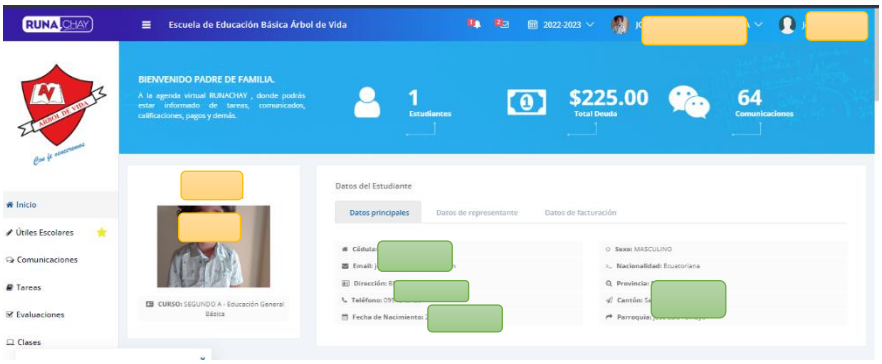


Figura 188: Acceso con los datos de las victimas

Unas víctimas reportaron el mensaje

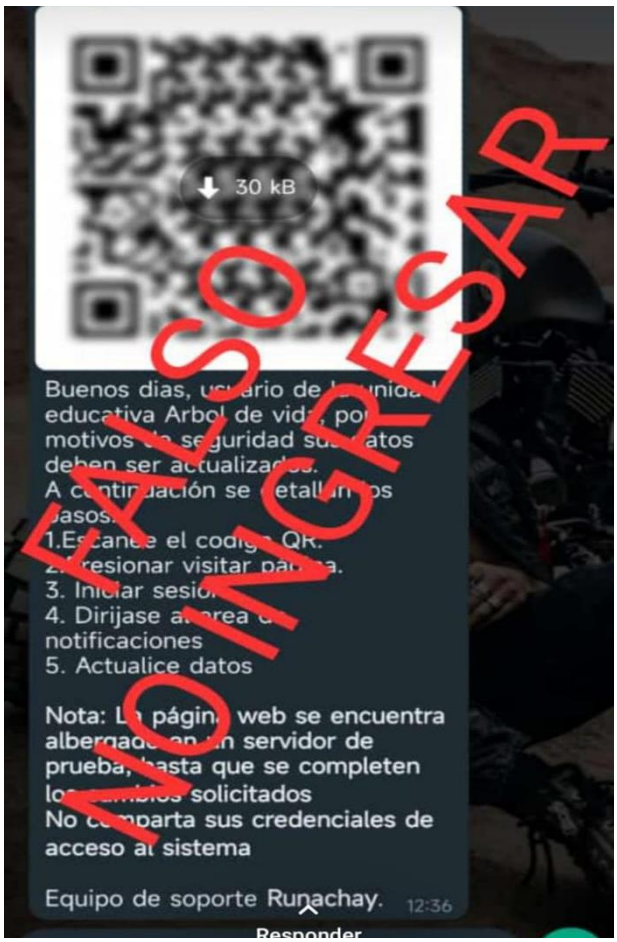


Figura 189: Víctimas reportaron el mensaje

Solicitaron cambio de contraseña a los usuarios luego de la prueba

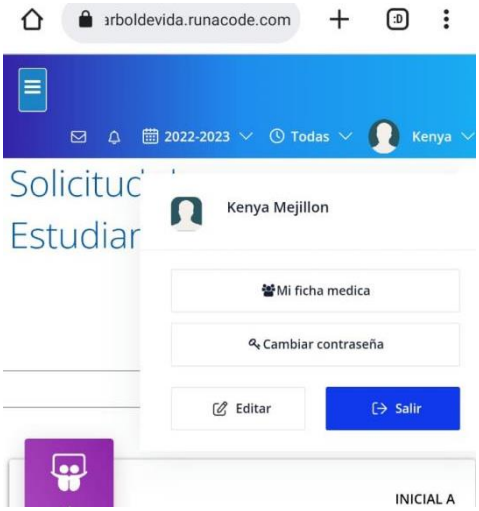


Figura 190: Solicitud de cambio de contraseña luego de la prueba

Anexo19. Informe de auditoría

ÍNDICE

1. AUDITORÍA PRELIMINAR DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN

1.1 DATOS DE LA EMPRESA AUDITADA

Cliente: Unidad Educativa Árbol de Vida. Preparado por: Kenya Mejillón

Fecha: 3-Febrero-2023 Periodo: 2023

1.2 ALCANCE DE AUDITORÍA DEL ÁREA DE T.I.

La presente auditoría consiste en la evaluación del aplicativo de la unidad árbol de vida, implica la revisión de interfaces en los módulos que soportan los procesos académicos de la institución, manuales de procedimientos y análisis de la seguridad y la integridad en el procesamiento de datos mediante pruebas técnicas.

1.3. OBJETIVOS DE AUDITORÍA DEL ÁREA DE T.I.

Evaluar la seguridad del aplicativo y base de datos del aplicativo en los módulos matriculación e ingreso de notas, mediante herramientas de auditoría informática, para identificar vulnerabilidades y proponer mejoras de seguridad basado en marco de la norma ISO 27001 referida a la gestión de la seguridad de la información, el marco internacional de trabajo para gobernabilidad y gestión de las tecnologías de la información COBIT 5.0, el estándar NIST SP 800 que brinda controles de seguridad y privacidad para todos los sistemas de información y el estándar de accesibilidad Web Content Accessibility Guidelines(WCAG).

1.4. OBSERVACIONES Y RECOMENDACIONES

Durante la visita preliminar del período agosto 10 del 2022 a 3 de febrero del 2023, los resultados obtenidos luego de la revisión y verificación de las interfaces y ejecución de pruebas junto con la evaluación de los controles implementados que garantizan la seguridad de los recursos informáticos y de la información, se obtuvo lo siguiente:

1.4.1. DISEÑO RESPONSIVE

De la revisión efectuada se pudo constatar que al acceder al aplicativo desde diferentes navegadores y dispositivos, no tenía un diseño responsivo, en muchas ocasiones el contenido se descuadraba y no se podía navegar con facilidad.

El estándar de accesibilidad Web Content Accessibility Guidelines(WCAG) 2.2 menciona la importancia de cumplir con directrices claves para la accesibilidad, percepción, operatividad y comprensibilidad en los sitios web.

Por lo expuesto se recomienda a la institución que solicite al proveedor del aplicativo que el contenido sea adaptable automáticamente a diferentes tamaños y dispositivos, uso de imágenes y videos deben tener un tamaño adaptable y un texto alternativo accesible, también la estructura html debe ser clara y lógica para que las personas con discapacidades puedan navegar y comprender el contenido del aplicativo, de la misma manera el uso de colores contrastantes adecuados para que las personas con discapacidades visuales puedan leer y comprender el contenido, finalmente que se hagan pruebas en diferentes dispositivos para garantizar la accesibilidad y diseño responsivo.

Comentario de la Administración

1.4.2. RESGUARDO DE INFORMACIÓN/COPIAS DE SEGURIDAD

Al momento de realizar la revisión de las opciones que posee el aplicativo desde un usuario administrador, no existe la opción de resguardo de información o hacer copia de seguridad.

El estándar NIST SP 800-53(Security and Privacy Controls for Federal Information Systems and Organizations) en la sección SC (Control de seguridad) define los requisitos de seguridad para proteger y garantizar la integridad, confidencialidad y disponibilidad los sistemas de información y los activos de información donde es muy relevante las copias de seguridad y recuperación de información.

Adicionalmente la norma ISO/IEC 27001:2005 sección 5, Seguridad de la información, y específicamente en su cláusula 6, Administración de activos establece la necesidad de identificar, clasificar y proteger los activos de información y establecer medidas de seguridad para garantizar su confidencialidad, integridad y disponibilidad.

Se recomienda que integren en el aplicativo web la opción de resguardo de información. Puede considerar los controles establecidos por NIST SP 800-53 e ISO/IEC 27001:2005 tales como realización periódica de copias de seguridad, protección de las copias de seguridad contra la pérdida y el acceso no autorizado, pruebas regulares de recuperación para asegurarse de que las copias de seguridad sean válidas y se puedan recuperar en caso de una falla.

En general, la inclusión de la opción de hacer copias de seguridad en la interfaz de administrador es una buena práctica para mejorar la seguridad y disponibilidad de los datos en una aplicación web.

Comentario de la Administración

1.4.3. DUPLICACIÓN DE REGISTROS

En la revisión de los usuarios registrados en el sistema, en la sección de representantes se evidenció que hay registros duplicados, un problema común que se presenta en muchos sistemas. Esta situación puede tener consecuencias graves para la integridad de los datos y la toma de decisiones basadas en ellos, ya que puede llevar a información redundante o contradictoria. Además, puede aumentar el tamaño de la base de datos y disminuir la eficiencia y velocidad del sistema.

La norma ISO/IEC 27001 para la seguridad de la información en la sección de gestión de acceso detalla la importancia de la implementación de un proceso riguroso de gestión de acceso y verificación de identidad porque permite garantizar la integridad y confiabilidad de los datos y la protección de la privacidad de los usuarios.

Se recomienda realizar verificaciones periódicas de los registros de usuarios para detectar y corregir cualquier duplicación. se puede emplear técnicas o procedimientos de la norma ISO/IEC 27001 para detectar y prevenir duplicación de registros tales como asignación de identificadores únicos a cada usuario para evitar la creación de múltiples registros, validación de información de usuario, monitorear los registros de acceso para detectar cualquier actividad sospechosa que pueda indicar la creación de registros duplicados.

Comentario de la Administración

1.4.4. GESTIÓN DE SESIONES

El aplicativo no tiene establecido tiempos límites de inactividad para que las sesiones sean inválidas y requieran ingreso de credenciales nuevamente, mantener una sesión activa durante varias horas de inactividad puede ser un riesgo de seguridad si el usuario no cierra sesión en un equipo compartido o en un dispositivo inseguro. Esto puede permitir a un atacante acceder a la cuenta y a la información del usuario.

La norma ISO/IEC 27001:2005 referida a la gestión de sesiones facilita los requisitos que permiten asegurar la gestión adecuada de las sesiones de los usuarios en los sistemas informáticos. Adicionalmente el estándar NIST SP 800-63B en la sección Autenticación y sesión de usuario menciona la importancia de implementar mecanismos para gestión de sesiones segura y describe las mejores prácticas para el inicio y la finalización de sesiones de usuario

Se recomienda determinar política de seguridad y los requisitos de privacidad de la aplicación, también establecer e implementar un tiempo límite de inactividad para la sesión, después del cual se cierra automáticamente y el usuario debe iniciar sesión de nuevo. Esta medida ayuda a proteger la privacidad y la seguridad de la información del usuario para evitar que terceras personas pueden tener acceso en ese lapso de tiempo y realice modificaciones en el sistema sin ser percibido.

Sin embargo, si se desea tener una sesión persistente para una mejor experiencia del usuario, es posible que se permita mantener la sesión activa durante un período de tiempo más largo, siempre y cuando se implementen medidas de seguridad adecuadas para proteger la privacidad y la seguridad de la información del usuario. Por ejemplo, implementar la autenticación de dos factores o la protección mediante contraseña fuerte para proteger la cuenta.

Comentario de la Administración

1.4.5. EMISIÓN DE CERTIFICADOS, COMPROBANTES DE MATRÍCULA Y ESTADOS DE PERIODOS ACADÉMICOS.

Al realizar pruebas de interfaz en el módulo matriculación se evidenció que no hay una correcta secuencia de los procesos, ya que al solicitar cupo para matriculación se puede establecer el estado del cupo solicitado como: aprobado, aprobado con nivelación y reprobado; sin embargo al estar en este proceso, sin haber procesado la matricula, permite emitir certificados, fichas y comprobantes de matrícula, lo correcto sería inhabilitar estas opciones mientras el proceso de matriculación no se haya ejecutado.

También al realizar pruebas de interfaz en el módulo ingreso de notas se observó que al seleccionar periodos académicos (parciales, quimestres) no vigentes, el aplicativo no permite modificar notas, pero si añadir insumos (trabajos), no deshabilita dicha opción, también en las notas ingresadas en esos periodos, permite ver detalles y agregar una observación.

La norma ISO/IEC 27001:2005 referida a la gestión de la seguridad de la información facilita los lineamientos que permiten asegurar la confidencialidad, integridad y disponibilidad de la información, así como los sistemas que la procesan.

Se recomienda diseñar y establecer un manual de los procedimientos del aplicativo para su debida revisión y aprobación de cumplimiento lógico, evaluar que se empleen condiciones en los procesos para controlar habilitación de opciones en el momento adecuado, además de definir la periodicidad de las pruebas de integridad y funcionalidad de los procesos..

Comentario de la Administración

1.4.6. MANUAL DE USUARIO

Durante el proceso de auditoría se constató que la institución no cuenta con manual de usuario que les permita adquirir información de las operaciones que el aplicativo ofrece, el medio que les otorgó el equipo de desarrolladores para comprender las distintas funcionalidades fue mediante videos tutoriales colgados en el aplicativo y el canal de YouTube del grupo desarrollador, también les brindaron capacitaciones al personal de la institución.

El marco internacional COBIT 5.0 para la Dirección de TI en el área de garantía de la calidad del proceso en el subproceso de administración de la documentación y la norma ISO 9001 (Sistemas de gestión de la calidad) mencionan la importancia de tener un manual de usuario porque se puede comprender mejor, cómo utilizar la tecnología y cómo cumplir con los estándares y regulaciones relevantes, lo que a su vez ayuda a garantizar la calidad y la eficiencia de los procesos de TI

Se recomienda solicitar al equipo de desarrollo del aplicativo un manual de usuario, donde se detalle de forma clara todas las especificaciones y funcionalidades del aplicativo, solicitar actualizaciones del mismo, toda esa información puede ser útil para solucionar problemas y resolver dudas rápidamente, prevenir vulnerabilidades y errores de seguridad. En resumen, tener un manual de usuario es importante en términos de seguridad de la información porque puede ayudar a garantizar que los usuarios utilicen los productos o servicios de manera segura y que se cumplan los estándares de seguridad relevantes.

Comentario de la Administración

1.4.7. VALIDACIONES DE ENTRADA DE DATOS

En la revisión de formularios de matriculación se evidenció que en gran parte de los campos, no existe la correcta validación según el tipo de dato, lo que implica registro de información errónea y en muchos casos ilógica en los procesos.

Tanto la norma ISO/IEC 27001 y owasp top 10, recomiendan la validación de los datos de entrada en formularios como una medida de seguridad para proteger la integridad y la confidencialidad de los datos; ISO/IEC 27001 establece la necesidad de validar los datos antes de su procesamiento o almacenamiento.

Se recomienda que se apliquen mecanismos para hacer validaciones de entrada de datos como verificar que los datos introducidos sean del formato correcto y cumplan con los requisitos específicos, verificar que los datos introducidos estén dentro de los límites permitidos y sean válidos, verificación de integridad es decir que sean coherentes, verificación de autenticidad, si los datos introducidos provienen de una fuente autorizada.

La validación inadecuada de los datos de entrada en formularios es una de las diez principales vulnerabilidades de seguridad en aplicaciones web; al validar los datos de entrada en formularios según su tipo, se pueden detectar y prevenir errores y ataques, como la inyección SQL o la manipulación de datos no autorizados.

Comentario de la Administración

1.4.8. USO DE LIBRERIAS JAVASCRIPT VULNERABLES

Al realizar diversos escaneos con la herramienta owasp zap, se obtuvo que el aplicativo emplea algunas bibliotecas de JavaScript utilizadas por la aplicación tienen vulnerabilidades conocidas que pueden ser explotadas por un atacante para realizar acciones maliciosas. Estas vulnerabilidades pueden ser de diversos tipos, como errores de seguridad en el código, dependencias obsoletas o inseguras, o configuraciones inadecuadas; una biblioteca de JavaScript puede tener una vulnerabilidad que permita a un atacante ejecutar código malicioso en el contexto de la aplicación, lo que puede permitirle acceder a información confidencial o realizar acciones no autorizadas.

El estándar de seguridad de OWASP (Open Web Application Security Project) en la sección A9:2021 - Utilización insegura de componentes externos, donde menciona la importancia de mantener las bibliotecas JavaScript y una serie de buenas prácticas que deben considerar.

Se recomienda actualizaciones que incluyen parches de seguridad para corregir vulnerabilidades conocidas, mantener las bibliotecas actualizadas asegura que estás protegido de problemas de seguridad ya que las bibliotecas antiguas pueden no ser compatibles con versiones más recientes del navegador o del sistema operativo, lo que puede causar problemas de compatibilidad y errores.

Antes de utilizar una biblioteca, investigue su reputación y busque información sobre vulnerabilidades conocidas o problemas de seguridad, utilizar bibliotecas de fuentes confiables y reconocidas, como GitHub o npm, para asegurarse de que sean de calidad y seguras, también es una buena práctica monitorear los informes de seguridad y responder rápidamente a cualquier vulnerabilidad detectada en una biblioteca.

Siguiendo estas recomendaciones de estándar de seguridad, se pueden reducir los riesgos de vulnerabilidades en las bibliotecas JavaScript y mejorar la seguridad, el rendimiento y la compatibilidad de la aplicación de la aplicación.

Comentario de la Administración

1.4.9. VULNERABILIDAD DE CLICKJACKING

En los escaneos que se realizaron mediante herramientas de auditoría se evidenció que el servidor no tiene definido el encabezado X-Frame-Options anticlicjacking. El encabezado X-Frame-Options permite a un servidor web especificar si una página web puede ser cargada en un marco o no. Si un servidor web tiene definido el encabezado X-Frame-Options con un valor adecuado, se puede evitar que una página web se muestre en un marco y, por lo tanto, protegerla de los ataques de clicjacking. Al no tener definido el encabezado X-Frame-Options, significa que no se está protegiendo adecuadamente contra los ataques de clicjacking y que la página web puede ser cargada en un marco sin restricciones. Esto puede permitir a los atacantes engañar a los usuarios y hacer clic en enlaces o botones maliciosos sin su conocimiento. Debido a lo expuesto se dio paso a la ejecución de este ataque, se realizó la prueba mediante poc's donde se comprobó la efectividad del mismo.

Al comprobar la efectividad del ataque se recomienda emplear las medidas que ofrece el proyecto owasp en su sección A9:2021 Registro y supervisión insuficiente, como el configurar o usar encabezados HTTP X-FRAME-OPTIONS con protección anti-clikjacking, para evitar la carga de páginas en marcos o iframes no deseados con JavaScript; además, se recomienda registrar y monitorear todas las solicitudes a la aplicación, especialmente aquellas que implican la manipulación de la interfaz de usuario, para detectar posibles intentos de clickjacking.

Comentario de la Administración

1.4.10. VULNERABILIDAD DE CROSS SITE SCRIPTING

Mediante los escaneos se obtuvo que el aplicativo web no tiene definido en el encabezado protección XSS. El encabezado X-XSS-Protection es un mecanismo que permite a un servidor web especificar la configuración de protección contra XSS para el navegador, .el encabezado puede indicar que el navegador debe bloquear la ejecución de scripts maliciosos o que debe notificar al usuario sobre una posible vulnerabilidad. Si el servidor no tiene definido el encabezado X-XSS-Protection, significa que no se está protegiendo adecuadamente contra los ataques de XSS, lo cual hace susceptible al aplicativo frente a ese ataque común para robar datos, credenciales de usuarios. Se realizaron pruebas de inserción de script malicioso que tuvieron éxito en el módulo matriculación.

La norma ISO 27001 referida a la gestión de la seguridad de la información facilita los lineamientos que permiten asegurar la confidencialidad, integridad y disponibilidad de la información, así como los sistemas que la procesan. De la misma manera owasp top 10 en su lista de las 10 amenazas web más importantes, se encuentra el XSS en na de ellas, describe las diferentes formas de XSS y proporciona recomendaciones y mejores prácticas para proteger contra esta amenaza.

Por lo tanto, es recomendable definir y configurar adecuadamente el encabezado X-XSS-Protection para garantizar una protección adecuada contra los ataques y seguridad de una aplicación web. También recomendamos seguir controles especificados por los estándares de seguridad para evitar ser víctima del ataque XSS, siendo las siguientes: administración de usuarios, ambientes de procesamiento, auditoria automática de los sistemas, tratamiento y protección de la información; también se recomiendan las siguientes prácticas de seguridad: validación rigurosa de todos los datos de entrada antes de procesarlas y rechace aquellos que no cumplan con los criterios establecidos, codificación de salidas dinámicas para que los navegadores las interpreten como texto en lugar de código, implementar una política de contenido seguro (CSP) para limitar qué tipo de contenido puede ser ejecutado en la página, utilización de funciones de escape para codificar las entradas y las salidas en diferentes contextos, como HTML, JavaScript y atributos HTML, protección contra el almacenamiento persistente de datos maliciosos limitando la cantidad de información que se almacena en el lado del cliente, y asegurar de que esta información no pueda ser manipulada por un atacante, protección contra el robo de sesión, monitorear continuamente el sistema para detectar y responder a posibles ataques XSS.

Comentario de la Administración

1.4.11. CONFIGURACIÓN INADECUADA DE COOKIES

El aplicativo tiene SSL, que es un protocolo de seguridad que se utiliza para proteger la privacidad y la integridad de los datos que se transmiten a través de Internet.

Al realizar el análisis SSL y escaneo con herramienta owasp zap, se evidenció que las cookies se crean sin el indicador seguro y configuración de cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud de entre sitios. Cuando una cookie se crea de esas formas, significa que puede ser enviada por el navegador al servidor web a través de una conexión no segura (HTTP) en lugar de una conexión segura (HTTPS), por lo tanto la información en la cookie puede ser interceptada y leída por terceros mientras se transmite desde el navegador al servidor, esto puede aumentar el riesgo de seguridad de la información.

La norma ISO/IEC 27001 en su sección protección de información en tránsito proporciona directrices para garantizar la confidencialidad y la integridad de la información durante su transmisión y almacenamiento en dispositivos intermedios, incluyendo la protección de la información en tránsito en redes públicas, privadas o en la nube. También OWASP en la sección A6:2017-Session Management del OWASP Top 10, proporciona recomendaciones en la gestión de sesiones y el uso seguro de cookies.

Se recomienda establecer flags de seguridad, es decir que las cookies se configuren con el indicador seguro para que solo se transmitan sobre conexiones seguras (HTTPS).

Usar sólo cookies necesarias: Almacenar solo la información necesaria en cookies, evitando incluir información confidencial o sensible para evitar que los atacantes puedan inyectar código malicioso en las cookies y robar información sensible.

Establecer cookies seguros y HTTPOnly para prevenir ataques XSS y otros ataques en los que los atacantes pueden acceder y manipular los datos almacenados en las cookies.

Establecer cookies con un tiempo de vida limitado para reducir el tiempo durante el cual los atacantes pueden acceder a los datos de la cookie después de que el usuario ha cerrado la sesión.

Encriptar los datos sensibles almacenados en las cookies para proteger los datos confidenciales de accesos no autorizados.

Validar y filtrar adecuadamente los datos almacenados en las cookies

Comentario de la Administración

1.4.12. VULNERABILIDAD DENEGACIÓN DE SERVICIOS (DdoS)

Al realizar la prueba de denegación de servicio al aplicativo de la institución, no se logró el objetivo de colapsar su funcionamiento, por lo que cuentan con un servidor web que tiene integrado entre sus servicios, protección ante ataques de este tipo, manteniendo la disponibilidad y la integridad de la información.

Sin embargo el estándar NIST SP 800-53 en la sección continuidad de operaciones (COOP) e ISO 27001, en la sección de seguridad de la disponibilidad de la información, parte del control de seguridad de la disponibilidad, definen las siguientes buenas prácticas que son recomendables seguir:

- Identificación de amenazas y riesgos: Es importante identificar y evaluar las amenazas y riesgos asociados con los ataques de DoS y DDoS.
- Protección de redes: Es necesario implementar medidas de seguridad para proteger las redes, como firewalls, router, switches y dispositivos de seguridad de aplicaciones.
- Monitoreo de tráfico: El monitoreo en tiempo real es esencial para detectar y mitigar ataques de DoS y DDoS.
- Detección de anomalías: Se deben implementar soluciones de detección de anomalías para identificar patrones de tráfico anormales y detectar posibles ataques.
- Mitigación de ataques: Es importante implementar soluciones de mitigación de ataques, como servidores proxy, sistemas de limpieza de tráfico, y soluciones de red distribuidas de mitigación de ataques.
- Plan de contingencia: Es esencial tener un plan de contingencia en caso de un ataque de DoS o DDoS, incluyendo la identificación de soluciones alternativas para mantener la disponibilidad y continuidad de los servicios.
- Capacitación: Capacitar a los empleados sobre los riesgos de los ataques de DoS y DDoS y cómo prevenirlos y mitigarlos.

Comentario de la Administración

1.4.13. VULNERABILIDAD DE INYECCIÓN SQL

Al realizar prueba de inyección sql en formularios de entrada de datos, no se obtuvo información mediante la inyección de sentencias sql en formularios, ni url, tampoco se hallaron vulnerabilidades SQLI en el aplicativo con el uso de herramientas sqlmap y escáner de vulnerabilidad. En el caso de inyección en url se evidenció que al enviar la url hay una codificación de caracteres especiales, como mecanismo que evita que estos sean interpretados como parte de la consulta SQL, lo que reduce el riesgo de que un atacante pueda ejecutar código malicioso en una base de datos

Sin embargo se recomienda implementar controles y aplicar buenas prácticas establecidas por estándares de seguridad para garantizar la seguridad, disponibilidad e integridad de la información de los sistemas informáticos la ISO 27001 como estándar internacional de seguridad de la información, proporciona un marco de referencia para la gestión de la seguridad de la información, también incluye mejores prácticas de seguridad técnica y operativa, que proporciona recomendaciones para proteger contra una amplia gama de amenazas a la seguridad de la información, incluida la inyección SQL, de la misma manera owasp top 10 en su lista de las 10 amenazas web más importantes, se encuentra el SQL injection como una de ellas, detalla cómo detectar y prevenir la inyección SQL con buenas prácticas para protegerse contra esta amenaza.

Se recomienda considerar los siguientes aspectos: validar y filtrar todas las entradas de usuario antes de procesarlas para evitar la inyección SQL y otros tipos de inyección; utilizar la parametrización de consultas en lugar de construir consultas dinámicas concatenando valores de entrada, que pueden ser manipulados por un atacante, llevar un registro detallado de todas las actividades de la base de datos, incluidas las consultas y transacciones, para detectar cualquier actividad sospechosa., implementar firewalls y soluciones de seguridad para proteger la infraestructura de base de datos contra ataques externos.

Comentario de la Administración

1.4.14. SEGURIDAD DE CONTRASEÑAS

Tras realizar ingeniería social, se capturaron credenciales de usuarios registrados en el aplicativo, donde se observó que utilizan contraseñas débiles que les asignan en el registro, estos usuarios no han actualizado la contraseña lo que los hace susceptibles a robo de sesión por medio de ataques de diccionario, fuerza bruta o phishing.

Si cuentan con opción de cambio de contraseña donde se establecen requisitos para crear una contraseña segura, pero no es una exigencia, los usuarios pueden saltar ese paso.

El estándar de seguridad NIST SP 800-63B en la sección de la gestión de la autenticación y los requisitos de seguridad para la autenticación de usuarios, brinda políticas de fortalecimiento de contraseñas para proteger la información y garantizar la confidencialidad de los usuarios.

Adicionalmente ISO 27001 para la gestión de la seguridad de la información, proporciona una guía para la implementación de controles de seguridad, incluidos los controles de autenticación.

Se recomienda emplear políticas y buenas prácticas como establecer una longitud mínima de al menos 8 caracteres para las contraseñas, que sean complejas, es decir, que contengan una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, prohibición de contraseñas comunes como "password123", "admin", “12345678”, verificación de contraseñas para detectar y bloquear ataques de fuerza bruta y otros tipos de ataques contra la seguridad de las contraseñas y renovación de contraseñas con cierta frecuencia, para reducir el riesgo de compromiso de las contraseñas como exigencia mas no como una opción.

Comentario de la Administración

GLOSARIO DE TERMINOS

COBIT 5.0: un marco de gobierno de tecnología de la información que proporciona una guía para la gestión de TI y la entrega de servicios de TI de manera efectiva y eficiente.

ISO/IEC 27001: un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) para ayudar a las organizaciones a proteger sus datos y sistemas.

Web Content Accessibility Guidelines (WCAG): son una serie de pautas publicadas por la W3C (World Wide Web Consortium) para garantizar que el contenido de la web sea accesible para todas las personas, incluyendo personas con discapacidades.

NIST SP 800-53: es un estándar de seguridad de la información publicado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Establece un conjunto de controles de seguridad y privacidad para sistemas de información federales y organizaciones.

X-Frame-Options: es un encabezado HTTP de seguridad que se utiliza para proteger contra ataques de clickjacking. Indica al navegador si debe permitir que un sitio web sea incrustado dentro de un iframe.

X-XSS-Protection: es un encabezado HTTP de seguridad que ayuda a proteger contra ataques de XSS (cross-site scripting). Activa un filtro de XSS en el navegador del usuario para evitar que se ejecute código malicioso.

Autenticación de dos factores: método de autenticación que requiere dos formas diferentes de verificar la identidad de un usuario, como una contraseña y un código de acceso único enviado a un dispositivo móvil.

Ataque DDOS: un ataque de denegación de servicio (DOS) es un intento de sobrecargar un servidor o red con tráfico inútil o malicioso

Ataque XSS: tipo de ataque informático en el que un atacante inyecta código malicioso en una página web para robar información o tomar el control de un sitio web.

Cookies: archivos pequeños que se almacenan en el navegador web del usuario y se utilizan para rastrear la actividad del usuario en un sitio web y personalizar su experiencia.

Diseño responsivo: enfoque de diseño web que se adapta automáticamente a diferentes tamaños de pantalla y dispositivos para proporcionar una experiencia de usuario óptima.

Flags de seguridad: valores que se establecen en el sistema operativo o en una aplicación para controlar el acceso y la seguridad, como permisos de usuario, contraseñas y políticas de seguridad.

Formularios de entrada de datos: campos que se utilizan en una página web o aplicación para recopilar información del usuario, como nombre, dirección, correo electrónico o contraseña.

GitHub: plataforma de alojamiento de código fuente y gestión de versiones que permite a los desarrolladores colaborar en proyectos de software.

HTML: lenguaje de marcado utilizado para crear páginas web y aplicaciones que se muestran en un navegador web. Permite definir la estructura y el contenido de una página web mediante etiquetas y atributos.

HTTP: Protocolo de transferencia de hipertexto. Es el protocolo utilizado para la transferencia de datos en la web.

HTTPS: Protocolo de transferencia de hipertexto seguro. Es una versión cifrada y segura del protocolo HTTP que utiliza SSL / TLS para proteger los datos transferidos.

Iframes: etiquetas HTML que permiten incrustar una página web dentro de otra. Se utilizan a menudo para mostrar contenido de terceros en una página.

Inyección SQL: un tipo de ataque de seguridad informática en el que un atacante inserta código SQL malicioso en una entrada de datos para manipular una base de datos.

JavaScript: un lenguaje de programación utilizado para crear aplicaciones web interactivas y dinámicas en el navegador del usuario. Es ampliamente utilizado para agregar funcionalidad a sitios web y aplicaciones.

NPM: es un gestor de paquetes para el lenguaje de programación JavaScript. Permite a los desarrolladores compartir y reutilizar código en sus proyectos.

OWASP: es un proyecto de código abierto que se enfoca en mejorar la seguridad de las aplicaciones web. Publica una lista de los 10 riesgos de seguridad más críticos que

enfrentan las aplicaciones web y proporciona herramientas y recursos para ayudar a los desarrolladores a proteger sus aplicaciones.

Servidores proxy: es un servidor i que actúa como intermediario entre un cliente y otro servidor. Un servidor proxy puede utilizarse para ocultar la dirección IP del cliente, aumentar la seguridad, acelerar la navegación y filtrar contenido.

SQLmap: es una herramienta de prueba de penetración de código abierto que automatiza la detección y explotación de vulnerabilidades de inyección SQL en aplicaciones web.

URL: Uniform Resource Locator. Es la dirección que se utiliza para acceder a un recurso en la web. La URL incluye el protocolo, el nombre de dominio y la ruta al recurso.

Anexo 20. Checklist

Aspecto a considerar	Cumple		Observación
	Si	No	
¿Existe validación de número de cédula?		**X**	Permite ingreso de cualquier dato
¿Existe validación en el formulario de almacenamiento de entradas en null?	**X**		
¿Existe validaciones en el ingreso de fechas según rango de edades adecuadas?		**X**	
¿Hay generación automática de número de matrícula?	**X**		
¿Se comprueba datos registrados en el sistema?	**X**		
¿Se verifica la cuenta de correo electrónico?		**X**	No exige que el ingreso de email cumpla con el formato adecuado
¿El promedio se genera de forma automática?	**X**		
¿Se refleja el estado de parciales?	**X**		
¿Tienen establecido un rango de notas?	**X**		
¿Tienen establecido calificación con decimales?	**X**		
¿Se deshabilitar opciones del proceso matrícula cuando el estado de la solicitud esta reprobado?	**X**		
¿Hay requisitos para la creación de contraseñas seguras?	**X**		
¿Se cumple con los requisitos de contraseñas seguras?		**X**	
¿Se solicita confirmación de contraseña nueva?	**X**		
¿Hay correcta codificación de variables string en formulario de matriculación?		**X**	Permite inserción de script malicioso
¿Hay correcta codificación de variables string en módulo ingreso de notas?	**X**		
¿Existe manual de usuario?		**X**	No, cuentan con video tutoriales
¿Emplean codificación de caracteres especiales?	**X**		
¿Existe configuración para protección de ataque Ddos?	**X**		
¿Tienen definido la configuración de protección ante clickjacking?		**X**	El servidor no tiene definido el encabezado X-Frame-Options anticlicjacking
¿Tienen definido la configuración de protección XSS?		**X**	El aplicativo web no tiene definido en el encabezado protección XSS
¿Los usuarios cambian la contraseña asignada por defecto en el registro?		**X**	Muchos usuarios, no cambian ka contraseña asignada en el registro

Anexo 21. Permiso de la intitución

ESCUELA DE EDUCACIÓN BASICA
"ARBOL DE VIDA"
Salinas - J. L. Tamayo Barrio Vinicio yagual 1
Cel 0998199919

Sr. Ing.
José Sánchez Aquino
DIRECTOR DE LA CARRERA TECNOLOGÍAS DE LA INFORMACIÓN

De mis consideraciones.

Una vez solicitado el permiso correspondiente para realizar **la AUDITORÍA INFORMÁTICA PARA EVALUAR LA SEGURIDAD DEL APLICATIVO** en nuestra institución educativa por parte de la estudiante Kenya Gissell Mejillón González con C. I. 2450134263 , cúmpleme informar la respectiva autorización para que se realice esta labor relacionada a su titulación profesional.

J. L. Tamayo, 5 de agosto del 2022

ESCUELA DE EDUCACIÓN BÁSICA "ARBOL DE VIDA" SECRETARIA J.L. TAMAYO - SALINAS

Lcdo. Douglas Maldonado Calcedo Msc
Director
C. I. # 0908440654