UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD: EXÁMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

"Análisis de seguridad controlado en aplicaciones web de una institución financiera utilizando herramientas de ciberseguridad y buenas prácticas de OWASP"

AUTOR
ANA LUISA CARVACA ORRALA

PROFESOR TUTOR
ING. IVAN CORONEL SUAREZ, MSIA

LA LIBERTAD – ECUADOR
2022

AGRADECIMIENTO

Agradezco a la Universidad Estatal Península de Santa Elena y a los docentes que formaron parte de mi desarrollo académico.

A la Institución Financiera por la confianza y permitirme realizar mi proyecto de titulación.

A mi mamá, Ana Isabel, quien me acompañó durante toda mi carrera y se encargó de hacerme la vida más fácil para que pueda estudiar. ¡GRACIAS! TE AMO.

A mi Tío y jefe Lcdo. José Orrala Peña, aunque ya no te encuentres con nosotros no puedo dejar de agradecerte por permitirme trabajar y aprender de ti durante estos años.

Ana Luisa Carvaca Orrala

DEDICATORIA

Dedico este trabajo a mi abuelita Ilsia Emilia, a quien he extraño todos los días desde su partida, y me llena de tristeza no compartir este momento con ella.

A mi abuelito Miguel, quien me ha amado como una hija, a mis padres Ana y Luis, y hermanos Freddy, Evelyn, Diana y Yuliana.

Ana Luisa Carvaca Orrala

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación denominado: **"Análisis de seguridad controlado en aplicaciones web de una institución financiera utilizando herramientas de ciberseguridad y buenas prácticas de OWASP"**, elaborado por la estudiante Carvaca Orrala Ana Luisa, de la carrera de Tecnologías de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.

La libertad, agosto del 2022

…….

Ing. Iván Coronel Suárez, MSIA.

TRIBUNAL DE GRADO

Ing. Jaime Orozco, Mgt.

DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Iván Coronel Suárez, MSIA

PROFESOR TUTOR

Lsi. Daniel Quirumbay, MSIA

PROFESOR DE ÁREA

Ing. Marjorie Coronel, Mgt

DOCENTE GUÍA

RESUMEN

El presente trabajo de titulación está dedicado al departamento de Tecnologías de la Información de una Cooperativa de Ahorro y Crédito, la cual no ha sometido a sus aplicaciones web a un análisis de seguridad. Por esta razón fue importante ejecutar un análisis de vulnerabilidades que le permita conocer el riesgo al que está expuesta. Para el desarrollo de este trabajo se utilizó principalmente el Top 10 de OWASP 2021 el cual es una lista de los diez riesgos más importante en las aplicaciones web, y se complementó con la guía de pruebas de seguridad de aplicaciones web v4.2 de OWASP que brinda varias metodologías utilizadas en este proyecto, tales como: la guía de pruebas de penetración, la guía de valoración de riesgos y la guía de escritura de informes. Luego del análisis se descubrió que las aplicaciones web de la institución son vulnerables a cinco de los diez riesgos de seguridad del Top Ten.

Palabras clave: Análisis, aplicaciones web, OWASP Top 10, riesgos, seguridad.

ABSTRACT

This degree work is dedicated to the Information Technology department of a Savings and Credit Cooperative, which has not submitted its web applications to a security analysis. For this reason, it was important to perform a vulnerability analysis that allows to know the risk to which it is exposed. For the development of this work we mainly used the OWASP Top 10 2021, which is a list of the ten most important risks in web applications, and was complemented with the OWASP Web Application Security Testing guide v4.2, which provides several methodologies used in this project, such as: the penetration testing guide, the risk assessment guide and the report writing guide. After the analysis it was found that the institution's web applications are vulnerable to five of the Top Ten security risks.

Keywords: Analysis, Web applications, OWASP Top 10, risks, security.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Firmado electrónicamente por:
ANA LUISA CARVACA

Ana Luisa Carvaca Orrala

TABLA DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

La finalidad de este trabajo fue analizar las vulnerabilidades a las que están expuestas las aplicaciones web de la Cooperativa de Ahorro y Crédito en base la lista del Top Ten de OWASP en su versión del año 2021. Se realizaron pruebas de penetración tanto manuales y con herramientas automatizadas bajo un ambiente controlado. Como resultado final se redactó un informe con los riesgos encontrados con su nivel de severidad y recomendaciones para mitigarlos.

En el capítulo 1. se detalla información que nos permite entender la problemática de la entidad financiera y la solución planteada. Además, encontrará los antecedentes, descripción del proyecto, los objetivos generales y específicos, justificación y alcance.

En el capítulo 2. encontrará el marco teórico en el que se abordaran temas y conceptos que permitan entender mejor el contexto del proyecto, también se muestra la metodología elegida para desarrollar el proyecto y las técnicas de recolección de información empleadas.

En el capítulo 3. Se hace el desarrollo práctico, esto implica la especificación de los requerimientos del proyecto, las pruebas de penetración pasivas y activas, la valoración de los riesgos de las vulnerabilidades encontradas y la redacción del informe final.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1. ANTECEDENTES

En un informe anual realizado por el equipo de investigación y análisis de Kaspersky revela el aumento de un 24% en ciberataques en latinoamérica durante los primeros ocho meses del año 2021 en comparación con el año 2020. Según Kaspersky, Ecuador ha registrado un aumento del 75% en la tendencia de crecimiento en ciberataques [1], y el 5% en ataques de tipo ransomware durante el año 2021 [2]. Una investigación realizada por el instituto Ponemon sobre los riesgos de seguridad de las aplicaciones empresariales indica que las empresas encuestadas coinciden en un 38% que los mayores ataques de seguridad van dirigidos a la capa de aplicación, sin embargo, la inversión dedicada para cubrir este riesgo es tan solo del 17% [3].

El sector financiero tiene mayor índice de digitalización, ya que diariamente incrementa el número de usuarios que realizan transacciones a través de internet y dispositivos móviles, buscando aprovechar las ventajas de la tecnología que tienen como consecuencia el surgimiento de nuevos riesgos que se deben prevenir para evitar posibles ataques o situaciones que exponen la seguridad de las entidades financieras y de sus usuarios [4, p. 17]. Todas estas instituciones deben garantizar que son lo suficientemente resilientes, teniendo recursos técnicos, mecanismos de defensa y personal capacitado.

El 72.42% de los usuarios de servicios bancarios prefieren realizar sus transacciones a través de Internet. Sin embargo, solo el 60% de las entidades Bancarias de América latina y el Caribe demuestran que tienen apoyo por parte de la alta dirección hacia la gestión de riesgos de seguridad, y solo el 65% exige la adopción de buenas prácticas de ciberseguridad [4, pp. 7,120]. Según la Organización de los Estados Americanos OEA muestra como resultado que el 67% del grupo denominado “Bancos pequeños” no están implementando herramientas, controles o procesos usando tecnologías digitales emergentes para garantizar la seguridad de la información [4, p. 10].

Este trabajo estará dirigido a una institución ecuatoriana denominada como una Cooperativa de Ahorro y Crédito que provee productos y servicios financieros a más de 35.000 usuarios, contando con agencias en varias ciudades del país. Pertenece al segmento 2 de las entidades del sector Financiero Popular y Solidario.

Son cooperativas de ahorro y crédito las formadas por personas naturales o jurídicas con el vínculo común determinado en su estatuto, tiene como objetivo la realización de las operaciones financieras, debidamente autorizadas por la Superintendencia, exclusivamente con sus socios [5]. Pertenecen al segmento dos las entidades del sector financiero popular y solidario las instituciones que según el tipo y saldo de sus activos mayores a 20'000.000,00 hasta 80'000.000,00 dólares [6].

Sus organismos de control son la Superintendencia de Economía Popular y Solidaria SEPS la cual es un organismo técnico de supervisión y control de las entidades del sector Financiero Popular y Solidario [7]; la Corporación del Seguro de Depósitos CODESE, es una institución que protege los recursos de los usuarios del sistema financiero nacional y de seguros privados [8]; y el Banco Central del Ecuador BCE que es una persona jurídica de derecho público y forma parte de la Función Ejecutiva de duración indefinida con autonomía institucional, administrativa, presupuestaria y técnica [9].

En la observación realizada (Ver anexo 1) se pudo destacar que la institución financiera cuenta con un sitio web que permite a sus asociados realizar diferentes tipos de transacciones en sus servicios en línea, tales como: solicitud de transferencia, solicitud de tarjeta de débito, solicitudes de créditos, formulario de reclamo y un buzón de comentarios. Cada uno de estos servicios se realizan mediante un formulario disponible directamente en el sitio web sin necesidad de iniciar sesión previamente. Tanto el formulario de solicitud de transferencia, el formulario de solicitud de tarjeta de crédito, y el formulario de solicitud de crédito no cuentan con métodos que validen los datos que los usuarios ingresan al formulario.

Aunque estos servicios cumplen con las funciones por las que fueron desarrollados, es totalmente diferente a las aplicaciones web de los bancos más grandes país, ya que

permite realizar transacciones sin previo acceso a una cuenta personal pudiendo ser un punto débil ante ciberdelincuentes provocando graves perjuicios económicos [10].

También cuenta con una aplicación web que permite realizar transacciones a sus asociados con credenciales de acceso personales, sin embargo, la página de inicio de sesión no cuenta con las suficientes medidas de ciberseguridad, lo cual podría ser un blanco fácil ante ataques automatizados. Incluso los mensajes para el inicio de sesión incorrecta evidencian los nombres de las tablas de la base de datos pudiendo permitir ataques de inyección. Según la OEA el robo de bases de datos crítica, el compromiso de credenciales de usuarios privilegiados y la pérdida de datos son riesgos de seguridad digital que merecen la mayor atención por parte de las entidades bancarias [4].

Adicionalmente, en la entrevista realizada al jefe del departamento de TI de la institución (Ver anexo 2) se identificó que; aunque siguen el estándar ISO 27001 que es una norma internacional sobre la gestión de la seguridad de la información [11], no se ha realizado un análisis de vulnerabilidades enfocado a las aplicaciones web de la empresa. Además, no cuentan con el suficiente presupuesto, personal especializado, y área independiente para la gestión de seguridad de la información, esto se debe a que la normativa expedida por la Superintendencia de Economía Popular y Solidaria no lo exigía anteriormente, es por esta razón que la empresa no atendía esta necesidad, forzando al departamento de TI a auto especializarse para poder cubrir la seguridad de la información de la empresa.

En un trabajo realizado en la Universidad de Ciencias aplicadas de Turku en Finlandia, se evaluó la seguridad de la aplicación web del comisionado bajo el marco de OWASP top 10, en el que se pudo detectar vulnerabilidades de autenticación rota y uso de componentes y bibliotecas con vulnerabilidades conocidas [12]. Pese a que se obtuvo buenos resultados con el uso del software Burp Suite que incluye varias herramientas automáticas y manuales para realizar pruebas de seguridad de aplicaciones web [13], esto no garantiza que el estudio se hizo de forma exhaustiva. Por esta razón en este trabajo se utilizarán varias herramientas de software libre específicas para las pruebas de cada riesgo del Top Ten de OWASP sobre la aplicación web de la entidad financiera de estudio y así realizar un correcto análisis de vulnerabilidades.

En Ecuador, estudiantes de la universidad de las fuerzas armadas realizaron un análisis de riesgos de las aplicaciones web de la Superintendencia de Bancos y Seguros, bajo las recomendaciones del Top Ten de OWASP 2010 donde se evaluaron tres sistemas, el Sistema de Población de Identificadores SPI, el Sistema de Auditoria de Prevención de Lavado de Activos SAPLA y el Sistema para Otorgar Credenciales a Intermediarios de Seguros SOCI, pudiendo detectar los riesgos de Almacenamiento Criptográfico Inseguro, y Protección insuficiente en la capa de transporte [14]. Sin embargo, el OWASP Top Ten del año 2010 actualmente se considera obsoleto ya que las tecnologías y riesgos van cambiando y evolucionando [15]. Por esta razón se trabajará bajo el marco de OWASP Top Ten del año 2021, que es un marco totalmente actualizado sobre las diez vulnerabilidades críticas de las aplicaciones web.

Un análisis de riesgos de la plataforma web transaccional de la Cooperativa de Ahorro y Crédito Jardín Azuayo realizado bajo la Norma ISO 27001 permitió identificar riesgos y amenazas dentro de la plataforma. Aunque la matriz de riesgos realizada muestra riesgos de nivel medio y alto no se puede afirmar que se realizó el estudio de forma exhaustiva, ya que no se emplearon herramientas especializadas de seguridad para realizar el análisis de riesgos, y tampoco se ejecutaron pruebas internas, solo fue un análisis superficial con el rol de un usuario de la cooperativa [16].

El sector financiero es uno de los mayores objetivos para los ciberdelincuentes [4], por lo que es necesario implementar medidas para enfrentar riesgos de ciberseguridad y salvaguardar la seguridad de la información que éstas poseen. Por esta razón se propone realizar un análisis de seguridad basado en una de las listas se riesgos de seguridad más importantes a nivel mundial como es el Top Ten de OWASP 2021 para conocer las vulnerabilidades a las que se expone la institución financiera y sus usuarios.

1.2. DESCRIPCIÓN DEL PROYECTO

El proyecto abierto de seguridad de aplicaciones web, o más conocido como OWASP por sus siglas en inglés, es una fundación sin fines de lucro que trabaja para mejorar la seguridad de aplicaciones web; ofrece a toda su comunidad proyectos, herramientas,

documento, foros y capítulos totalmente gratuitos [17]. Cuenta con una lista de importantes proyectos desarrollados con diferentes empresas a nivel mundial, entre los más destacados tenemos al Top Ten de OWASP que es un informe que describe los diez riesgos de seguridad más críticas de las aplicaciones web, elaborado por un equipo de expertos en ciberseguridad de todo el mundo basado en datos analizados provenientes de varias organizaciones [17].

Las diez categorías son:

F2.A01: 2021-Control de Acceso Roto: con este control se busca corregir fallas en la divulgación de información no autorizada, modificación, destrucción de la información o que terceros realicen acciones fuera de los límites permitidos [18].

F2. A02: 2021-Fallos de Cifrado: se enfocan en fallas o ausencia de cifrado, la cual conduce a la exposición de datos sensibles. Busca que las aplicaciones web protejan correctamente los datos sensibles de los usuarios que pueden ser robados y utilizados para fines maliciosos. Requiriendo métodos de protección adicionales como cifrado en almacenamiento o tránsito, y va acompañado de las regulaciones, leyes o requisitos de la institución y del país, en este caso la Ley Orgánica de Protección de Datos Personales [19].

F2. A03: 2021-Inyección: se buscan fallas de inyección, ocurre cuando un parámetro de la aplicación web permite incrustar comandos maliciosos y engañar al intérprete para acceder a la base de datos [20].

F2. A04: 2021-Diseño Inseguro: es una nueva categoría que se añadió a esta lista y se enfoca en los riesgos relacionados con la arquitectura y diseño de las aplicaciones web. No se debe confundir fallas de diseño con los defectos de implementación ya que se puede tener un diseño inseguro que no será solucionado con una buena implementación, o un diseño seguro no se arregla con una implementación correcta [21].

F2. A05: 2021-Configuración de Seguridad Incorrecta: subió un puesto en comparación con la lista del Top Ten del año 2017. Se pueden encontrar configuraciones de seguridad incorrectas cuando se habilitan o instalan funciones innecesarias [22].

F2. A06: 2021-Componentes Vulnerables y Obsoletos: se pueden presentar vulnerabilidades de este tipo cuando no se conoce todas las versiones de los componentes que se utilizan, si el software es vulnerable, no es compatible o no está actualizado, no se prueban la compatibilidad de las bibliotecas actualizadas o parcheadas [23].

F2. A07:2021- Fallas de Identificación y Autenticación: anteriormente llamada "Autenticación Rota" y actualmente incluye enumeraciones de debilidades comunes (CWE) [24] relacionados con fallas de identificación. Pueden existir debilidades de autenticación si la aplicación permite ataques automatizados, credenciales de acceso predeterminadas o conocidas, o procesos de recuperación de credenciales débiles, autenticación multifactorial ineficiente o inexistente [25].

F2. A08:2021-Fallas de Software e integridad de Datos: es una nueva categoría dentro de la lista, están relacionados con la infraestructura y el código que no protegen contra violaciones de integridad. Se enfoca en hacer suposiciones relacionadas con actualizaciones de software, datos críticos y canalizaciones de CI /CD sin verificar la integridad [26].

F2. A09:2021-Fallas de Registro y Monitoreo: es fundamental detectar y responder infracciones de seguridad; ayuda a detectar, escalar y responder las infracciones activas [27].

F2. A10:2021-Falsificación de solicitudes del lado del servidor: ocurren cuando una aplicación web está obteniendo un recurso remoto sin validar la URL proporcionada por el usuario. Permite que un atacante coaccione a la aplicación para que envíe una solicitud diseñada a un destino inesperado, incluso cuando está protegido por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL) [28].

El presente trabajo estará dirigido al departamento de TI de una Institución financiera, busca analizar las vulnerabilidades críticas que exponen la seguridad de las aplicaciones web de la institución, realizando pruebas de seguridad bajo el marco de OWASP Top Ten 2021. Las pruebas de seguridad de aplicaciones web se dedican a evaluar únicamente la seguridad de una aplicación web, implica un análisis activo de la aplicación en busca de debilidades, fallas técnicas o vulnerabilidades. Todo problema identificado deberá ser presentado al propietario del sistema mediante un informe final que contiene la valoración de riesgos y recomendaciones para mitigarlos [29]. Este análisis comprenderá las siguientes fases:

FASE 1. PRUEBAS PASIVAS

- A través de técnicas y herramientas de análisis de seguridad recolectar la información necesaria.

- Identificar posibles riesgos de seguridad en la aplicación web y los puntos de acceso por las que un intruso podría ingresar al sistema.

FASE 2. PRUEBAS ACTIVAS

Realizar pruebas con técnicas y herramientas especializadas para detectar si la aplicación web de la institución es vulnerable a los diez riesgos más comunes de las aplicaciones web, y comprenderá las siguientes fases:

- **F2. PA01: Recopilación de información:** Esta categoría contiene diez pruebas para realizar la recopilación de información, aquí se pretende detectar fugas de información sensible sobre la aplicación web [30]. Las pruebas de esta fase aparte de recopilar información, permite evaluar la existencia de componente vulnerables o desactualizados correspondiente al sexto riesgo de seguridad del Top Ten.

- **F2. PA02: Pruebas de gestión de configuración e implementación:** Esta categoría contiene once pruebas de penetración para comprobar si existen vulnerabilidades

provocadas por una mala configuración o implementación de componentes en la aplicación web [30]. Estas pruebas permiten evaluar la existencia de configuraciones de seguridad incorrectas correspondiente al quinto riesgo de seguridad del Top Ten.

- **F2. PA03: Pruebas de gestión de identidad:** Esta categoría contiene cinco pruebas que permitirán comprobar si existe una mala gestión en la identificación de roles o usuarios [30]. Estas pruebas permiten evaluar la existencia de fallas de integridad de datos correspondiente a la séptima categoría del Top Ten.

- **F2. PA04: Pruebas de autenticación:** Esta categoría contiene diez pruebas de seguridad para comprobar si los mecanismos de autenticación de la aplicación web son lo suficientemente fuertes [30]. Estas pruebas permiten evaluar la existencia de fallas de autenticación correspondiente a la séptima categoría del Top Ten.

- **F2. PA05: Pruebas de autorización:** Esta categoría contiene cuatro pruebas para comprobar la existen fallas de autorización en la aplicación web [30]. Esta prueba hace referencia al control de acceso roto correspondiente a la primera categoría del Top Ten.

- **F2. PA06: Pruebas de validación de entrada:** Esta categoría contiene diecinueve pruebas para validar entradas, van desde pruebas de falsificación de solicitudes al servidor y pruebas de inyección [30]. Permiten evaluar la existencia de Fallas de inyección y falsificación de solicitudes del lado del servidor, correspondientes a las categorías tres y diez del Top Ten.

- **F2. PA07: Manejo de errores:** Esta categoría abarca dos pruebas de seguridad para comprobar la existencia de un inadecuado manejo de errores en la aplicación web [30]. Esta prueba permite evaluar la existencia de un diseño inseguro, correspondiente a la cuarta categoría del Top Ten.

- **F2. PA08: Pruebas de cifrado débil:** Contiene cuatro pruebas que permiten comprobar si existe un cifrado débil [30], estas pruebas permiten identificar la

existencia de fallas criptográficas, correspondiente a la segunda categoría del Top Ten.

- **F2. PA09: Fallas de integridad de datos y software:** Esta categoría es la octava del top ten y no forma parte de la metodología de pruebas de penetración propuesta por OWASP, fue añadida para poder evaluar esta vulnerabilidad y sus pruebas serán basadas en el informe y CWE mapeados en la documentación del OWASP Top Ten 2021.

- **F2. PA10: Fallas de registro y monitoreo de seguridad**: Esta categoría es la novena de la lista del top ten y no forma parte de la metodología de pruebas de penetración de OWASP, sin embargo, fue añadida y para evaluarla se basó en la lista de los CWE mapeados para esta categoría en la documentación del OWASP Top Ten 2021.

FASE 3. INFORME FINAL

Desarrollado en dos fases:

F3. IF01: VALORACIÓN DE RIESGOS

Se utilizó la guía de valoración de riesgo propuesto en la guía de pruebas de seguridad de aplicaciones web de OWASP v3.0, el modelo estándar para calcular el riesgo es:

Riesgo= Probabilidad de ocurrencia * Impacto

La metodología de OWASP descompone la valoración de riesgos en 6 pasos descritos a continuación.

PASO 1. IDENTIFICANDO UN RIESGO

Para poder identificar un riesgo de seguridad que necesita ser valorado se debe recopilar información sobre los agentes causantes de la amenaza y la vulnerabilidad involucrada [31].

PASO 2. FACTORES PARA ESTIMAR LA PROBABILIDAD DE OCURRENCIA

La probabilidad de ocurrencia es una medida aproximada de que una vulnerabilidad sea explotada por un atacante [31]. No es necesario ser precisos, por lo que se puede identificar con valores de probabilidad alta, media y baja. Cada factor cuenta con un conjunto de opciones, cada opción cuenta con una valoración que va del 0 al 9 de acuerdo con su probabilidad de ocurrencia, estas cifras se emplearán más adelante para estimar la probabilidad de ocurrencia global [31].

- **Factores que afectan a la vulnerabilidad:** Tiene como objetivo estimar la probabilidad de que la vulnerabilidad sea descubierta y explotada [31].

    - Facilidad de descubrimiento
    - Facilidad de explotación
    - Conocimiento de la vulnerabilidad

PASO 3. FACTORES PARA ESTIMAR EL IMPACTO

El impacto técnico se puede dividir en las tradicionales áreas de la seguridad que son la confidencialidad, integridad, disponibilidad [31]. Su objetivo es valorar el tamaño del impacto si una vulnerabilidad del sistema es explotada.

Así mismo, cada factor cuenta con un conjunto de opciones, cada opción cuenta con una valoración que va del 0 al 9 de acuerdo con el nivel de impacto asociado, estas cifras se emplearán más adelante para estimar el impacto global [31].

- **Factores de impacto técnico**

    - Pérdida de confidencialidad
    - Pérdida de integridad
    - Pérdida de disponibilidad

PASO 4. DETERMINACIÓN DE LA SEVERIDAD DEL RIESGO

Para calcular la severidad global del riesgo es necesario poner en conjunto la probabilidad de ocurrencia estimada y el impacto estimado. Solo se necesita comprender si la probabilidad de ocurrencia y el impacto es alta, media o baja [31]. Se dividirá la escala del 0 al 9 en tres partes.

PROBABILIDAD DE OCURRENCIA Y NIVELES DE IMPACTO	
0 a < 3	BAJO
3 a < 6	MEDIO
6 a <9	ALTO

Tabla 1 Rangos de probabilidad de ocurrencia y niveles de impacto

Método repetitivo: Se utilizará el método repetitivo para seguir un proceso formal para puntuar los factores y calcular el resultado [31].

Determinando la severidad: Para determinar la severidad de un riesgo es necesario combinar la probabilidad de ocurrencia y el impacto [31].

SEVERIDAD DEL RIESGO GLOBAL				
IMPACTO	ALTO	Medio	Alto	Crítico
	MEDIO	Bajo	Medio	Alto
	BAJO	Nota	Bajo	Medio
		BAJO	MEDIO	ALTO
	PROBABILIDAD DE OCURRENCIA			

Tabla 2 Severidad del riesgo global

PASO 5. DECIDIENDO QUE ARREGLAR

Como regla principal, se debe atender primero los problemas que hayan obtenido una puntuación severa para poder reducir significativamente el riesgo global [31]. Es importante recordar que no todos los riesgos merecen la pena ser atendidos, algunos pueden llegar a ser justificables si se basa en el costo para solucionar dicha incidencia.

PASO 6. AJUSTANDO TU MODELO DE VALORACIÓN DEL RIESGO

Este modelo se puede ajustar a las necesidades del negocio, se puede añadir factores que representen mejor la organización, personalizar opciones asociadas a cada factor o ponderar factores asignando un peso para enfatizar a aquellos que se consideren más significativos.

F3 IF02: REDACCIÓN DE INFORME FINAL

Para la redacción del informe final se utilizará la guía de escritura de informes propuesta por OWASP en la guía de pruebas de seguridad de aplicaciones web 4.0 que mantiene la siguiente estructura:

1. INTRODUCCIÓN

1.1.CONTROL DE VERSIONES

Es un registro en una tabla para llevar el control de los cambios realizados al informe final.

1.2.TABLA DE CONTENIDO

Es una página que enliste el contenido del documento.

1.3.EL EQUIPO

Una lista de los miembros del equipo detallando su experiencia y calificaciones.

1.4.ALCANCE

Son los límites y las necesidades del compromiso acordado con la organización.

1.5.LIMITACIONES

Las limitaciones con los impedimentos que se presentaron a lo largo del desarrollo del proyecto.

1.6.CRONOLOGÍA

La duración del compromiso.

2. RESUMEN EJECUTIVO

Contiene el objetivo de la prueba, los hallazgos claves y las recomendaciones técnicas

3. HALLAZGOS

Esta sección está dirigida al equipo técnico, debe incluir toda la información necesaria para comprender la vulnerabilidad

3.1. RESUMEN DE HALLAZGOS

Una lista de los hallazgos con su nivel de riesgo

3.2. DETALLES DE LOS HALLAZGOS

Descripción detallada de qué es la vulnerabilidad, cómo explotarla y los dalos de su explotación.

Las herramientas que se utilizaron para el desarrollo del proyecto son:

Brup Suite Community Edition: Es una aplicación de con un kit de herramientas de prueba dinámica diseñado para realizar pruebas de escaneo de vulnerabilidades, entre los principales incluye un Proxy HTTP(s)/ WebSocketsm repetidores, decodificadores y un Burp Intruso de demostración [32].

Censys: Esta herramienta muestra información de equipos, servidores o de cualquier dispositivo conectado a internet, muestra la dirección IP pública y de más información disponible en internet sobre el objetivo de la búsqueda [33].

Duck Duck Go: Es una empresa de privacidad en Internet que le permite tomar el control de su información personal en línea sin inconvenientes, sin hacer concesiones. Ofrece respuestas más acertadas para las búsquedas realizadas [34].

Google Hacking: Es una poderosa técnica de piratería de Google, indexa implacablemente mensajes de error, archivos otra información útil en directorios vulnerables de sitios web [35].

Kali Linux: Es una distribución de GNU/Linux, contiene herramientas destinadas a realizar auditoria, y seguridad informática y proteger ante posibles ataques [36]

Nmap: Es una herramienta de código abierto para la exploración de vulnerabilidades y la detección de redes [37]**.**

OWASP ZAP: Es un escáner web de vulnerabilidades que permite auditar diferentes aplicaciones web. Permite comprobar las peticiones y respuestas entre cliente y servidor, levanta un proxy que se encargará de capturar todas las peticiones para su posterior estudio [38].

WhoIs: Es una herramienta de búsqueda de información de propietarios de nombres de dominio, sitios web, y direcciones IP [39].

La línea de investigación a la que aportará este proyecto es Tecnologías y Sistemas de la Información (TSI) y está ligada a las sub líneas de investigación TSI en las organizaciones y en la sociedad; Ingeniería y gestión de TSI [40].

1.3. OBJETIVOS DEL PROYECTO

1.3.1. OBJETIVO GENERAL

Elaborar un informe de los riesgos de seguridad encontrados basado en la guía de escritura de informes de OWASP.

1.3.2. OBJETIVOS ESPECÍFICOS

- Adaptar la metodología de pruebas de penetración de OWASP, al Top Ten 2021 de OWASP, para obtener una metodología híbrida.

- Identificar los riesgos de seguridad de la aplicación web de la institución financiera con herramientas y técnicas de análisis de seguridad web.

- Valorar los riesgos de seguridad encontrados en las aplicaciones web bajo la Metodología de Valoración de Riesgos OWASP para priorizarlos según su criticidad.

1.4. JUSTIFICACIÓN DEL PROYECTO

La Superintendencia de Economía Popular y Solidaria dentro de las "Recomendaciones para el manejo de información y administración de ciberseguridad en el Sector Financiero Popular y Solidario" [41] establece que las instituciones financieras deben someter a sus sistemas electrónicos al menos una vez al año a una revisión de la seguridad de sus activos mediante ejercicios prácticos y controlados, que simulen varios tipos de amenazas posibles, tales como ethical hacking, pentesting, entre otros; exponiendo a la infraestructura que soporta los servicios de la Entidad a diferentes escenarios de nivel básico a avanzando en medida de lo posible.

Así mismo, dentro de las Normas de Control para las Entidades de los Sectores Financieros Popular y Solidario en el artículo 9.3.2 literal e) las entidades deben garantizar la mitigación de las vulnerabilidades del código fuente de las aplicaciones [42]. De igual manera, la seguridad de la información no está orientada especialmente a proteger los activos de una institución, sino también de la información personal y crítica de sus clientes.

La nueva Ley Orgánica de Protección de Datos Personales establece que los responsables del tratamiento de los datos personales deben implementar todas las medidas de seguridad necesarias para garantizar la seguridad de los datos personales ante cualquier riesgo, amenaza o vulnerabilidad pudiendo adoptar estándares, mejores prácticas, códigos de protección o cualquier otro mecanismo que se considere adecuado para el tratamiento de los datos [43].

Por esta razón se considera que realizar un análisis de seguridad basado en las buenas prácticas de seguridad de aplicaciones web de OWASP Top Ten 2021 ayudará a la institución tener una evaluación real sobre la seguridad de la información de sus aplicaciones web y poder ejecutar acciones correctivas que eviten sufrir incidentes de seguridad y pérdidas de información crítica.

Este análisis permitirá: encontrar las fallas de identificación y autenticación de los usuarios hacia el sistema, verificando si las credenciales de acceso cumplen con las reglas

mínimas de seguridad establecidas; inspeccionar si la aplicación web es vulnerable ante ataques de inyección; corroborar si el diseño de la aplicación y las configuraciones de seguridad estén implementadas de forma correcta; identificar fallas de software e integridad de datos, verificar si cuentan con procedimientos para el monitoreo periódico de accesos, operaciones privilegiadas e intentos de accesos no autorizados; y detectar si el servidor acepta solicitudes de peticiones falsas.

La elaboración de este proyecto contribuye a los objetivos del Plan de Creación de Oportunidades vigente desde el 2021 hasta el 2025 en [44]:

Directriz 1: Soporte territorial para la garantía de derechos
Lineamiento territorial A. Acceso equitativo a servicios y reducción de brechas territoriales.
A4. Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios.
Objetivos del Eje Económico
Objetivo 5. Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social.
Política 5.5 Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población.
Objetivos del Eje Seguridad Integral
Objetivo 10. Garantizar la Soberanía nacional, integridad territorial y seguridad del estado
Política 10.1 Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del ciberespacio y proteger su infraestructura crítica.

1.5. ALCANCE DEL PROYECTO

En base a los problemas identificados en la institución financiera sobre las vulnerabilidades dentro de su aplicación web se propone:

- Análisis de seguridad en las aplicaciones web basado en el marco del OWASP Top Ten 2021 utilizando herramientas de software libre.

- Redactar un informe detallado de las vulnerabilidades encontradas con la valoración de riesgo y recomendaciones para mitigarlos.

Este trabajo está dirigido al departamento de Tecnologías de la Información de una institución financiera. Se utilizará la metodología de pruebas que propone OWASP en su Guía de Pruebas versión 4.0 [31] que consta de dos fases.

En la primera fase llamada "Modo Pasivo" se emplearán herramientas y técnicas que permitan recolectar toda la información necesaria para conocer la lógica de la aplicación. Como resultado de esta fase se espera comprender los puntos de acceso por las que un intruso podría ingresar al sistema.

En la segunda fase llamada "Modo Activo" se empieza a realizar pruebas manuales y con herramientas especializadas para detectar las vulnerabilidades, esta fase estará dividida por diez subcategorías, solo se escogió las categorías que permiten evaluar los diez riesgos de seguridad de OWASP [30]. Se espera obtener como resultado una lista de las vulnerabilidades encontradas.

F2. PA01: Recopilación de información
F2. PA02: Pruebas de gestión de configuración e implementación
F2. PA03: Pruebas de gestión de identidad
F2. PA04: Pruebas de autenticación
F2. PA05: Pruebas de autorización
F2. PA06: Pruebas de validación de entrada
F2. PA07: Manejo de errores
F2. PA08: Criptografía
F2. PA09: Fallas de integridad de datos y software
F2. PA10: Fallas de registro y monitoreo de seguridad

Adicionalmente se añadirá una tercera fase llamada “Informe final” que constará de dos subfases, valoración de riesgos y redacción de informe. En la primera subfase se valorará el riesgo utilizando la Metodología de Valoración de Riesgos de OWASP y se espera obtener como resultado la estimación de severidad del riesgo global de cada una de las vulnerabilidades encontradas. La segunda subfase abarca la redacción del informe final de pruebas en el que se detallarán los resultados obtenidos, y recomendaciones para mitigar dichos riesgos. La estructura y redacción de este informe se basará en la guía de escritura de informes de pruebas de OWASP.

Aunque la institución también cuenta con una aplicación móvil, y la Superintendencia de Economía Popular y Solidaria indique en sus normas la ejecución de pruebas de vulnerabilidades de seguridad en todas las áreas que sean parte de la ejecución de transacciones a través de la banca electrónica [41], este trabajo solo estará enfocado a la aplicación web ya que el OWASP Top Ten analiza riesgos únicamente en aplicaciones web.

CAPITULO II

2. MARCO TEORÍCO Y METODOLOGÍA DEL PROYECTO

2.1. MARCO CONCEPTUAL

2.1.1. SEGURIDAD INFORMÁTICA

Es el conjunto de medidas preventivas, de detección y de corrección, destinadas a proteger la integridad, confidencialidad y disponibilidad de los recursos informáticos [45].

2.1.1.1. CONFIDENCIALIDAD

Busca que la información sensible, privada o secreta no sea revelada a terceros no autorizados, la protección de la confidencialidad se aplica a los datos almacenados durante el procesamiento, mientras son transmitidos o se encuentren en tránsito [46].

2.1.1.1.1. AUTENTICACIÓN

Es la capacidad de demostrar que un usuario o una aplicación es realmente quien dicha persona o aplicación asegura ser [47]. Se conoce como autenticación al proceso de confirmación que un remitente es quien dice ser a la hora de intentar acceder a un sistema, en este proceso intervienen dos partes; remitente y verificador [48, p. 11].

2.1.1.1.2. AUTENTICACIÓN MULTIFACTOR

La autenticación multifactor es una solución robusta de gestión de acceso en que los usuarios deben comprobar su identidad con al menos dos factores de verificación diferentes [49].

2.1.1.1.3. TIPOS DE AUTENTICACIÓN

Autenticación por conocimiento: El remitente facilita información que solo él conoce, por ejemplo, una clave [48, p. 11].

Autenticación por algo poseído: El remitente posee algún objeto que le permite identificar su identidad, como por ejemplo una tarjeta inteligente, una tarjeta de coordenadas o una llave de seguridad USB [48, p. 11].

Autenticación por característica física: El usuario utiliza algún rasgo físico para identificarse, por lo que es necesario implementar algún dispositivo biométrico [48, p. 11].

2.1.1.2. INTEGRIDAD

Información siempre disponible para encontrarse a disposición de personas autorizadas en el momento que la requieran, los sistemas informáticos que almacenan y procesan información deben funcionar correctamente todo el tiempo, evitando interrupciones de servicios ante cualquier situación que se presente [46].

2.1.1.2.1. NO REPUDIO

El no repudio evita que ni el origen ni el destino nieguen la transmisión de un mensaje, cuando se envía un mensaje el receptor es capaz de comprobar que el emisor lo envió y viceversa [50].

2.1.1.3. DISPONIBILIDAD

Garantiza que la información no haya sido manipulada o alterada por usuarios no autorizados, evitando la pérdida de consistencia mientras se almacena, procesa o transmite [46].

2.1.2. CIFRADO DE DATOS

Es la forma de traducir datos de texto original (texto claro) a texto cifrado; los usuarios pueden acceder a los datos cifrados con una clave de cifrado y a los datos descifrados con una clave de descifrado [51]. El cifrado ayuda a garantizar la confidencialidad,

autenticación e integridad, y los algoritmos de cifrados se clasifican en simétricos, asimétricos e híbridos [52].

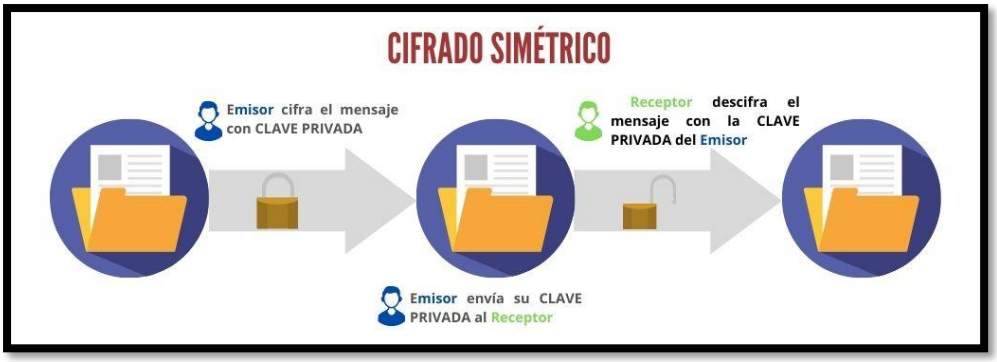


Ilustración 1 Cifrado simétrico [52]

Ilustración 2 Cifrado asimétrico [52]

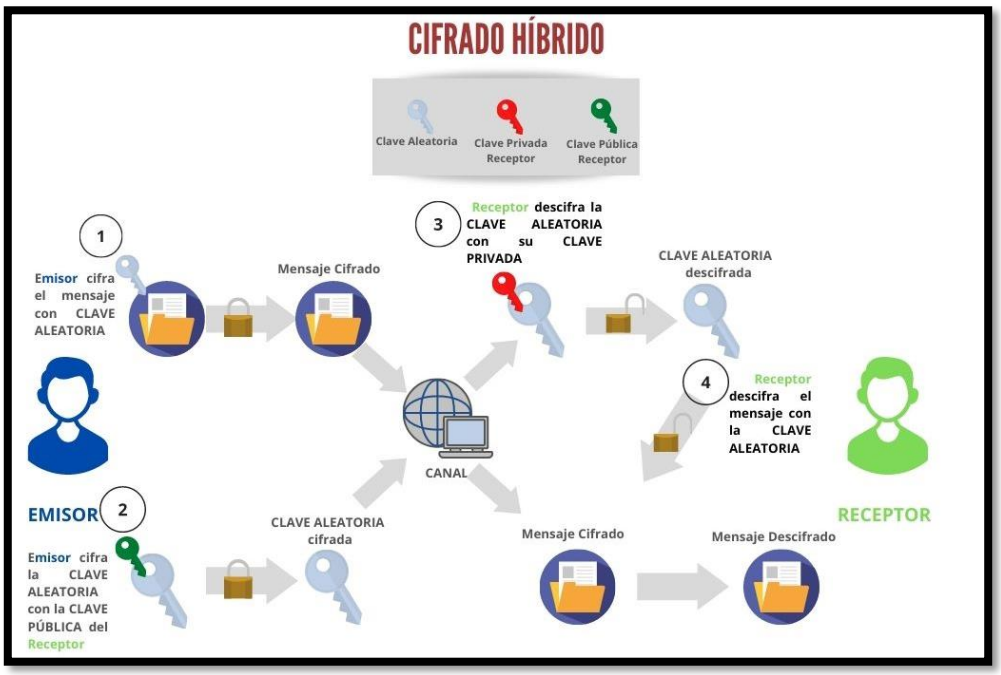


Ilustración 3 Cifrado Híbrido [53]

2.1.3. COMMON WEAKNESS ENUMERATION CWE

Es una lista desarrollada por la comunidad de tipos de debilidades se software y hardware. Sirve como un lenguaje común, una vara de medir para las herramientas de seguridad y como una línea de base para los esfuerzos de identificación, mitigación y prevención de debilidades [54].

2.1.4. SECURITY SOCKETS LAYER SSL

SSL es un protocolo de cifrado diseñado para proporcionar comunicaciones y transferencias de datos seguros a través de internet. Permite a los clientes autenticar la identidad de los servidores mediante la verificación de sus certificados digitales y rechazar las conexiones si el certificado del servidor no es emitido por una autoridad certificadora (CA) de confianza [55].

2.1.5. FINGERPRINTING (TOMA DE HUELLAS DIGITALES)

Las huellas dactilares son características de un objeto que lo hace distinguir de otros objetos similares [56]. La toma de huellas dactilares se define como el proceso de agregar huellas digitales o marcas a un objeto, o de identificar aquellos que ya han sido insertados dentro de un objeto [56].

2.1.6. PENTESTING

El pentesting es una metodología realizada para descubrir vulnerabilidades y/o fallos de seguridad en cualquier entorno informático; está diseñado para clasificar y determinar los alcances y repercusiones de los fallos de seguridad y brindar entornos de posibles alcances de un ataque, además evalúa la eficiencia de la defensa con la que cuentan [57]. Dependiendo del conocimiento del objetivo se dividen en tres tipos; caja blanca, caja negra y caja gris.

2.1.6.1. CAJA BLANCA (WHITE BOX)

Son las pruebas más fáciles de realizar y una de las más completas, puesto que la empresa proporciona toda la información posible sobre la infraestructura tecnológica con el fin de

detectar puntos de fallos o vulnerabilidades potenciales teniendo un tiempo de ejecución más rápido que otro tipo de pruebas [57]. El pentester tiene conocimiento de todo aspecto de seguridad de la entidad como medidas, estructura de red, contraseñas, entre otros [58].

2.1.6.2. CAJA NEGRA (BLACK BOX)

En este tipo de pruebas no se posee ningún tipo de información de los sistemas o infraestructura del objetivo, se simula un ataque de intrusión real sobre los sistemas como si fuera un atacante legítimo para conocer qué tan débil o fuertes se encuentran [57]. En este tipo de pruebas se actúa de forma similar a un ciberdelincuente para tratar de reconocer fallos en la estructura de la red sin causar daños en la empresa [58].

2.1.6.3. CAJA GRIS (GREY BOX)

Es una combinación de las pruebas de caja blanca y caja negra, puesto que se conoce cierta información para poder realizar las pruebas. Es utilizado para identificar vulnerabilidades en sectores determinados. Es más restable y proporciona una estimación más real de las amenazas [57]. El pentester no posee información específica para realizar las pruebas de penetración, por esta razón requiere de tiempo y recursos para identificar la información necesaria acerca de las posibles vulnerabilidades existentes [58].

2.2. MARCO TEÓRICO

2.2.1. LISTAS DE VULNERABILIDADES MÁS COMUNES

2.2.1.1. OWASP TOP TEN

Este es un proyecto que describe los diez riesgos más críticos para la seguridad de aplicaciones web. Este informe se escribe en base a datos provenientes de más de cuarenta organizaciones internacionales además de una encuesta realizada a personas de la industria que luego son analizados por un equipo de expertos de todo el mundo, su versión más reciente fue lanzada a finales del año 2021 en la cual se añadieron tres nuevas categorías [15].

Su lista es actualizada cada tres o cuatro años ya que las técnicas de explotación son cambiantes y se actualizan constantemente, se estructura en orden de criticidad y el riesgo que implican para una organización la posible explotación de cada riesgo; al pasar los años, nuevos riesgos son añadidos a la lista y otros son eliminados debido a que dejaron de ser el foco de atención para los atacantes [15].

El informe del Top Ten de OWASP además de la categorización de los riesgos más comunes, también incluye una descripción de cada vulnerabilidad de la lista, el vector de ataque, ejemplos de escenarios de ataque, y la lista de CWE mapeados; incluye también recomendaciones para los desarrolladores, tester, administradores de la aplicación y para las organizaciones, todo esto para mitigar las vulnerabilidades que pueden presentar las mismas [59]. Esto nos asegura una gestión más efectiva de vulnerabilidades, prevención y mitigación.

Mitigar las vulnerabilidades de las aplicaciones web permiten disminuir el riesgo ante una amenaza de explotación que puede generar un incidente de seguridad que conlleve a la interrupción de la operación normal de la empresa [59]. Mejorar los procesos y generar conciencia de seguridad son los primeros pasos que conllevan aplicar buenas prácticas de seguridad, generando tranquilidad para la empresa y sus usuarios [59].

2.2.1.2. CWE/SANS TOP 25 MOST DANGEROUS SOFTWARE ERRORS

Es una lista de las 25 principales debilidades de software más peligrosas e impactantes del 2022, a menudo son fáciles de encontrar y explotar. Para elaborar esta lista se aprovechó los datos se utilizaron datos del Catálogo de Vulnerabilidades Explotadas Conocidas (KEV), establecido de acuerdo con la " Directiva Operativa Vinculante 22-01-Reducción del Riesgo Significativo de Vulnerabilidades Explotadas Conocidas " por CISA en noviembre de 2021. El KEV es una fuente de vulnerabilidades que se sabe que han sido explotadas en la naturaleza [60]. Se aplicó una fórmula a los datos para calificar cada debilidad en función de la prevalencia y la gravedad. El Conjunto de datos analizados para calcular el TOP 25 de 2022 contenía un total de 37899 registros CVE de los dos años calendario anteriores.

Su última versión es la del 2022 y ha tenido varios cambios en comparación a la lista del año 2021, cuenta con tres nuevas entradas en el Top 25 los cuales son el CWE-362 (“Condición de Carrera”) ubicándose en el rango N°22, el CWE-94 (“Control inadecuado de Generación de código, inyección de código”) en el puesto N°25, y el CWE -400 (“Consumo de recursos no controlados”) en el puesto N°23.

El Top 25 además de enlistar los principales errores de software más peligrosos también brinda una descripción breve y una extendida para cada debilidad, términos alternativos, relaciones, modos de introducción, consecuencias comunes, probabilidad de explotación, ejemplos demostrativos, mitigación y detección [61].

2.2.2. CWE/SANS Top 25 2022 vs OWASP Top Ten 2021

CWE/SANS TOP 25 2022		
RANGO	IDENTIFICACIÓN	NOMBRE
1	CWE-787	Escritura fuera de los límites
2	CWE-79	Neutralización incorrecta de la entrada durante la generación de la página web ("Cross-site Scripting")
3	CWE-89	Neutralización incorrecta de elementos especiales utilizados en un comando SQL ('inyección SQL')
4	CWE-20	Validación de entrada incorrecta
5	CWE-125	Lectura fuera de los límites
6	CWE-78	Neutralización incorrecta de elementos especiales utilizados en un comando de sistema operativo ('inyección de comando de sistema operativo')
7	CWE-416	Usar después gratis
8	CWE-22	Limitación incorrecta de un nombre de ruta a un directorio restringido ('Path Traversal')
9	CWE-352	Falsificación de solicitud entre sitios (CSRF)
10	CWE-434	Carga sin restricciones de archivos con tipo peligroso
11	CWE-476	Desreferencia de puntero NULL
12	CWE-502	Deserialización de datos no confiables
13	CWE-190	Desbordamiento de enteros o ajuste
14	CWE-287	Autenticación incorrecta
15	CWE-798	Uso de Credenciales Codificadas
16	CWE-862	Autorización faltante
17	CWE-77	Neutralización incorrecta de elementos especiales utilizados en un comando ('inyección de comando')
18	CWE-306	Autenticación faltante para función crítica
19	CWE-119	Restricción incorrecta de operaciones dentro de los límites de un búfer de memoria
20	CWE-276	Permisos predeterminados incorrectos
21	CWE-918	Falsificación de solicitud del lado del servidor (SSRF)
22	CWE-362	Ejecución concurrente usando recursos compartidos con sincronización incorrecta ("Condición de carrera")
23	CWE-400	Consumo de recursos no controlado
24	CWE-611	Restricción incorrecta de la referencia de entidad externa XML
25	CWE-94	Control inadecuado de la generación de código ("Inyección de código")

OWASP TOP TEN 2021		
RANGO	IDENTIFICACIÓN	NOMBRE
1	A01:2021	Control de acceso roto
2	A02:2021	Fallas criptográficas
3	A03:2021	Inyección
4	A04:2021	Diseño inseguro
5	A05:2021	Configuración incorrecta de seguridad
6	A06:2021	Componentes vulnerables y desactualizados
7	A07:2021	Fallas de identificación y autenticación
8	A08:2021	Fallas de integridad de datos y software
9	A09:2021	Fallas de registro y monitoreo de seguridad
10	A10: 2021	Falsificación de solicitud del lado del servidor

Ilustración 4 Relación entre el Top 25 de SANS y el OWASP Top Ten 2021 (Elaboración propia)

La lista del CWE/SANS Top 25 abarca debilidades comunes de software y hardware que se puede encontrar en la arquitectura, diseño, código o implementación. Mientras que el OWASP Top Ten comprende un consenso sobre los riesgos de seguridad más críticos de aplicaciones web. Es decir, el Top Ten de OWASP brinda la categoría principal, mientras que los CWE es un desglose de cada problema.

En la figura anterior se puede observar que quince de las veinticinco debilidades del Top de SANS se incluyen dentro de seis categorías del Top ten de OWASP, y algunos CWE del Top 25 no se incluyen en el OWASP Top Ten, esto se debe a que los CWE cubren problemas de software y no solo específico de aplicaciones web como el Top Ten.

Ambas listas ayudan a los desarrolladores a centrarse en las principales debilidades de seguridad, sin embargo, la mejor opción para este proyecto es el Top Ten de OWASP que está orientado principalmente a aplicaciones web, y no se cierra a CWE específicos como el TOP 25 de SANS, al contrario, cada categoría del Top Ten de OWASP incluyen muchos más CWE orientados a aplicaciones web que los que se muestra en la lista del Top 25 del año 2022.

2.2.3. METODOLOGÍAS DE PENTESTING

2.2.3.1. INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK ISSAF

Es un marco de referencia de código abierto para realizar análisis y pruebas de seguridad, ofrece una propuesta valiosa para asegurar la infraestructura mediante la evaluación de los controles de seguridad contra vulnerabilidades críticas. Examina la seguridad de la red, sistema, aplicación, o centrarse en infraestructura física [62].

El marco de Evaluación de Seguridad de Sistemas de Información se desarrolla mediante tres fases:

- **Fase 1. Planificación y Preparación:** Comprende los pasos para el intercambio de informaciones iniciales, planificación y pruebas de seguridad [63].

- **Fase 2. Evaluación:** Se aplican las pruebas de seguridad de la metodología de penetración ISSAF [63].
- **Fase 3. Reportes, Limpieza y Destrucción de Artefactos:** Toda la información creada y almacenada en los sistemas como parte de las pruebas de seguridad se eliminan [63].

2.2.3.2. PTES

Este estándar permite realizar una auditoria muy completa, tiene instrucciones detalladas de cómo realizar las pruebas, es fácil de entender y de adaptar en cualquier entorno [62]. El estándar para la ejecución de Pruebas de Penetración está compuesto por siete fases:

- **Preacuerdo:** Se define el alcance y los objetivos de la prueba de penetración [63].
- **Recopilación de Inteligencia:** Se realiza la recolección de información de inteligencia desde fuentes abiertas [63].
- **Modelado de amenazas:** Se enuncian las posibles estrategias de penetración [63].
- **Análisis de vulnerabilidades:** Se descubren vulnerabilidades que puedan ser explotadas [63].
- **Explotación:** Se intentan explotar las vulnerabilidades descubiertas [63].
- **Post Explotación:** Los especialistas de seguridad pueden continuar escalando el proceso de explotación.
- **Reporte:** Se comunica al cliente la información que le permita solucionar las vulnerabilidades encontradas.

2.2.3.3. OPEN WEB APPLICATION SECURITY PROJECT OWASP

La guía de pruebas de seguridad de aplicaciones web de OWASP propone una metodología de pruebas de intrusión, se basa en el enfoque de caja gris. El probador no sabe nada o tiene muy poca información sobre la aplicación a probar, y las divide en dos fases [30]:

- **Pruebas pasivas:** Se pretende comprender la lógica de la aplicación y los puntos de acceso de la aplicación web.

- **Pruebas activas:** Durante las pruebas activas un probador comienza a utilizar las metodologías descritas en las siguientes secciones, el conjunto de pruebas activas fue divididas es 12 categorías.

  - ✓ Recopilación de información
  - ✓ Pruebas de gestión de configuración e implementación
  - ✓ Pruebas de gestión de identidad
  - ✓ Pruebas de autenticación
  - ✓ Pruebas de autorización
  - ✓ Pruebas de gestión de sesiones
  - ✓ Pruebas de validación de entrada
  - ✓ Manejo de errores
  - ✓ Criptografía
  - ✓ Pruebas de lógica de negocios
  - ✓ Pruebas del lado del cliente
  - ✓ Pruebas de API

2.2.4. ¿QUÉ METODOLOGÍA DE PENETRACIÓN ELEGIR?

En un estudio comparativo sobre metodologías de pruebas de penetración enfocado a aplicaciones web en el que se incluyó las tres metodologías antes descritas, se obtuvo como resultado que ninguna enuncia en su totalidad las principales diez vulnerabilidades de aplicaciones web, e incluso algunas de ellas no cuentan con información suficiente sobre cómo probarlas [63].

La metodología PTES obtuvo una puntuación de 12/39 puntos, ISSAF una puntuación de 16/39, y OWASP una puntuación de 30/39 obteniendo la puntuación más alta. OWASP, pese a no contar con pruebas de seguridad que permitan evaluar dos riesgos de seguridad pertenecientes a la lista del Top Ten de OWASP del año 2017 los cuales son, deserialización insegura y el registro y monitoreo de la aplicación web, fue considerada la mejor metodología de pruebas de penetración para aplicaciones web.

Se realizó un análisis comparativo entre la lista del Top Ten del año 2021 y la metodología de pruebas de penetración que propone la Guía de Pruebas de Seguridad de Aplicaciones Web v4.0 de OWASP para verificar si sus pruebas cubren esta lista actualizada.

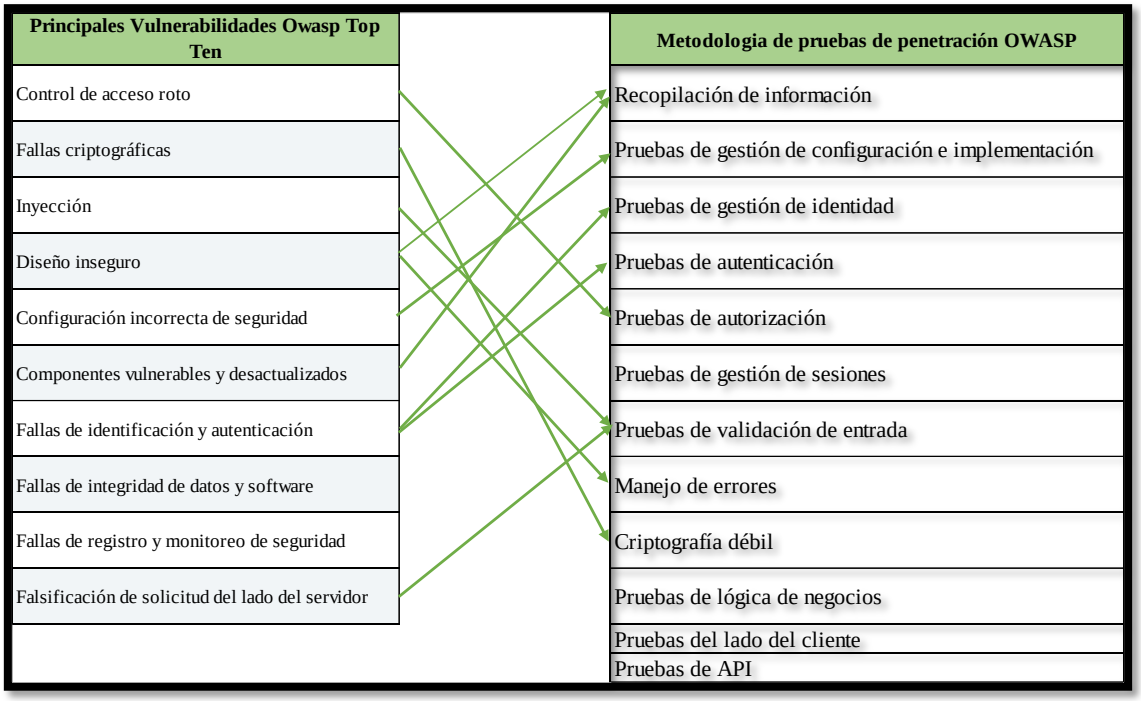


Ilustración 5 Top Ten 2021 vs Metodología de pruebas de penetración de OWASP (Elaboración propia)

En comparación, la deserialización insegura desaparece en el Top Ten 2021, y el registro y monitoreo de seguridad sube una categoría. De las doce categorías de la metodología de pruebas de penetración de OWASP, se puede observar que ocho de ellas cuentan con pruebas para evaluar ocho de los diez riesgos del Top Ten de OWASP. En base a esto se comprueba que esta es una de las metodologías que más se alinea a este proyecto.

2.3. METODOLOGÍA DEL PROYECTO

2.3.1. METODOLOGÍA DE INVESTIGACIÓN

Para conocer la situación actual de la empresa se optó por realizar entrevistas al jefe del departamento de TI, también se utilizó la técnica de observación siguiendo la metodología

de investigación de tipo diagnóstica [64]. La variable es: cantidad de riesgos de seguridad conocidos sobre la aplicación web de la institución financiera.

Debido a que existe poca información sobre análisis de seguridad realizados bajo el marco de OWASP Top Ten 2021 en entidades financieras, se utilizará la metodología de investigación de tipo exploratoria [65], donde se revisará proyectos similares que se hayan aplicado en diferentes industrias para realizar un análisis comparativo entre estas soluciones y lo que se espera lograr.

2.3.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Se utilizó la técnica de entrevista de manera no estructurada dirigida al jefe del departamento de TICs para conocer información y situación actual de la institución en seguridad informática.

De la entrevista realizada se obtuvo el siguiente contexto; según la normativa de la SEP las entidades financieras regidas por la misma deben seguir el estándar ISO 27001 para la seguridad de la información, sin embargo, esta entidad no ha realizado un análisis de seguridad a sus aplicaciones web.

La entidad financiera no cuenta con un especialista encargado en salvaguardar la seguridad de la información, lo cual es preocupante al ser una empresa en rápido crecimiento con presencia en varias provincias del país.

El área de tecnologías no cuenta con presupuesto para invertir en la seguridad de la información, viéndose en la necesidad de cubrir la seguridad con las herramientas que tienen a disposición lo cual no es la mejor práctica. Se debe contar con los mecanismos necesarios para garantizar la correcta gestión de seguridad de la información para evitar futuros incidentes de seguridad.

La aplicación web cuenta con un sistema protector de intrusos, que debe alertar al departamento de TI cuando un usuario está tratando de realizar acciones fuera de sus permisos permitidos. Y cuentan con un “HelpDesk” que permite a los empleados alertar

de forma inmediata cuando detectan alguna anomalía de seguridad y ellos reciban atención a la alerta de manera inmediata.

En la pregunta 11 de la entrevista, la normativa a la que hace referencia es la "Norma de Control para la administración del Riesgo Operativo y Riesgo Legal en las Entidades del Sector Financiero Popular y Solidario Bajo el Control de La Superintendencia de Compañías" la cual tiene como objetivo manejar una adecuada administración integral de riesgos, minimizando pérdidas que se pueden derivar de eventos ocasionados por fallas o insuficiencia de procesos, personas, tecnologías de la información y eventos externos [42]. En esta normativa no se nombra la protección de datos personales, solo especifica la correcta administración ante riesgos operativos.

Continuando con los métodos de recolección de información, la técnica de observación indirecta de bajo riesgo se la utilizó para recabar información y realizar un reconocimiento de las aplicaciones web de la institución financiera. Esta tuvo una duración de 1 semana y se obtuvo como resultado la identificación del dominio principal, un subdominio y cincuenta y ocho rutas de acceso que en su mayoría son solo informativas, se puede destacar que no existe un orden jerárquico entre las rutas de acceso encontradas, e incluso varias de ellas no se podían acceder desde el menú principal. Así mismo mediante la navegación libre por el sitio web se encontró que aún existían plantillas predeterminadas que no han sido eliminadas.

Se recabó información como: los mensajes de error ante un inicio de sesión incorrecto revelan el nombre de la tabla y campo de la base de datos. También, los formularios "Solicitud de Transferencia", "Solicitud de Tarjeta de débito" y "Solicitud de Créditos" en los que los usuarios pueden realizar transacciones financieras sin la necesidad de autenticarse como en la aplicación web no validan de forma correcta la información que ellos digitan.

Al término de este proyecto, los beneficiados directos será el departamento de TICs el cual se encarga de la infraestructura y seguridad informática de la institución ya que obtendrá un informe de las vulnerabilidades encontradas con recomendaciones que le permitirá tomar medidas correctivas. Y la empresa en general ya que cumplirá con parte

de las disposiciones legales planteadas por la Superintendencia de Economía Popular y Solidaria.

2.3.3. METODOLOGÍA DE DESARROLLO

Para llevar el desarrollo de la solución tecnológica de manera organizada se optó por seguir la metodología de pruebas de penetración propuesta por la guía de pruebas de seguridad web de OWASP con un enfoque de caja gris. Esta metodología consta de dos fases llamadas “Pruebas Pasivas” para la recolección de información, “Pruebas Activas” constituida por diez subfases que hacen referencia a la lista del OWASP Top Ten del año 2021. Y se añadió una tercera fase llamada Informe Final conformado por dos subfases, valoración de riesgos y redacción de informe final. (ver ilustración 6)

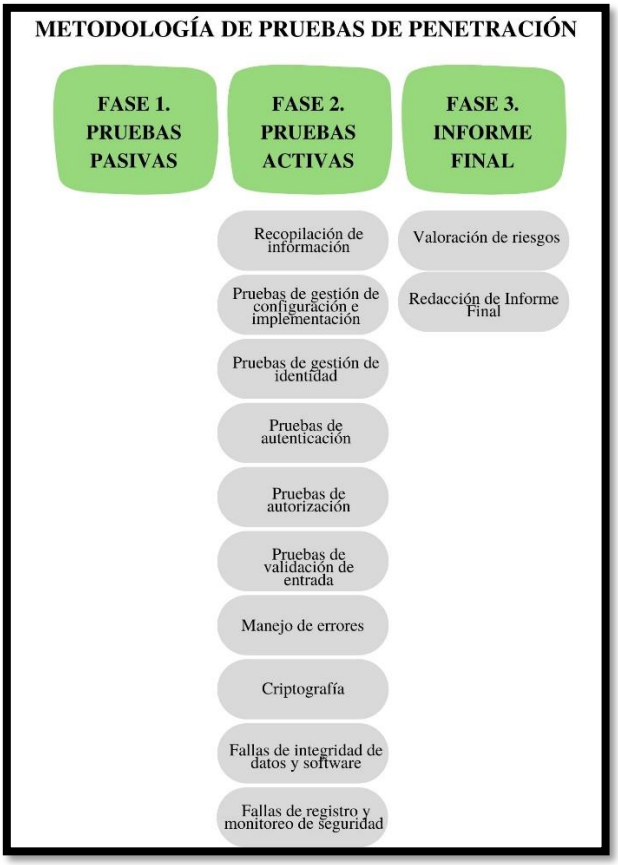


Ilustración 6 Metodología de pruebas de penetración a utilizar [15] [30]

Fase 1. Pruebas Pasivas: Se utilizó motores de búsqueda como Duck Duck Go, Google Hacking, WhoIs, Censys y navegación libre por el sitio web que permitieron recolectar

la información y conocer la lógica de la aplicación. Como resultado de esta fase se comprendió los puntos de acceso por las que un intruso podría ingresar al sistema.

Fase 2. Pruebas Activas: Se realizó pruebas manuales y con herramientas especializadas para detectar las vulnerabilidades de cada uno de los riesgos que forman parte de la lista del Top Ten de OWASP 2021, de las doce categorías que propone la metodología de penetración se utilizó ocho de ellas, y se añadió dos categorías más que comprenden las dos vulnerabilidades del Top Ten que no fueron cubiertas por la metodología.

F2. PA01: Recopilación de información
F2. PA02: Pruebas de gestión de configuración e implementación
F2. PA03: Pruebas de gestión de identidad
F2. PA04: Pruebas de autenticación
F2. PA05: Pruebas de autorización
F2. PA06: Pruebas de validación de entrada
F2. PA07: Manejo de errores
F2. PA08: Criptografía
F2. PA09: Fallas de integridad de datos y software
F2. PA10: Fallas de registro y monitoreo de seguridad

Fase 3. Informe Final

Esta fase está constituida por dos subfases, la valoración de riesgos y redacción el informe final en el que se detalla los resultados obtenidos tal como lo define la guía de OWASP.

F3. IF01: Valoración de riesgos: El modelo estándar de valoración de riesgo es
Riesgo= Probabilidad de ocurrencia * Impacto
La metodología de OWASP descompone la valoración de riesgos en 6 pasos
Paso 1: Identificando un riesgo
Paso 2: Factores para estimar la probabilidad de ocurrencia
Paso 3: Factores para estimar el Impacto
Paso 4: Determinación de la Severidad del Riesgo
Paso 5: Decidiendo que arreglar

Paso 6: Ajustando tu modelo de valoración del riesgo

F3. IF02: Redacción de Informe Final

La redacción del informe es el producto final de este proyecto, ayudará a los beneficiarios comprender los hallazgos, debe ser fácil de entender y detallará los riesgos encontrados en la fase dos de la metodología de pruebas utilizada [31].

La guía para la presentación de informes de OWASP consta de la siguiente estructura:

1. Introducción
1.1 Control de versiones
1.2 Tabla de contenido
1.3 El equipo
1.4 Alcance
1.5 Limitaciones
1.6 Cronología
2 Resumen ejecutivo
3 Hallazgos
3.1 Detalles de los Hallazgos

CAPITULO III

3. PROPUESTA

3.1. REQUERIMIENTOS

RQ1	Entrevista al jefe del departamento de TI para recopilar información
RQ2	Para la ejecución de herramientas de detección de vulnerabilidades se necesitará el monitoreo por parte del departamento de TI para responder ante cualquier incidente que pueda ocurrir
RQ3	Autorización para realizar las pruebas en el ambiente real
RQ4	Se necesitará un usuario con credenciales de acceso para realizar pruebas manuales para el ambiente real
RQ5	Todas las pruebas ejecutadas en el ambiente real deben ser informadas al jefe del departamento de TI
RQ6	Solo identificará riesgos de seguridad de la aplicación web, no abarcará redes o aplicación móvil
RQ7	Instalación de máquina virtual Kali Linux con al menos 4GB de RAM y 50 GB de almacenamiento
RQ8	Utilizar la metodología de pruebas de penetración propuesta en la guía de pruebas de seguridad de aplicaciones web de OWASP v 4.0 para el desarrollo del proyecto
RQ9	Para las categorías que se incluyeron en la fase dos de la metodología, se realizarán las pruebas según la guía del Top Ten de OWASP
RQ10	Utilizar la lista de los CWE mapeados en la lista del Top Ten de OWASP en caso de que la metodología de pruebas de penetración no presente suficiente información sobre como ejecutar las pruebas
RQ11	Las pruebas activas solo se realizarán dentro de los plazos establecidos por el departamento de TI
RQ12	Mantener la confidencialidad de la información obtenida y no mostrar datos que permitan identificar a la institución.
RQ13	Utilizar la metodología de valoración de riesgos OWASP para valorar los riesgos de seguridad detectados
RQ14	Se utilizará la guía de escritura de informe de pruebas OWASP para la redacción del informe final
RQ15	Entregar el informe final al jefe del departamento de TICs de la institución

Tabla 3 Requerimientos del proyecto

3.2. DESARROLLO

Para mantener la confidencialidad de la institución a la que se realizó el análisis de seguridad de sus aplicaciones web, dentro de este documento se sustituyó el nombre del sitio web original de la empresa por “sitiowebfinanciero”.

WSTG es el identificador de pruebas de la Guía de pruebas de seguridad web por sus siglas en inglés. Cada escenario tendrá un identificador en el siguiente formato, WSTG-<categoría>-<número>, en el que “categoría” es un parte superior de 4 caracteres que identifican el tipo de prueba o debilidad, y “número” es un valor numérico que hace referencia al número de prueba.

3.2.1. FASE 1. MODO PASIVO

Nombre de la fase	**FASE 1. MODO PASIVO**					
Identificador de la prueba	WSTG-INFO-01	**Nombre de la prueba**	Reconocimiento de descubrimiento de motores de búsqueda para detectar fugas de información			
Objetivo	Identificar qué información confidencial de diseño y configuración de la aplicación está expuesta directa o indirectamente en el sitio web de la institución o a través de servicios de terceros.					
Herramienta/método	**Resultados**					
Duck Duck Go	Este motor realiza búsquedas más exhaustivas, encontró páginas predeterminadas que debieron ser eliminadas por el desarrollador. muestran código XML en el que se destaca que el sitio está hecho en WordPress versión 5.6.8					
	Nota	Ver anexo 3				
Google	Se utilizaron dorks de Google para recopilar información, **site:sitiowebfinanciero.com** muestra las rutas de acceso del sitio web. **Link:sitiowebfinanciero.com** muestra los sitios que enlazan con el dominio de la cooperativa. De esta información se pudo recabar cuarenta y ocho rutas de acceso de la aplicación web,de las cuales siete son formularios que admiten el ingreso de datos por parte del usuario,cabe destacar que dichos formularios no tienen las suficientes validaciones de los datos que se ingresan, las otras rutas son solo informativas. También se identificaron páginas preedeterminadas que no han sido eliminadas. Adicionalmente cuenta con un subdominio que pertenece a la aplicación web de la cooperativa https://enlinea.sitiowebfinanciero.com/					
	Nota	Ver anexo 4				
	Con el Dork **inurl: sitioweb financiero** se identificó un enlace sospechoso **https://sitiowebfinanciero.com.atlaq.com/** al acceder a él se visualizó una recopilación detallada de información referente al sitio web de la cooperativa, tales como: nombre de dominio, fecha de registro y caducidad, el registrador de dominio utilizado. También presenta una sección llamada "Análisis de metadatos", "Seguridad", "Geografía", "Análisis de DNS" y "Análisis SEO"					
	Nota	Ver anexo 5				
WhoIs	Se logró identificar el proveedor de dominio del sitio web, al igual que datos relevantes como fechas de registro y expiración, nombres de servidores y datos personales del contacto registrante como dirección y número telefónico.					
	Nota	Ver anexo 6				
Censys	Al utilizar este motor de búsqueda reveló información que la institución hace uso de 3 hospedadores, muestra la ubicación, los puertos que utilizan, sus proveedores de software, IP públicas y los productos de software					
	Hospedador	Amazon-02	**Ubicación**	Estados Unidos	**Nombre del Servicio**	HTTP
	Puertos	80 y 443	**Proveedores de Software**	Amazon, apache y PHP	**Productos de Software**	Equilibrador de carga elástica, HTTPD, PHP y cookies
	Nota	Ver anexo 7				

Tabla 4 Reconocimiento pasivo mediante motores de búsqueda

3.2.2. FASE 2. MODO ACTIVO

F2. PA01: RECOPILACIÓN DE INFORMACIÓN

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA01: RECOPILACIÓN DE INFORMACIÓN**		
Identificador de la prueba	WSTG-INFO-08	**Nombre de la prueba**	Marco de aplicaciones web de huellas dactilares
Objetivo	Huella digital de los componentes que utilizan las aplicaciones web.		
Riesgo a probar	A06: 2021-Componentes Vulnerables y Obsoletos		
Herramienta/método	**Resultados**		
Uso de herramientas de escaneo automatizado ZAP	La aplicación web corre en un servidor apache		
	Encabezados HTTP	Se realizó un escaneo automatizado, el cual generó 723 alertas de seguridad, el servidor filtra información de los campos de encabezado de respuesta HTTP "X-Powered-By" mostrando el lenguaje de programación y versión en el que está desarrollada la aplicación. PHP7.4.30	
	Cookies	Las Cookies han sido configuradas sin la bandera HttpOnly que revelan información del marco que están utilizando. En el análisis de ZAP se encontraton 77 alertas de seguridad asociadas a esta vulnerabilidad. Tampoco fueron configuradas con el atributo SameSite que es una contramedida eficaz para la falsificación de solicitudes entre sitios, se generaron 79 alertas de seguridad asociadas a esta debilidad.	
		AWSELBCORS	Son cookies de Equilibrio de carga elástica de AWS (Amazon Web Service)
		AWSELB	
		PHPSESSID	Identificador predeterminado que PHP usa para las cookies generadas por session_start()
		wordpress_test_cookie	Identificador de cookie de wordpress, se utiliza para que los usuarios verifiquen si el navegador acepta las cookies
	Nota	ver anexo 8	

Tabla 5 Identificación de huellas dactilares de marco de aplicaciones

F2. PA02: PRUEBAS DE GESTIÓN DE CONFIGURACIÓN E IMPLEMENTACIÓN

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**PA02: PRUEBAS DE GESTIÓN DE CONFIGURACIÓN E IMPLEMENTACIÓN**		
Identificador de la prueba	WSTG-CONF-02	**Nombre de la prueba**	Configuración de la plataforma de aplicaciones de prueba
Objetivo	Asegúrese de que se hayan eliminado los archivos predeterminados y conocidos.		
Riesgo a probar	A05: 2021-Configuración de Seguridad Incorrecta		
Herramienta/método	**Resultados**		
Archivos y directorios de ejemplo conocidos	Archivos de muestra para el beneficio del desarrollador visibles en la web, navegando por el mapa de sitio revela la existencia de 16 sitios predeterminados que no han sido eliminados del sitio web de la institución desde el 2016		
	https://sitiowebfinanciero.com/10-ways-to-design-for-the-human-brain/		
	https://sitiowebfinanciero.com/is-search-engine-submission-necessary/		
	https://sitiowebfinanciero.com/low-cost-email-marketing-software/		
	https://sitiowebfinanciero.com/the-best-colleges-to-study-marketing-soft/		
	https://sitiowebfinanciero.com/why-designers-need-marketing-skills/		
	https://sitiowebfinanciero.com/create-great-wordpress-theme-and-you-will-win/		
	https://sitiowebfinanciero.com/why-is-important-to-have-great-financial/		
	https://sitiowebfinanciero.com/stick-with-your-concept-but-do-your-homework/		
	https://sitiowebfinanciero.com/three-social-media-hacks-for-the-busy-entrepreneur/		
	https://sitiowebfinanciero.com/harvest-great-ideas-from-your-companys-best-assets/		
	https://sitiowebfinanciero.com/a-digital-prescription-for-the-pharma-industry/		
	https://sitiowebfinanciero.com/retail-banks-wake-up-to-digital-lending-this-year/		
	https://sitiowebfinanciero.com/seven-weeks-working-pro-bono-with-a-charity/		
	https://sitiowebfinanciero.com/strategic-and-commercial-approach-with-issues/		

	https://sitiowebfinanciero.com/within-the-construction-industry-as-their-overdraft/	
	https://sitiowebfinanciero.com/hola-mundo/	
	Nota	Ver anexo 9
Comentario revisión	Dentro de los códigos fuentes de varios subdominios del sitio web y de la aplicación web se encontró comentarios que revelan información que no debería estar disponible en el ambiente de producción, incluyendo datos personales de un usuario de la cooperativa.	
	Nota	Ver anexo 10

Tabla 6 Pruebas de configuración incorrecta

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**PA02: PRUEBAS DE GESTIÓN DE CONFIGURACIÓN E IMPLEMENTACIÓN**		
Identificador de la prueba	WSTG-CONF-04	**Nombre de la prueba**	Revise la copia de seguridad antigua y los archivos sin referencia en busca de información confidencial
Objetivo	Encuentre y analice archivos sin referencia que puedan contener información confidencial.		
Riesgo a probar	A05: 2021-Configuración de Seguridad Incorrecta		
Herramienta/método	**Resultados**		
Inferencia del esquema de nombres utilizado para el contenido publicado	Se identifica el esquema de nomenclatura reconocible y organización de la página y directorios utilizando palabras claves que describen su función.		
	Nota	Ver anexo 4	
Otras pistas en el contenido publicado	En la ilustración del anexo 9 se evidencian pistas de contenido publicado que puede conducir al descubrimiento de funcionalidades ocultas.		
	Nota	Ver anexo 9	
	Utilizando /robot.txt nos muestra las pistas sobre los directorios sin referencias podemos verificar que permite acceder a admin-ajax.php mientras que wp-admin no está permitido el acceso.		
	Nota	Ver anexo 11	

Tabla 7 Revisión de archivos sin referencia con información confidencial

F2. PA03: PRUEBAS DE GESTIÓN DE IDENTIDAD

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA03: PRUEBAS DE GESTIÓN DE IDENTIDAD**		
Identificador de la prueba	WSTG-IDNT-02	**Nombre de la prueba**	Proceso de registro de usuario de prueba
Objetivo	Verificar que los requisitos de identidad para el registro de usuarios estén alineados con los requisitos comerciales y de seguridad. Validar el proceso de registro.		
Riesgo a probar	A07:2021- Fallas de Identificación y Autenticación		
Herramienta/método	**Resultados**		
Verificación de los requisitos de identidad para el registro de usuario estén alineados a los requisitos comerciales y de seguridad	**1. ¿Cualquiera puede registrarse para acceder?**		
	R1. No, solo usuarios que tengan una cuenta de ahorros en la cooperativa, el campo "Número de cuenta de ahorros" es obligatorio		
	2. ¿Los registros son examinados por un ser humano antes del aprovisionamiento o se otorgan automáticamente si se cumplen los criterios?		
	Se otorgan automáticamente si se cumplen los criterios		
	3. ¿Puede la misma persona o identidad registrarse varias veces?		
	No, se genera un mensaje de advertencia: "Ya te has registrado previamente, por favor inicia sesión o recupera tu contraseña."		
	4. ¿Los usuarios pueden registrarse para diferentes roles o permisos?		
	No, desde la aplicación web para acceder a la banca virtual solo permite el registro de usuarios/clientes. Mientras que el inicio de sesión del administrador solo permite acceder con credenciales de acceso, pero no registrarse.		
	5. ¿Qué prueba de identidad se requiere para que un registro sea exitoso?		
	Las pruebas de identidad que solicita la aplicación para registrarse son: cédula de identidad, fecha de nacimiento, número de cuenta del cliente, y el uso de un factor de verificación por medio de código enviado vía SMS al número celular registrado del cliente.		
	6. ¿Se verifican las identidades registradas?		
	No se verifican todas las identidades registradas, al intentar registrarse solo se valida el número de cédula del cliente, no se validan los demás campos que solicita la aplicación para el registro.		
	Nota	Ver anexo 12	

Tabla 8 Prueba de proceso de registro de usuario

F2. PA04: PRUEBAS DE AUTENTICACIÓN

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA04: PRUEBAS DE AUTENTICACIÓN**		
Identificador de la prueba	WSTG-ATHN-03	**Nombre de la prueba**	Prueba de mecanismo de bloqueo débil
Objetivo	Evaluar la capacidad del mecanismo de bloqueo de cuentas para mitigar la adivinación de contraseñas por fuerza bruta		
Técnica	A07:2021- Fallas de Identificación y Autenticación		
Herramienta/método	**Resultados**		
Mecanismo de bloqueo	1. Se inició sesión con una contraseña incorrecta 3 veces.	La aplicación permite tres intentos incorrectos de inicio de sesión, restringiendo la cuenta y solicitando que se cambie la contraseña.	
		Mensaje para usuario restringido: *"Usuario o contraseña incorrectos. Estimado Cliente, su usuario ha sido restringido por exceder el número de intentos fallidos permitidos, seleccione la opción desbloquear usuario / recuperar contraseña' ó 'olvidé mi pin'"*	
		Nota	Ver anexo 13
	2. Se inició sesión correctamente con la contraseña correcta, lo que demuestra que el mecanismo de bloqueo no se activa después de 3 intentos de autenticación incorrectos luego de 15 minutos.	No cuentan con un mecanismo de bloqueo, solo restricción del usuario que se activó después de tres intentos de inicio de sesión fallidos se esperó un tiempo de 15 a 20 minutos para iniciar sesión con las credenciales de acceso correctos, la aplicación volvió a mostrar el mensaje para usuario restringido.	
		" Usuario o contraseña incorrectos. Estimado Cliente, su usuario ha sido restringido por exceder el número de intentos fallidos permitidos, seleccione la opción 'desbloquear usuario / recuperar contraseña' ó 'olvidé mi pin'."	
Mecanismo de desbloqueo	Se realizó el proceso de recuperación de contraseña	Un mecanismo de desbloqueo solo debe usarse para desbloquear cuentas. No es lo mismo que un mecanismo de recuperación de contraseña, pero podría seguir las mismas prácticas de seguridad.	
		Para recuperar la contraseña nos piden llenar tres campos; cédula, fecha de nacimiento y el número de cuenta. Intencionalmente se llenaron mal los campos "fecha de nacimiento" y "número de cuenta" para verificar que se estén validando dichos campos, si los tres datos son correctos nos redirige automáticamente a una nueva ventana para ingresar la nueva contraseña. Se observó que la aplicación permitió reutilizar la contraseña anterior. Una vez cambiada la contraseña el sistema nos redirige a una nueva ventana para digitar el factor de autenticación que fue enviado al número celular registrado.	
		Nota	Ver anexo 14

Tabla 9 Pruebas sobre el mecanismo de bloqueo y desbloqueo

F2. PA05: PRUEBAS DE AUTORIZACIÓN

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA05: PRUEBAS DE AUTORIZACIÓN**		
Identificador de la prueba	WSTG-ATHZ-04	**Nombre de la prueba**	Pruebas de referencias de objetos directos inseguros IDOR
Objetivo	Identificar los puntos donde puede ocurrir referencias a objetos.		
Riesgo a probar	A01: 2021-Control de Acceso Roto		
Herramienta/método	**Resultados**		
Escenario 1: El valor de un parámetro se usa directamente para recuperar un	Se explorará esta vulnerabilidad cambiando manualmente parámetros del URL para obtener acceso directo a objetos de datos de la aplicación web sin pasar por verificaciones de autorización.		
	En la cuenta de un usuario autenticado de prueba se visualiza un saldo disponible de $19.64, la URL muestra el número de la cuenta por lo que se procedió a cambiar este objeto por otro al azar y verificar si se puede obtener información de otro usuario. Al modificar los últimos dígitos del identificador		

registro de la base de Datos	único se logró obtener el saldo disponible del usuario víctima el cual es de $308.92 comprobando así la existencia de este riesgo de seguridad.	
	Dirección URL antes de la prueba	https://enlinea.sitiowebfinanciero.com/nombreentidad/consultas/detalle/xx0000046724/xxx
	Dirección URL después de la prueba	https://enlinea.sitiowebfinanciero.com/nombreentidad/consultas/detalle/xx00000xxxX2/xxx
	Nota	Ver anexo 15
Escenario 2: Cambio del valor de un parámetro utilizando el proxy BurpSuite para extraer información sensible	En base a la prueba del escenario 1, se utilizó un proxy para revelar más información de esta vulnerabilidad	
	Con el mismo usuario autenticado, se modificó la solicitud GET utilizando el número de cuenta de un usuario que encontramos en la prueba WSTG-CONF-02 anexo 10, esto nos reveló su número de cédula, nombres completos, su código de cliente, y el saldo total de su cuenta.	
	Nota	Ver anexo 16

Tabla 10 Prueba de referencia de objetos IDOR

F2. PA06: PRUEBAS DE VALIDACIÓN DE ENTRADA

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA06: PRUEBAS DE VALIDACIÓN DE ENTRADA**		
Identificador de la prueba	WSTG-INPV-05	**Nombre de la prueba**	Pruebas de inyección SQL
Objetivo	Identificar puntos de inyección de SQL. Evaluar la severidad de la inyección y el nivel de acceso que se puede lograr a través de ella.		
Riesgo a probar	A03: 2021-Inyección		
Herramienta/método	**Resultados**		
Inyección SQL clásica	.' OR 1=1 --	La URL de inicio de sesión de clientes Al realizar diferentes inyecciones de código en los campos del formulario de inicio de sesión, la aplicación muestra el mismo mensaje de error *"Usuario o contraseña incorrectos. NO SE PUEDE GUARDAR SIN VALOR AL CAMPO CUSUARIO DE LA TABLA TUSUARIOSESIONES"* por lo que se deduce que no se puede realizar inyección sql por este método.	
	CUSUARIO=1 OR 1=1 --		
	Nota	Ver anexo 17	
sqlmap	sqlmap --dbms=mysql -u "https://enlinea.sitiowebfinanciero.com/financiero/login" --dbs --tamper=space2comment --random-agent --level=5 --risk=3	Se ejecutó este comando de sqlmap sobre el dominio **enlinea.sitiowenfinanciero.com/financiero/login** para realiza una inyección SQL al URL de inicio de sesión para clientes e intentar obtener las tablas de la base de datos, se utilizó tamper para intentar Bypasear el WAF (Web Application Firewall) y --random-agent para ejecutarlo con un agente aleatorio, sin embargo al terminar el análisis sqlmap monstró el mensaje *"Todos los parámetros probados no parecen ser inyectables"* por lo que no se lo considerará como un riesgo de seguridad	
	Nota	Ver anexo 18	
	sqlmap --dbms=mysql -u "http://sitiowebfinanciero.com/simulador/formularios-captacion/index.php?c=curriculum" --dbs --tamper=space2randomblank --random -agent --level=5 --risk=3	Se ejecutó la misma prueba de inyección al domio http://sitiowebfinanciero.com/simulador/formularios-captacion/index.php?c=curriculum, durante el análisis se perdió la comunicación, la cooperativa cuenta con un IPS que bloqueó las peticiones realizadas por sqlmap y restringiendo ejecutar cualquier herramienta sobre la URL sitiowebfinanciero.com	
	Nota	Ver anexo 19	

Tabla 11 Pruebas de inyección SQL

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA03: PRUEBAS DE VALIDACIÓN DE ENTRADA**		
Identificador de la prueba	WSTG-INPV-19	**Nombre de la prueba**	Pruebas de falsificación de solicitudes del lado del servidor
Objetivo	Probar si los puntos de inyección SSRF son explotables.		
Riesgo a probar	A10:2021-Falsificación de solicitudes del lado del servidor		
Herramienta/método	**Resultados**		
Obtener un archivo local	Se modificó la URL **https://sitiowebfinanciero.com/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%sitiowebfinanciero.com%2Fcredinversion%2F a https://sitiowebfinanciero.com/wp-json/oembed/1.0/embed?format=xml&url=url=file:///etc/passwd** para intentar obtener un archivo local, pero no se tuvo éxito.		
	Nota	ver anexo 20	

Tabla 12 Pruebas de falsificación de solicitudes del lado del servidor

F2. PA07: MANEJO DE ERRORES

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA07: MANEJO DE ERRORES**		
Identificador de la prueba	WSTG-ERRH-01	**Nombre de la prueba**	Pruebas para el manejo inadecuado de errores
Objetivo	Identificar la salida de error existente.		
Riesgo a probar	A04: 2021-Diseño Inseguro		
Herramienta/método	**Resultados**		
Aplicaciones	Identificar posibles puntos de entrada donde la aplicación espera datos.	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario: Se llenó un formulario de solicitud de transferencia interbancaria con datos falsos y erróneos para comprobar la inexistencia de validaciones de datos ingresados por el usuario, las secciones de los Datos del Ordenante y Datos de transferencia dentro de los campos *"nombres"* y *"cédula"* permiten digitar letras, números y caracteres especiales sin tener una cantidad límite. Así mismo la fecha de nacimiento admite años superiores al actual, y los campos donde se ingresan los números de cuenta también admite letras y caracteres especiales, sin embargo, cuenta con un límite de doce caracteres. Como se observa en el mensaje de error de la ilustración 17, no muestra errores referentes a la masiva cantidad de datos ingresados, solo en el número de cuenta a debitar.	
		En la sección de Inicio de Sesión al ingreso de las credenciales de acceso *"NOMBRE DE USUSARIO"* y *"Contraseña"* se visualiza que estos campos no cuentan con restricciones en cuanto a cantidad y tipos de caracteres.	
		Para la recuperación de contraseña se visualizó que tampoco existe un límite de caracteres o validaciones en la selección de fecha.	
		Nota	Ver anexo 21
	Manejo inadecuado de errores	El manejo de errores revela rastros de pila u otros mensajes de error demasiado informativos para los usuarios. La página de inicio de sesión de la aplicación web genera un mensaje de error que incluye información confidencial de las tablas de la base de datos cuando se ingresan credenciales de acceso erróneas	
		mensaje error: *"Usuario o contraseña incorrectos. NO SE PUEDE GUARDAR SIN VALOR AL CAMPO CUSUARIO DE LA TABLA TUSUARIOSESIONES"*	
		Nota	Ver anexo 22
	Cierre de sesión inadecuado	Ocurre cuando un usuario cierra la pestaña del navegador sin haber cerrado sesión en su cuenta bancaria y un autor malintencionado recupere la sesión revisando el historial de navegación. Se realizaron varios intentos de recuperación de sesión teniendo como resultado que se puede recuperar la sesión incluso después de 10 minutos de haber cerrado la pestaña de forma incorrecta.	

Tabla 13 Prueba del manejo inadecuado de errores

F2. PA08: CIFRADO DÉBIL

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA08: CIFRADO DÉBIL**		
Identificador de la prueba	WSTG-CRYP-01	**Nombre de la prueba**	Pruebas de seguridad de capa de transporte débil
Objetivo	Revisar la fuerza criptográfica y la validez de certificados digitales		
Riesgo a probar	A02: 2021-Fallos de Cifrado		
Herramienta/método	**Resultados**		
Escenario 1. Certificados digitales-para el dominio https://sitiowebfinanciero.com/	Debilidades Criptográficas	La clave pública es de 2048 bits	
		El algoritmo de firma es de SHA-256	
	Validez	Tiene un periodo de validez desde el 29 de mayo de 2022 19:00:00 hasta el 28 de agosto de 2022 18:59:59, por lo que está dentro del periodo de validez definido	
		La entidad certificadora es cPanel, Inc. Certification Authority	
		No es válido para subdominios	
	Nota	Ver anexo 23	
Escenario 2. Certificados digitales-para el dominio https://enlinea.sitiowebfinanciero.com/	Debilidades Criptográficas	La clave pública es de 2048 bits	
		El algoritmo de firma es de SHA-256	
	Validez	Tiene un periodo de validez desde el 10 de febrero de 2022 19:00:00 hasta el 11 de marzo de 2023 18:59:59, por lo que está dentro del periodo de validez definido	
		La entidad certificadora es Amazon	
		Es válido para subdominios	
	Nota	Ver anexo 24	

Tabla 14 Revisión de la fuerza criptográfica de los certificados digitales

F2. PA09: FALLAS DE INTEGRIDAD DE DATOS Y SOFTWARE

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA09: FALLAS DE INTEGRIDAD DE DATOS Y SOFTWARE**		
Identificador de la prueba	F2. PA09	**Nombre de la prueba**	Inclusión de archivos de origen JavaScript Cross-Domain
Objetivo	Identificar fallas de integridad de datos y software		
Riesgo a probar	A10:2021-Falsificación de solicitudes del lado del servidor		
Herramienta/método	**Resultados**		
OWASP ZAP	El análisis automatizado con la herramienta ZAP generó 12 alertas de páginas que no incluyen uno o más archivos encriptados de un dominio de terceros en los parámetros:		
	<script type="application/javascript" src="https://api.ipify.org?format=jsonp&callback=getIP"></script>		
	<script src="https://code.jquery.com/ui/1.12.1/jquery-ui.js"></script>		
	<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>		
	<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.2/jquery.min.js"></script>		
	<script src="https://code.jquery.com/jquery-latest.min.js" type="text/javascript"></script>		
	<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/js/bootstrap.min.js"></script>		
	Nota	ver anexo 25	

Tabla 15 Riesgo de integridad identificado por la herramienta ZAP

F2. PA10: FALLAS DE REGISTRO Y MONITOREO DE SEGURIDAD

Nombre de la fase	**FASE 2. MODO ACTIVO**		
Nombre de la subfase	**F2. PA10: FALLAS DE REGISTRO Y MONITOREO DE SEGURIDAD**		
Identificador de la prueba	F2. PA09	**Nombre de la prueba**	Detección de monitoreo de seguridad de la aplicación web
Objetivo	Verificar la existencia de monitoreos de seguridad en las aplicaciones web		
Riesgo a probar	A09:2021-Fallas de Registro y Monitoreo		
Herramienta/método	**Resultados**		
OWASP ZAP	Mediante el análisis de vulnerabilidades automatizado con la herramienta ZAP se identificó que la aplicación web principal cuenta con un mecanismo de defensa que bloqueaba las peticiones que realizaba esta herramienta automatizada, luego de un par de pruebas, ya no permitió acceder a la aplicación web principal, se tuvo que utilizar una VPN para continuar con las pruebas.		
SQLMAP	Se ejecutó la herramienta sqlmap para hacer un ataque de inyección SQL hacia la aplicación web, luego de varios intentos, la aplicación volvió a restringir la conexión.		
	Nota	ver anexos 19	

Tabla 16 Detección de monitoreo de seguridad de la aplicación web

3.2.3. FASE 3. INFORME FINAL

F3. IF01: VALORACIÓN DE RIESGOS

1. IDENTIFICANDO EL RIESGO

No	ID	RIESGO ASOCIADO	VULBERABILIDAD INVOLUCRADA
1	V1	Control de acceso roto	El valor de un parámetro se usa directamente para recuperar un registro de la base de Datos de otro usuario
2	V2	Diseño inseguro	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario
3	V3	Diseño inseguro	Manejo inadecuado de errores revela mensajes de error demasiado informativos como nombre de campos y nombres de tablas de la base de datos
4	V4	Diseño inseguro	Cierre de sesión inadecuado permite recuperar la sesión luego de 10 minutos de inactividad
5	V5	Configuración incorrecta de seguridad	Archivos y directorios de ejemplo conocidos
6	V6	Configuración incorrecta de seguridad	Información sensible dentro de comentarios en el código fuente
7	V7	Configuración incorrecta de seguridad	Inferencia del esquema de nombres utilizado para el contenido publicado
9	V8	Configuración incorrecta de seguridad	Vulnerabilidad conocida sobre Cookies
10	V9	Fallas de identificación y autenticación	Mecanismo de desbloqueo permite reutilización de contraseñas
11	V10	Fallas de identificación y autenticación	Todas las identidades registradas no son validadas
12	V11	Fallas de integridad de datos y software	Inclusión de archivos de origen JavaScript Cross-Domain

Tabla 17 Riesgos identificados

2. FACTORES PARA ESTIMAR LA PROBABILIDAD DE OCURRENCIA

V1	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	El valor de un objeto se usa directamente para recuperar un registro de la base de Datos de otro usuario			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?				x
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?			x	
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?			x	

Tabla 18 Factores para estimar la vulnerabilidad del riesgo de referencia de objetos IDOR

V2	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?			X	
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?	X			
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?			X	

Tabla 19 Factores para estimar la vulnerabilidad del riesgo: la aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario

V3	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Manejo inadecuado de errores revela mensajes de error demasiado informativos como nombre de campos y tablas de la base de datos			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?			X	
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?	X			
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?				X

Tabla 20 Factores para estimar la vulnerabilidad del riesgo: Manejo inadecuado de errores revela mensajes de error demasiado informativos.

V4	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Cierre de sesión inadecuado permite recuperar la sesión luego de 10 minutos de inactividad			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?			X	
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta que punto es fácil para estos atacantes explotar esta vulnerabilidad?			X	
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?			X	

Tabla 21 Factores para estimar la vulnerabilidad del riesgo: Cierre de sesión inadecuado

V5	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Archivos y directorios de ejemplo conocidos			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?				X
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?	X			
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?			X	

Tabla 22 Factores para estimar la vulnerabilidad del riesgo: Archivos y directorios de ejemplo conocidos

V6	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Información sensible dentro de comentarios en el código fuente			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?			X	
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?		X		
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?		X		

Tabla 23 Factores para estimar la vulnerabilidad del riesgo: Información sensible dentro de comentarios en el código fuente

V7	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Inferencia del esquema de nombres utilizado para el contenido publicado			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?				X
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?		X		
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?	X			

Tabla 24 Factores para estimar la vulnerabilidad del riesgo: Inferencia del esquema de nombres utilizado para el contenido publicado

V8	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Vulnerabilidad conocida sobre Cookies			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?				X
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?		X		
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?				X

Tabla 25 Factores para estimar la vulnerabilidad del riesgo: Vulnerabilidad conocida sobre las Cookies

V9	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Mecanismo de desbloqueo permite reutilización de contraseñas			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?			X	
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?		X		
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?			X	

Tabla 26 Factores para estimar la vulnerabilidad del riesgo: Mecanismo de desbloqueo permite reutilización de contraseñas

V10	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Todas las identidades registradas no son validadas			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?			X	
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?	X			
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?		X		

Tabla 27 Factores para estimar la vulnerabilidad del riesgo: Todas las identidades de registro no son validadas

V11	FACTORES ASOCIADOS A LA VULNERABILIDAD			
RIESGO	Inclusión de archivos de origen JavaScript Cross-Domain			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?				X
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?		X		
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?				X

Tabla 28 Factores para estimar la vulnerabilidad del riesgo: Inclusión de archivos de origen Java Script Cross-Domain

3. FACTORES PARA ESTIMAR EL IMPACTO

V1	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	El valor de un objeto se usa directamente para recuperar un registro de la base de datos de otro usuario				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?				X	
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?		X			
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 29 Factores para estimar el impacto del riesgo: El valor de objeto se utiliza directamente para recuperar un registro de la base de datos de otro usuario

V2	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?	X				
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?	X				
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 30 Factores para estimar el impacto del riesgo: La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario

V3	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Manejo inadecuado de errores revela mensajes de error demasiado informativos como nombre de campos y nombres de tablas de la base de datos				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?				X	
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?				X	
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?		X			

Tabla 31 Factores para estimar el impacto del riesgo: Manejo inadecuado de errores revela mensajes de error demasiado informativos

V4	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Cierre de sesión inadecuado permite recuperar la sesión luego de 10 minutos de inactividad				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?				**X**	
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?			X		
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?		X			

Tabla 32 Factores para estimar el impacto del riesgo: Cierre de sesión inadecuado permite recuperar la sesión luego de 10 minutos de inactividad

V5	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Archivos y directorios de ejemplo conocidos				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?	X				
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?	X				
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 33 Factores para estimar el impacto del riesgo: Archivos y directorios de ejemplo conocidos

V6	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Información sensible dentro de comentarios en el código fuente				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?		X			
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?			X		
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 34 Factores para estimar el impacto del riesgo: Información sensible dentro de comentarios en el código fuente

V7	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Inferencia del esquema de nombres utilizado para el contenido publicado				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?	X				
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?	X				
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 35 Factores para estimar el impacto del riesgo: Inferencia del esquema de nombres utilizado para el contenido publicado

V8	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Vulnerabilidad conocida sobre Cookies				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?		X			
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?			X		
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 36 Factores para estimar el impacto del riesgo: Vulnerabilidades conocidas sobre las cookies

V9	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Mecanismo de desbloqueo permite reutilización de contraseñas				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?		X			
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?	X				
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 37 Factores para estimar el impacto del riesgo: Mecanismo de desbloqueo permite reutilización de contraseñas

V10	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Todas las identidades registradas no son validadas				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?	X				
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?		X			
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?	X				

Tabla 38 Factores para estimar el impacto del riesgo: Todas las identidades registradas no son validadas

V11	FACTORES ASOCIADOS AL IMPACTO TÉCNICO				
RIESGO	Inclusión de archivos de origen JavaScript Cross-Domain				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?		X			
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?				X	
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?				X	

Tabla 39 Factores para estimar el impacto del riesgo: Inclusión de archivos de origen JavaScript Cross-Domain

4. DETERMINANDO LA SEVERIDAD DEL RIESGO

V1. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: EL VALOR DE UN PARÁMETRO SE USA DIRECTAMENTE PARA RECUPERAR UN REGISTRO DE LA BASE DE DATOS DE OTRO USUARIO

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	El valor de un parámetro se usa directamente para recuperar un registro de la base de Datos de otro usuario	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	5	9
Probabilidad de ocurrencia global		7,00
VALORACIÓN		ALTO

Tabla 40 Probabilidad de ocurrencia global sobre el riesgo V1

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	El valor de un parámetro se usa directamente para recuperar un registro de la base de Datos de otro usuario	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	3	1
Impacto técnico global		4.33
VALORACIÓN		MEDIO

Tabla 41 Impacto técnico global sobre el riesgo V1

Severidad global: Alta

V2. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: LA APLICACIÓN NO VALIDA, FILTRA NI DESINFECTA LOS DATOS PROPORCIONADOS POR EL USUARIO

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	1	6
Probabilidad de ocurrencia global		4,67
VALORACIÓN		MEDIO

Tabla 42 Probabilidad de ocurrencia global sobre el riesgo V2

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	1	1
Impacto técnico global		1.33
VALORACIÓN		BAJO

Tabla 43 Impacto técnico global sobre el riesgo V2

Severidad: Baja

V3. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: MANEJO INADECUADO DE ERRORES REVELA MENSAJES DE ERROR DEMASIADO INFORMATIVOS COMO NOMBRE DE CAMPOS Y NOMBRES DE TABLAS DE LA BASE DE DATOS

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Manejo inadecuado de errores revela mensajes de error demasiado informativos como nombre de campos y nombres de tablas de la base de datos	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	1	9
Probabilidad de ocurrencia global		5.67
VALORACIÓN		MEDIO

Tabla 44 Probabilidad de ocurrencia global sobre el riesgo V3

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Manejo inadecuado de errores revela mensajes de error demasiado informativos como nombre de campos y nombres de tablas de la base de datos	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
9	7	5
Impacto técnico global		7.00
VALORACIÓN		ALTO

Tabla 45 Impacto técnico global sobre el riesgo V3

Severidad: Alta

V4. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: CIERRE DE SESIÓN INADECUADO PERMITE RECUPERAR LA SESIÓN LUEGO DE 10 MINUTOS DE INACTIVIDAD

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Cierre de sesión inadecuado	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	5	6
Probabilidad de ocurrencia global		6,00
VALORACIÓN		ALTO

Tabla 46 Probabilidad de ocurrencia global sobre el riesgo V4

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Cierre de sesión inadecuado	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
9	5	5
Impacto técnico global		6,33
VALORACIÓN		ALTO

Tabla 47 Impacto técnico global sobre el riesgo V4

Severidad: Crítica

V5. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: ARCHIVOS Y DIRECTORIOS DE EJEMPLO CONOCIDOS

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Archivos y directorios de ejemplo conocidos	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	1	6
Probabilidad de ocurrencia global		5,33
VALORACIÓN		MEDIO

Tabla 48 Probabilidad de ocurrencia global sobre el riesgo V5

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Archivos y directorios de ejemplo conocidos	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	1	1
Impacto técnico global		1,33
VALORACIÓN		BAJO

Tabla 49 Impacto técnico global sobre el riesgo V5

Severidad: Baja

V6. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: INFORMACIÓN SENSIBLE DENTRO DE COMENTARIOS EN EL CÓDIGO FUENTE

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Información sensible dentro de comentarios en el código fuente	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	3	4
Probabilidad de ocurrencia global		4,67
VALORACIÓN		MEDIO

Tabla 50 Probabilidad de ocurrencia global sobre el riesgo V6

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Información sensible dentro de comentarios en el código fuente	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	5	1
Impacto técnico global		4,00
VALORACIÓN		MEDIO

Tabla 51 Impacto técnico global sobre el riesgo V6

Severidad: Media

V7. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: INFERENCIA DEL ESQUEMA DE NOMBRES UTILIZADO PARA EL CONTENIDO PUBLICADO

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Inferencia del esquema de nombres utilizado para el contenido publicado	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	3	1
Probabilidad de ocurrencia global		4,33
VALORACIÓN		MEDIO

Tabla 52 Probabilidad de ocurrencia global sobre el riesgo V7

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Inferencia del esquema de nombres utilizado para el contenido publicado	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	1	1
Impacto técnico global		1,33
VALORACIÓN		BAJO

Tabla 53 Impacto técnico global sobre el riesgo V7

Severidad: Baja

V8. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: VULNERABILIDAD CONOCIDA SOBRE COOKIES

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Vulnerabilidad conocida sobre Cookies	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	3	9
Probabilidad de ocurrencia global		7,00
VALORACIÓN		ALTO

Tabla 54 Probabilidad de ocurrencia global sobre el riesgo V8

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Vulnerabilidad conocida sobre Cookies	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	5	1
Impacto técnico global		4,00
VALORACIÓN		MEDIO

Tabla 55 Impacto técnico global sobre el riesgo V8

Severidad: Alta

V9. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: MECANISMO DE DESBLOQUEO PERMITE REUTILIZACIÓN DE CONTRASEÑAS

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Mecanismo de desbloqueo permite reutilización de contraseñas	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	3	6
Probabilidad de ocurrencia global		5.33
VALORACIÓN		MEDIO

Tabla 56 Probabilidad de ocurrencia global sobre el riesgo V9

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Mecanismo de desbloqueo permite reutilización de contraseñas	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	1	1
Impacto técnico global		2,67
VALORACIÓN		BAJO

Tabla 57 Impacto técnico global sobre el riesgo V9

Severidad: Baja

V10. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: TODAS LAS IDENTIDADES REGISTRADAS NO SON VALIDADAS

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Todas las identidades registradas no son validadas	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	1	4
Probabilidad de ocurrencia global		4,00
VALORACIÓN		MEDIO

Tabla 58 Probabilidad de ocurrencia global sobre el riesgo V10

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Todas las identidades registradas no son validadas	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	3	1
Impacto técnico global		2.00
VALORACIÓN		BAJO

Tabla 59 Impacto técnico global sobre el riesgo V10

Severidad: Baja

V11. PROBABILIDAD DE OCURRENCIA GLOBAL E IMPACTO TÉCNICO GLOBAL DEL RIESGO: INCLUSIÓN DE ARCHIVOS DE ORIGEN JAVASCRIPT CROSS-DOMAIN

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Inclusión de archivos de origen JavaScript Cross-Domain	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	3	9
Probabilidad de ocurrencia global		7,00
VALORACIÓN		ALTO

Tabla 60 Probabilidad de ocurrencia global sobre el riesgo V11

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Inclusión de archivos de origen JavaScript Cross-Domain	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	7	7
Impacto técnico global		6,67
VALORACIÓN		ALTO

Tabla 61 Impacto técnico global sobre el riesgo V11

Severidad: Crítica

5. DECIDIENDO QUÉ ARREGLAR

A continuación, se presentan la lista los riesgos según su severidad en orden descendente:

N	ID	RIESGO ASOCIADO	VULBERABILIDAD INVOLUCRADA	NIVEL DE RIESGO
1	v11	Fallas de integridad de datos y software	Inclusión de archivos de origen JavaScript Cross-Domain	Crítico
2	V4	Diseño inseguro	Cierre de sesión inadecuado permite recuperar la sesión luego de 10 minutos de inactividad	Crítico
3	V3	Diseño inseguro	Manejo inadecuado de errores revela mensajes de error demasiado informativos	Alto
4	V1	Control de acceso roto	El valor de un objeto se usa directamente para recuperar un registro de la base de Datos de otro usuario	Alto
5	V8	Configuración incorrecta de seguridad	Vulnerabilidad conocida sobre Cookies	Alto
6	V6	Configuración incorrecta de seguridad	Información sensible dentro de comentarios en el código fuente	Medio
7	V9	Fallas de identificación y autenticación	Mecanismo de desbloqueo permite reutilización de contraseñas	Bajo
8	V5	Configuración incorrecta de seguridad	Archivos y directorios de ejemplo conocidos	Bajo
9	V10	Fallas de identificación y autenticación	Todas las identidades registradas no son validadas	Bajo
10	V2	Diseño inseguro	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario	Bajo
11	V7	Configuración incorrecta de seguridad	Inferencia del esquema de nombres utilizado para el contenido publicado	Bajo

Tabla 62 Vulnerabilidades encontradas según su nivel de riesgo

En base a la lista generaba a partir de los riesgos evaluados se construyó un mapa de calor para visualizar de mejor maneja el riesgo global de cada vulnerabilidad.

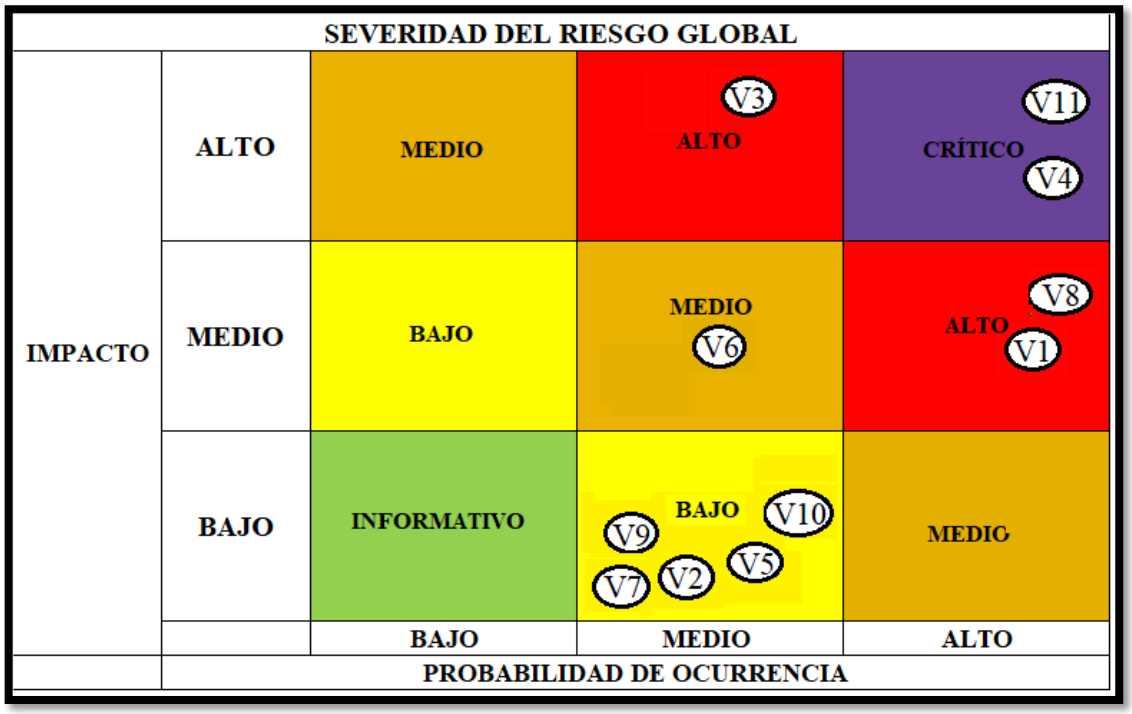


Ilustración 7 Mapa de calor de las vulnerabilidades según la severidad del riesgo

Lo primero que se debe arreglar son las vulnerabilidades que presentan mayor severidad, solventar los riesgos menos importantes no ayuda a reducir el riesgo global, incluso si son más fáciles o baratos. Cabe mencionar que no todos los riesgos merecen la pena ser solventados si su solución significa un gasto mayor que el beneficio que este represente. Queda a decisión del departamento de TI y a comité de Riesgo Operativo que riesgos solucionar.

F3. IF02: REDACCIÓN DE INFORME FINAL

Nombre de la fase	**F3. IF02: REDACCIÓN DE INFORME FINAL**				
Título	"INFORME DE ANÁLISIS DE SEGURIDAD CONTROLADO EN APLICACIONES WEB DE UNA INSTITUCIÓN FINANCIERA"				
Versión	1.0	**Fecha**	3/8/2022	**Autor**	Carvaca Orrala Ana Luisa
Contenido					
1.	INTRODUCCIÓN				
1.1.	CONTROL DE VERSIONES				
1.2.	TABLA DE CONTENIDO				
1.3.	EL EQUIPO				
1.4.	ALCANCE				
1.5.	LIMITACIONES				
1.6.	CRONOLOGÍA				
2.	RESUMEN EJECUTIVO				
3.	HALLAZGOS				
3.1.	RESUMEN DE HALLAZGOS				
3.2.	DETALLE DE LOS HALLAZGOS				
3.2.1.	V11. INCLUSIÓN DE ARCHIVOS DE ORIGEN JAVASCRIPT CROSS DOMAIN				
3.2.2.	V4. CIERRE DE SESIÓN INADECUADO PERMITE RECUPERAR LA SESIÓN LUEGO DE 10 MINUTOS DE INACTIVIDAD				
3.2.3.	V3. MANEJO INADECUADO DE ERRORES REVELA MENSAJES DE ERROR DEMASIADO INFORMATIVOS COMO NOMBRE DE CAMPOS Y NOMBRES DE TABLAS DE LA BASE DE DATOS				
3.2.4.	V1. EL VALOR DE UN OBJETO SE USA DIRECTAMENTE PARA RECUPERAR UN REGISTRO DE LA BASE DE DATOS DE OTRO USUARIO				
3.2.5.	V8. VULNERABILIDAD CONOCIDA SOBRE COOKIES				
3.2.6.	V6. INFORMACIÓN SENSIBLE DENTRO DE COMENTARIOS EN EL CÓDIGO FUENTE				
3.2.7.	V10. TODAS LAS IDENTIDADES REGISTRADAS NO SON VALIDADAS				
3.2.8.	V9. MECANISMO DE DESBLOQUEO PERMITE REUTILIZACIÓN DE CONTRASEÑAS				
3.2.9.	V5. ARCHIVOS Y DIRECTORIOS DE EJEMPLO CONOCIDOS				
3.2.10.	V2 LA APLICACIÓN NO VALIDA, FILTRA NI DESINFECTA LOS DATOS PROPORCIONADOS POR EL USUARIO				
3.2.11.	V7. INFERENCIA DEL ESQUEMA DE NOMBRES UTILIZADO PARA EL CONTENIDO PUBLICADO				
3.2.12.	SEVERIDAD DEL RIESGO GLOBAL				
Nota	Ver anexo 26				

Tabla 63 Ficha de información del informe de análisis de seguridad

CONCLUSIONES

Luego de realizar el análisis de seguridad se concluye que:

- La aplicación web es vulnerable a cinco de los diez riesgos de seguridad de la lista del Top Ten de OWASP.
- Presenta cuatro vulnerabilidades del riesgo "Configuración de seguridad Incorrecta" de la lista del Top Ten.
- Las vulnerabilidades más críticas pertenecen a los riesgos "Fallas de integridad de datos y software" y "Diseño inseguro"
- No existe un correcto manejo de los mensajes de error que la aplicación web muestra al usuario final.
- La aplicación web revela información sensible de otros usuarios al manipular un objeto de la URL.
- No se realizó una depuración en el código fuente para eliminar los comentarios con información sensible.

RECOMENDACIONES

El periodo de pruebas activas tuvo una duración de cuatro días, por lo que no se puede garantizar que se hayan identificado todos los posibles problemas de seguridad. Como tal, este informe sirve como un documento guía y no como una garantía de que el informe proporciona una representación completa de los riesgos que amenazan los sistemas en cuestión. La lista del Top Ten solo es una pequeña parte de los riesgos existentes para las aplicaciones web, por esta razón sugiero a la empresa realizar análisis de seguridad más profundo y completo a sus aplicaciones web.

REFERENCIAS

[1] Kaspersky, «Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021,» 2021.

[2] Kaspersky, «Ransomware: Desafío para empresas a pesar que ataques disminuyeron un 56% en 2021,» 2021.

[3] Ponemon Institute LLC, Reducing Enterprise Application Security Risks: More Work Needs to Be Done, Ponemon Institute, 2021, p. 5.

[4] Organización de los Estados Americanos OEA, Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe, Organización de los Estados Americanos, 2018.

[5] Instituto Nacional de Economía Popular y Solidaria - IEPS, «LEY DE LA ECONOMIA POPULAR Y SOLIDARIA,» Quito, 2012.

[6] Superintendencia de Economia Popular y Solidaria, «Segmentación de Entidades del Sector Financiero Popular y Solidario,» Quito, 2021.

[7] Superintendencia de Economía Popular y Solidaria SEPS, «SEPS,» [En línea]. Available: https://www.seps.gob.ec/interna?-que-es-la-seps-. [Último acceso: 2021].

[8] Corporación del Seguro de Depósitos CODESE, «CODESE,» [En línea]. Available: https://www.cosede.gob.ec/vision-mision-valores/. [Último acceso: 2021].

[9] Banco Central del Ecuador BCE, «BCE,» [En línea]. Available: https://www.bce.fin.ec/index.php/historia. [Último acceso: 2021].

[10] R. Gavilánez y D. Zambrano, Análisis de los ataques de hackers a entidades financieras: Una revisión post-literaria, Universidad de las Fuerzas Armadas-ESPE, 2017.

[11] International Organization for Standardization, «Normas ISO,» [En línea]. Available: https://www.normas-iso.com/iso-27001/. [Último acceso: 2021].

[12] M. Willberg, Web Application Security Testing With OWASP TOP 10 Framework, Turku University of Applied Sciences, 2019.

[13] PortSwigger, «Burp Suite es la elección de los profesionales de la seguridad en todo el mundo».

[14] M. R. F. S. Lenin Salgado, «Análisis De Riesgos De Las Aplicaciones Web De La Superintendencia De Bancos Y Seguros, Utilizando Las Recomendaciones Top Ten De OWASP Para Determinar Los Riesgos Más Críticos De Seguridad E Implementar Buenas Prácticas De Seguridad Para El Desarrollo De,» Universidad de las Fuerzas Armadas ESPE, 2014.

[15] OWASP, «Welcome to the OWASP Top 10 - 2021,» 2021.

[16] D. C. López Quinde, Análisis De Riesgos De La Plataforma Web Transaccional De La Cooperativa De Ahorro Y Crédito Jardín Azuayo, Universidad Técnica de Machala, 2019.

[17] OWASP, "Who is the OWASP Foundation?".

[18] Open Web Application Security Project OWASP, "A01:2021 – Broken Access Control," 2021.

[19] Open Web Application Security Project OWASP, "A02:2021 – Cryptographic Failures," 2021.

[20] Open Web Application Security Project OWASP, "A03:2021 – Injection," 2021.

[21] Open Web Application Security Project OWASP, "A04:2021 – Insecure Design," 2021.

[22] Open Web Application Security Project OWASP, "A05:2021 – Security Misconfiguration," 2021.

[23] Open Web Application Security Project OWASP, "A06:2021 – Vulnerable and Outdated Components," 2021.

[24] Common Weakness Enumeration, «CWE,» [En línea]. Available: https://cwe.mitre.org/. [Último acceso: 2021].

[25] Open Web Application Security Project OWASP, "A07:2021 – Identification and Authentication".

[26] Open Web Application Security Project OWASP, «A08:2021 – Software and Data Integrity Failures,» 2021.

[27] Open Web Application Security Project OWASP, "A09:2021 – Security Logging and Monitoring Failures," 2021.

[28] Open Web Application Security Project OWASP, "A10:2021 – Server-Side Request Forgery (SSRF)," 2021.

[29] E. Saad y R. Mitchell, Web Security Testing Guide Version 4.2, Open Web Application Security Project, 2020.

[30] Open Web Application Security Project OWASP, Web Security Testing Guide Version 4.2, OWASP, 2020.

[31] Open Web Application Security Project OWASP, GUÍA DE PRUEBAS OWASP, Open Web Application Security Project OWASP, 2008.

[32] PortSwigger, «PortSwigger,» [En línea]. Available: https://portswigger.net/burp/upgrade-community-to-pro. [Último acceso: 2022].

[33] CENSYS, «Una Internet segura comienza con Censys.».

[34] DuckDuckGo, «Duck Duck Go,» [En línea]. Available: https://duckduckgo.com/about. [Último acceso: 2022].

[35] S. Mansfield, «Google hacking 101,» *ScienceDirect,* nº 3, pp. 4-6, 2009.

[36] KALI, «KALI ORG,» [En línea]. Available: https://www.kali.org/.

[37] NMAP, «NMAP,» [En línea]. Available: https://nmap.org/.

[38] Open Web Application Security Project OWASP, "OWASP ZAP," [Online]. Available: https://owasp.org/www-project-zap/.

[39] Whois, «Whois Dominio,» [En línea]. Available: https://www.whoisdominio.com/.

[40] Consejo de la Facultad de Sistemas y Telecomunicaciones FACSISTEL, «Resolución RCF-FST-SO-09 No. 03-2021,» Universidad Estatal Peninsula de Santa Elena, La Libertad, 2021.

[41] Superintendencia de Economía Popular y Solidaria SEPS, Recomendaciones para el manejo de información y administración de ciberseguridad en el Sector Financiero Popular y Solidario, Quito: Superintendencia de Economía Popular y Solidaria SEPS, 2021.

[42] Superintendencia de Economía Popular y Solidaria SEPS, Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria, Superintendencia de Economía Popular y Solidaria SEPS, 2018.

[43] Asamblea Nacional de la República del Ecuador, Ley Orgánica de Protección de Datos Personales, Quito: Asamblea Nacional de la República del Ecuador, 2021.

[44] Secretaría Nacional de Planificación, Plan de Creación de Oportunidades 2021-2025, Quito: Secretaría Nacional de Planificación, 2021.

[45] F. Pacheco y H. Jara, Hackers al descubierto. USERSHOP, 2010.

[46] N. R. Niño Morante, Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque, Universidad Nacional Pedro Ruiz Gallo, 2018.

[47] International Business Machines IBM, «Identificación y autenticación».

[48] O. Parra Boldú, Análisis de Sistemas de autenticación y autorización para entornes web distribuidos, Universitat Oberta de Catalunya, 2019.

[49] A. Mendoza Arteaga, F. Bolaños Burgos, C. Cedeño Sarmiento y W. Saltos Rivas, «La importancia de la autenticación multifactor para el usuario final en unentorno financiero.,» *Revista de Tecnologías de la Información y las Telecomunicaciones,* vol. 4, nº 1, pp. 42-51, 2020.

[50] M. Cornejo Velázquez, I. González Ceron y M. Guerrero Rubio, Seguridad en Sistemas de Información Transaccional, Universidad Autónoma de Hidalgo, 2015, p. 3.

[51] International Business Machines IBM, «¿Qué es el cifrado? Definición de cifrado de datos».

[52] J. C. Mendoza, Demostración de cifrado simétrico y asimétrico, Quito: Ingenius.

[53] M. V. Vivanco Granda, V. H. Benítez Bravo, G. V. Moreano Sánchez y Á. G. Benítez Bravo, «Evaluación del Rendimiento de Comunicaciones entre las plataformas Java y .NETutilizando un Cifrado Híbrido,» *Ciencia Digital,* vol. 3, nº 2, pp. 141-161, 2019.

[54] The MITRE Corporation, "CWE Common Weakness Enumeration," [Online]. Available: https://cwe.mitre.org/. [Accessed 2022].

[55] L. Shung Huang, A. Rice, E. Ellingsen and C. Jackson, "Analyzing Forged SSL Certificates in the Wild," *IEEE,* 2014.

[56] J. Alfonso Aguilar, «ESQUEMAS DE FINGERPRINTING COMO PROTECCIÓN DE LOS DERECHOS DE AUTOR,» *Revista de Investigación en Tecnologías de la Información,* 2018.

[57] A. Y. Vanegas Romero, Pentesting, ¿Porque es importante para las empresas?, Bogotá: Universidad Piloto de Colombia, 2019.

[58] A. E. Rodriguez Llerena, «Herramientas fundamentales para el hacking ético,» *Revista Cubana de Informática Médica,* pp. 116-131, 2020.

[59] J. Zapata García, Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top ten de vulnerabilidades de OWASP, Universidad Nacional Abierta y a Distancia UNAD, 2018.

[60] Common Weakness Enumeration, «2022 CWE Top 25 Most Dangerous Software Weaknesses,» CWE, 2022.

[61] SysAdmin Audit, Networking and Security Institute SANS, «CWE/SANS TOP 25 errores de software más peligrosos,» 2022.

[62] K. Rodriguez Lago, «Metodologías para la auditoria de la seguridad,» 2017.

[63] H. R. González Brito y R. Montesino Perurena, «Capacidades de las metodologías de pruebas de penetración para,» *Revista Cubana de Ciencias Informáticas,* vol. 12, nº 4, pp. 52-65, 2018.

[64] N. Abatedaga, Epistemologìa y metodologías para planificar por consensos, 2008.

[65] S. M. V. C. M. T. Roberto Hernández Sampieri, Metodología de la Investigación, Mexico: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2014.

ANEXOS

ANEXO 1: FICHA DE OBSERVACIÓN

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

FICHA DE OBSERVACIÓN			
Objeto de observación	Aplicaciones Web de la Entidad Financiera		
Periodo sujeto a revisión:	1 semana	**Objetivo**	Realizar un reconocimiento de las aplicaciones
tipo de observación:	Indirecta	**Clasificación:**	BR
Descripción			
Navegar por el sitio web para identificar el sitemap, entender su estructura y conocer las funciones de la aplicación web			
Causas			
Conocer la estructura, contenido y funciones tanto del sitio web como de su aplicación web			
Efectos			
Saber desde que punto puede ser atacada			
Recomendaciones			
Evitar dejar a exposición pública información sensible de la institución.			

Firma del responsable de la observación

Ilustración 8 Ficha de Observación

ANEXO 2. FICHA DE ENTREVISTA

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

ENTREVISTA DIRIGIDA A JEFE DEL DEPARTAMENTO DE TI	
OBJETIVO	Obtener información sobre las acciones tomadas por la empresa para mantener la seguridad de la infotmación.

1	**¿Siguen algún estándar o manual de buenas prácticas de seguridad?**
R1	Si, el estandar ISO 27001.
2	**¿La empresa cuenta con responsables de la seguridad de la información que permitan cumplir con los criterios de confidencialidad, integridad y disponibilidad de la información, acorde al tamaño y complejidad de los procesos administrados por el negocio?**
R2	No contamos con un responsable especificamente dedicado a la seguridad de la información, solo con el departamento de TI.
3	**¿Cuentan con un comité de seguridad de la información que se encargue de evaluar, y supervisar el sistema de gestión de seguridad de la información?**
R3	No contamos con un comité de seguridad, sin embargo contamos con un comité de riesgo operativo que lo integran 3 personas que participan con voz y voto: el jefe de TI, jefe de riesgo y el Gerente general. Y pueden particicar solo con voz los auxiliares de sistemas.
4	**¿Han sufrido ciberataques? ¿Fue exitoso? ¿qué tipo de ataque fue?**
R4	Hasta el momento no.
5	**¿Cuentan con Un área independiente y especializada con personal capacitado y experiencia en gestión de seguridad de la información, acorde al tamaño y complejidad de sus operaciones?**
R5	No contamos con un área independiente en seguridad ya que la normativa anterior no la exigia, ahora si la exige. Se creará un área de seguridad que estará ligada al departamento de TI.
6	**¿Considera que cuentan con el suficiente presupuesto para garantizar la seguridad de la información de la empresa?**
R6	No, no hay un presupuesto destinado a la seguridad de información por lo que no era exigido por las entidades de control, el personal de TI nos hemos visto en la necesidad de autoeducarnos.

Ilustración 9 Ficha de entrevista 1/2

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

ENTREVISTA DIRIGIDA A JEFE DEL DEPARTAMENTO DE TI	
OBJETIVO	Obtener información sobre las acciones tomadas por la empresa para mantener la seguridad de la infotmación.

7	**¿Cumplen con procesos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios?**
R7	No, según la normativa de nuestras entidades de control la información digital debe permanecer con nosotros 20 años y como institución apenas tenemos 19 años de vida institucional.
8	**¿Realizan procedimientos para el monitoreo periódico de accesos, operaciones privilegiadas e intentos de accesos no autorizados?**
R8	Si, contamos con un IPS.
9	**¿Cuentan con mecanismos para que sus usuarios internos (empleados) reporten incidentes de seguridad?**
R9	Si, contamos con HelpDesk, en el que empleados pueden reportar cualquier tipo de situación relacionada a seguridad.
10	**¿Cuentan con un plan de comunicaciones que permitan informar a sus clientes cuando su información personal se haya visto comprometida?**
R10	No, definitivamente no tenemos. Recien estamos implementando el área de marketing que será el vocero con nuestros clientes.
11	**¿Tiene conocimiento de la nueva ley de protección de datos personales? ¿Que está haciendo la empresa para hacer cumplir esta ley?**
R11	Si tenemos conocimiento, pero lo de nosotros va mucho más allá según nuestra normativa que es la resolución del riesgo operativo 279 de la SEP.

Firma del responsable de la entrevista

Ilustración 10 Ficha de entrevista 2/2

ANEXO 3. RECONOCIMIENTO CON MOTOR DE BÚSQUEDA DUCK DUCK GO

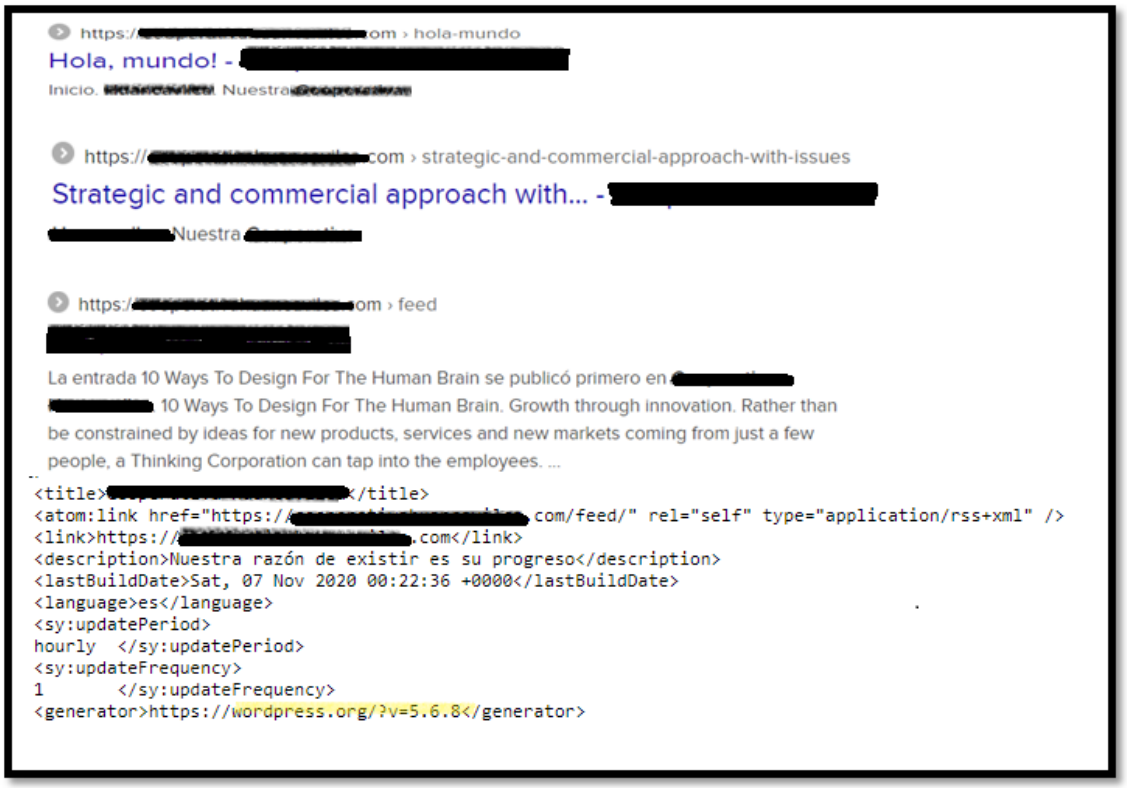


Ilustración 11 Página predeterminadas encontrada por el motor de búsqueda Duck Duck go

ANEXO 4. RECONOCIMIENTO CON MOTOR DE BÚSQUEDA GOOGLE

1	https:// sitiowebfinanciero.com/solicitud-de-reclamo/	25	https:// sitiowebfinanciero.com/videos-concursos/
2	https:// sitiowebfinanciero.com/quienes-somos/	26	https:// sitiowebfinanciero.com/inscripcion-club-ahorro/
3	https:// sitiowebfinanciero.com/contactos/	27	https:// sitiowebfinanciero.com/club-del-ahorro/
4	https:// sitiowebfinanciero.com/depositos-a-plazo-fijo/	28	https:// sitiowebfinanciero.com/simulador-de-ahorros/
5	https:// sitiowebfinanciero.com/directivos/	29	https:// sitiowebfinanciero.com/huancavilca-en-linea/
6	https:// sitiowebfinanciero.com/proteccion-derecho-de-socios-informe/	30	https:// sitiowebfinanciero.com/ahorro-a-la-vista/
7	https:// sitiowebfinanciero.com/proteccion_derechos_socios/	31	https:// sitiowebfinanciero.com/credigrupo/
8	https:// sitiowebfinanciero.com/trabajeconnosotros/	32	https:// sitiowebfinanciero.com/la-hormiguita-saving/
9	https:// sitiowebfinanciero.com/solicitud-de-credito/	33	https:// sitiowebfinanciero.com/fondos-de-reserva/
10	https:// sitiowebfinanciero.com/credito-emergente/	34	https:// sitiowebfinanciero.com/plan-de-ahorro-decimos/
11	https:// sitiowebfinanciero.com/creditos-institucionales/	35	https:// sitiowebfinanciero.com/pago-de-servicios/
12	https:// sitiowebfinanciero.com/credinversion/	36	https:// sitiowebfinanciero.com/supa/
13	https:// sitiowebfinanciero.com/microcredito/	37	https:// sitiowebfinanciero.com/tarjeta-de-debito/
14	https:// sitiowebfinanciero.com/credito-de-consumo/	38	https:// sitiowebfinanciero.com/sistema-de-pagos-interbancarios/
15	https:// sitiowebfinanciero.com/formulario-quejas/	39	https:// sitiowebfinanciero.com/pagos-y-envio-de-dinero/
16	https:// sitiowebfinanciero.com/simulador-credito/	40	https:// sitiowebfinanciero.com/pago-de-nomina/
17	https:// sitiowebfinanciero.com/solicitud-de-tarjeta-de-debito/	41	https:// sitiowebfinanciero.com/cajero-automatico/
18	https:// sitiowebfinanciero.com/ruleta/	42	https:// sitiowebfinanciero.com/historia/
19	https:// sitiowebfinanciero.com/depositos-seguros-con-la-cosede/	43	https:// sitiowebfinanciero.com/recaudacion-movil/
20	https:// sitiowebfinanciero.com/solicitud_transferencia/	44	https:// sitiowebfinanciero.com/organismos-de-control/
21	https:// sitiowebfinanciero.com/mi-futuro-seguro/	45	https:// sitiowebfinanciero.com/ley-de-transparencia/
22	https:// sitiowebfinanciero.com/cuenta-juvenil/	46	https:// sitiowebfinanciero.com/organigrama/
23	https:// sitiowebfinanciero.com/cuenta-infantil/	47	https:// sitiowebfinanciero.com/balances/
24	https:// sitiowebfinanciero.com/videos-concursos-jovenes/	48	https:// sitiowebfinanciero.com/inicio-2/

Ilustración 12 Micrositios de la entidad financiera

ANEXO 5. RESULTADO DEL DORK INRUL DEL GOOGLE

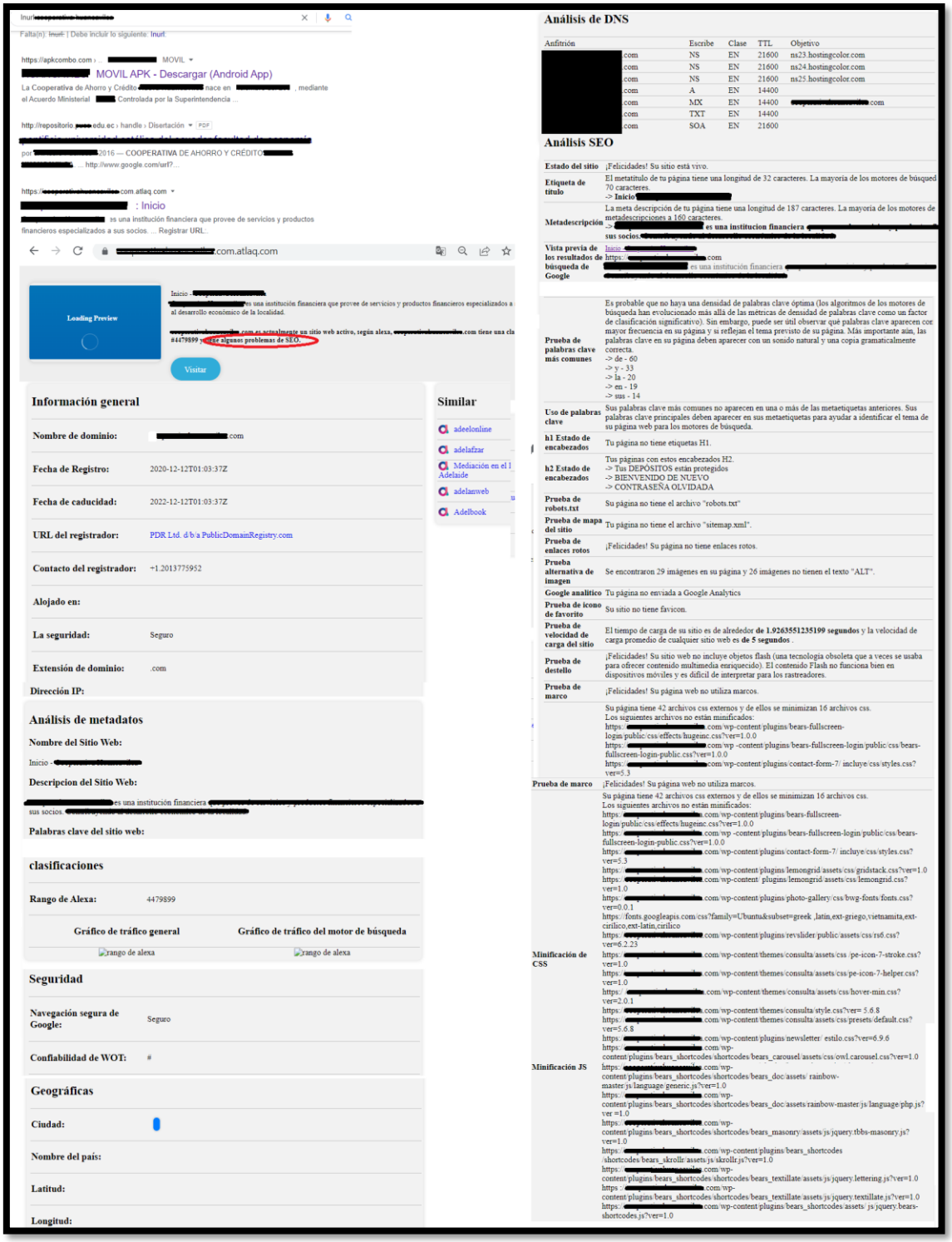


Ilustración 13 Resultados del sitio entidadfinanciera.com.atlaq.com

ANEXO 6. RECONOCIMIENTO CON EL MOTOR DE BÚSQUEDA WHOIS

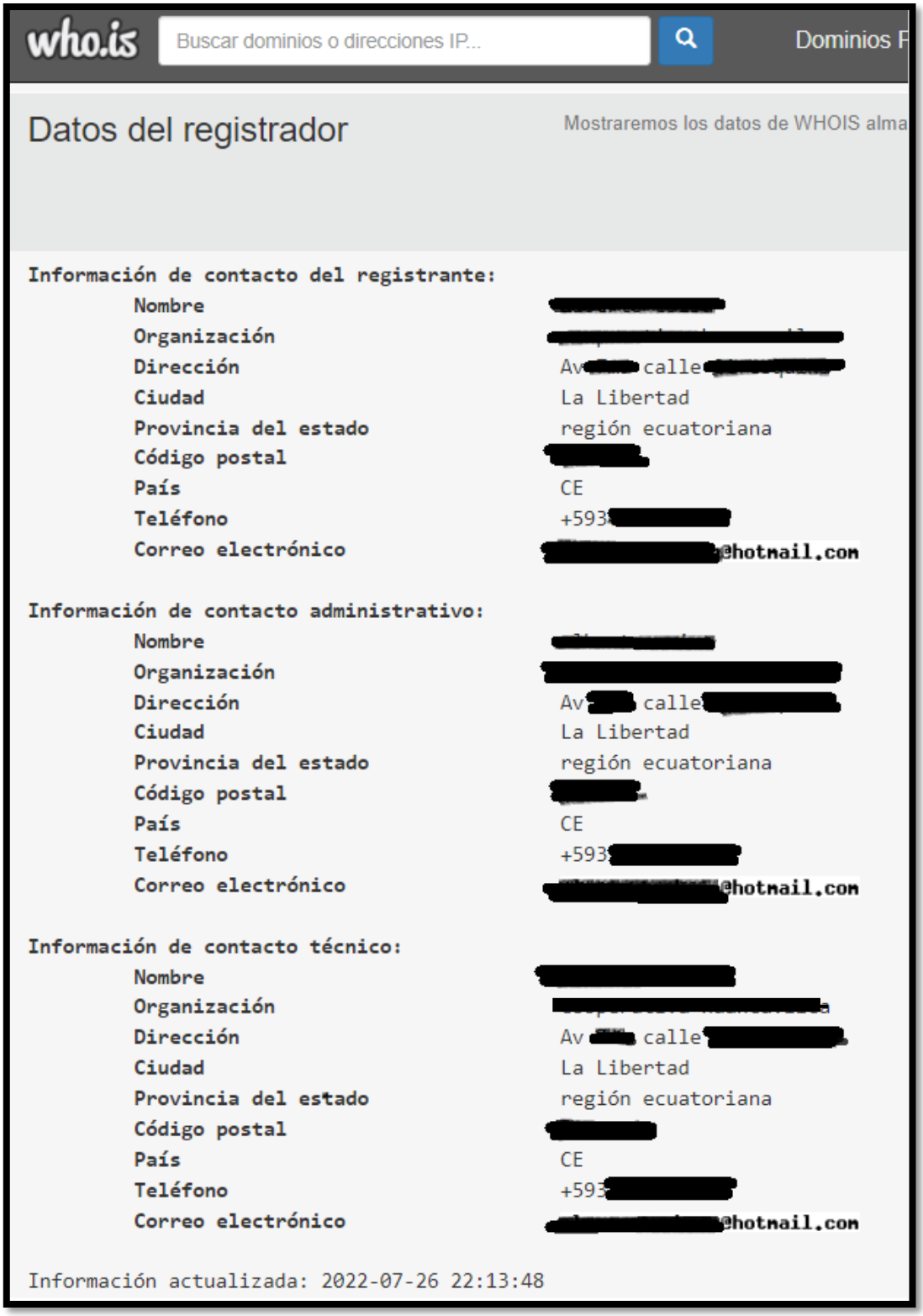
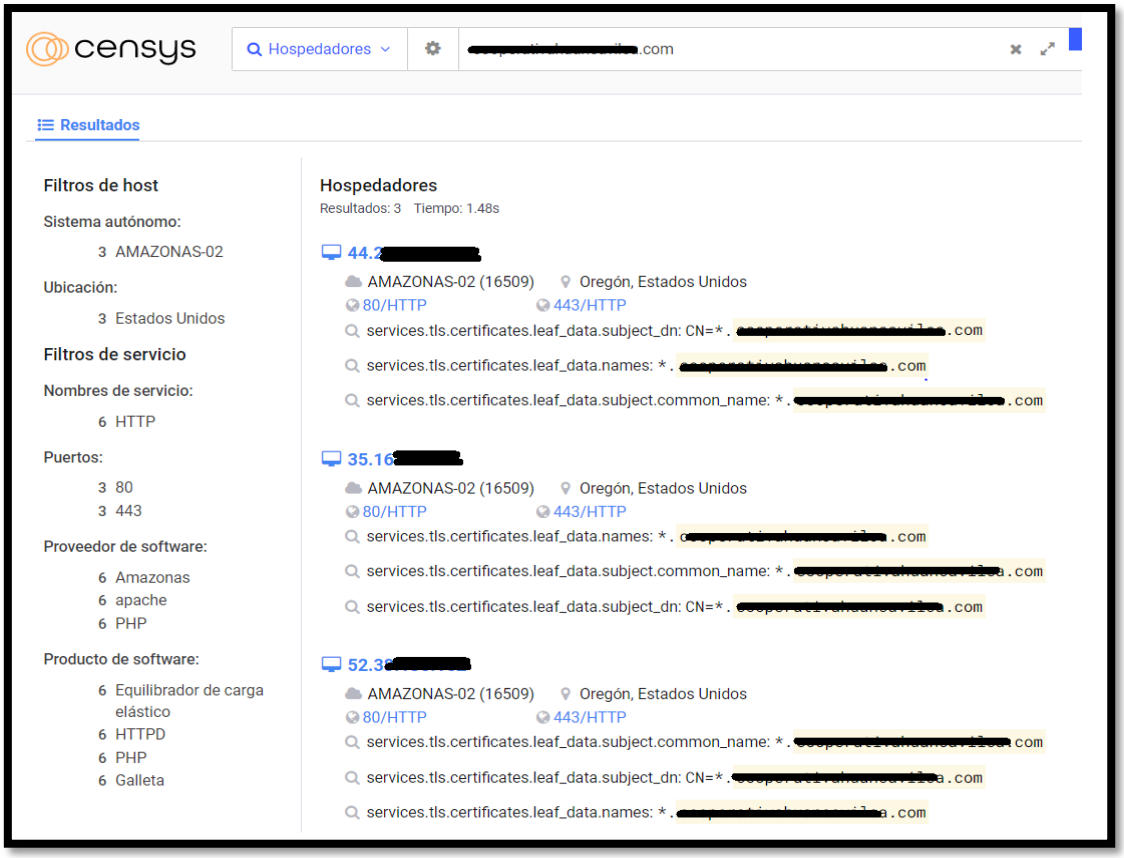


Ilustración 14 Información del dominio extraída del sitio web whois.com

ANEXO 7. RECONOCIMIENTO CON EL MOTOR DE BÚSQUEDA CENSYS



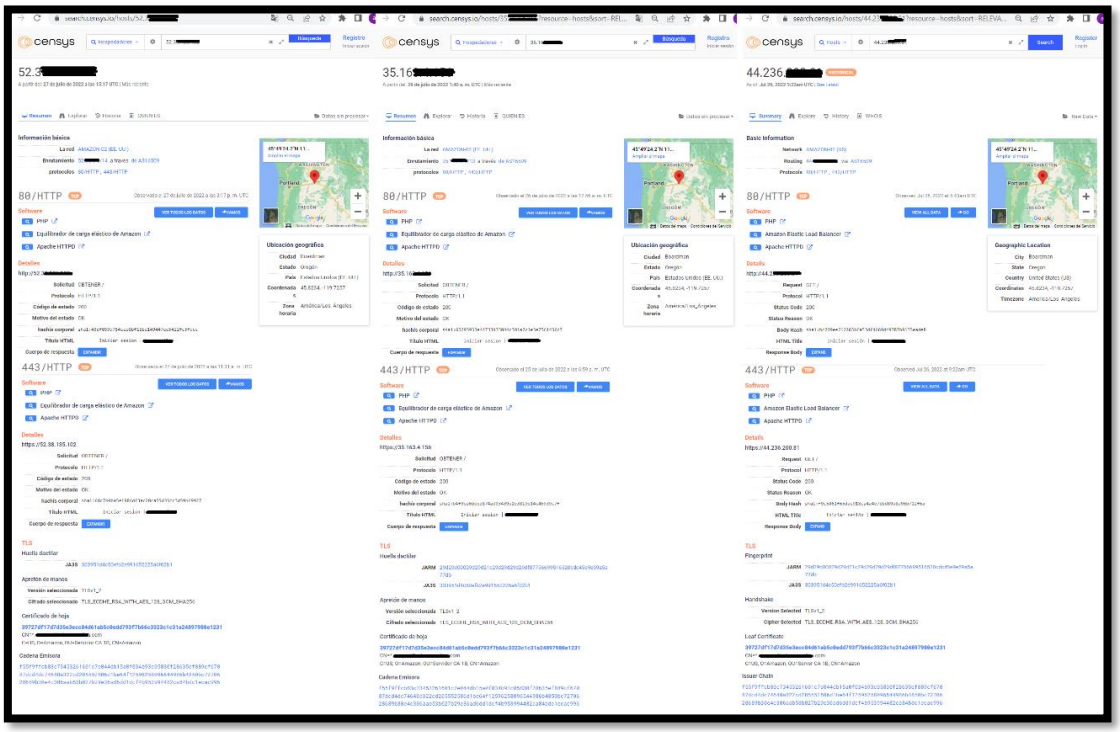


Ilustración 15 Información del dominio extraída del motor de búsqueda Censys

ANEXO 8. DESCUBRIMIENTO DE VULNERABILIDADES CONOCIDAS MEDIANTE LA TOMA DE HUELLAS DACTILARES DE LOS MARCOS

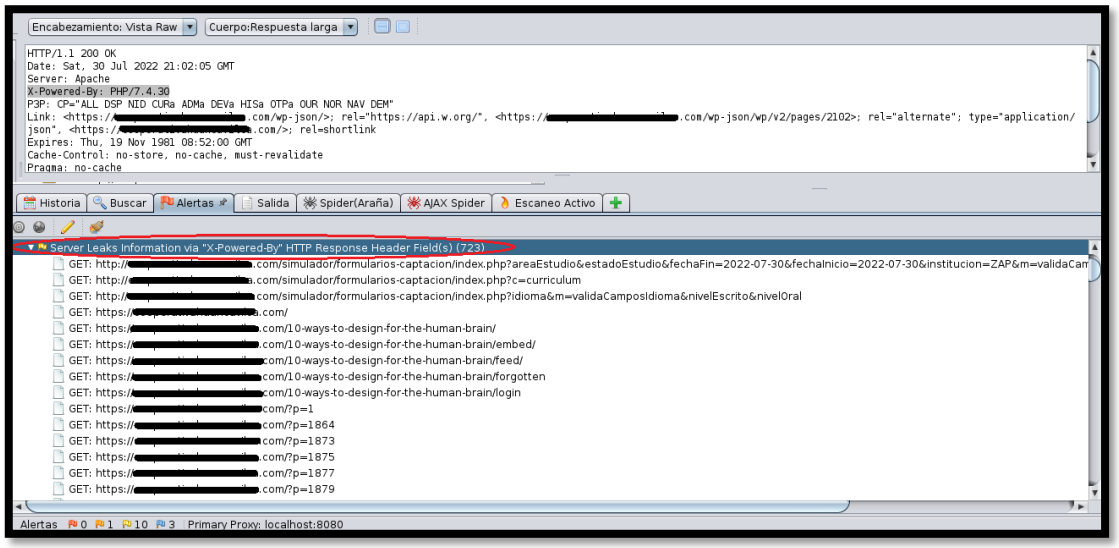


Ilustración 16 Identificación de vulnerabilidad conocida en php 7.4.30

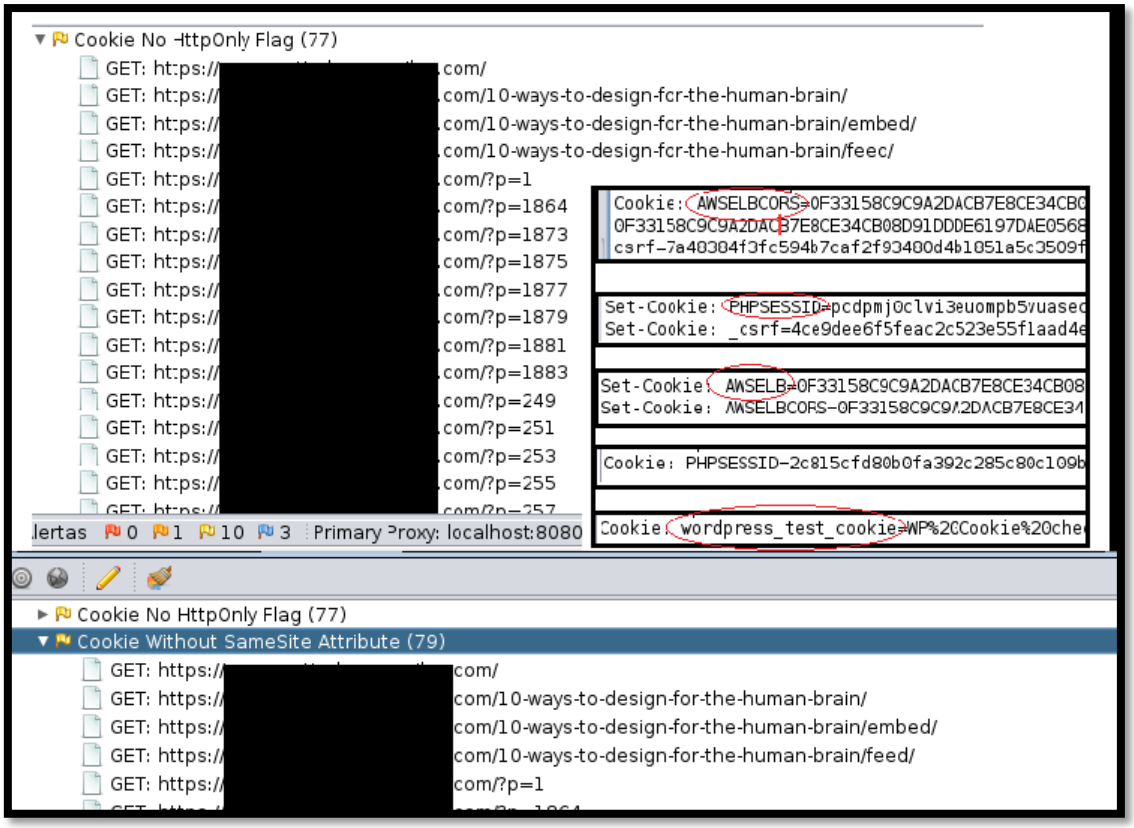


Ilustración 17 Cookies con nombres predeterminados que revelan el marco utilizado

ANEXO 9. SITIOS PREDETERMINADOS QUE NO HAN SIDO ELIMINADOS

Ilustración 18 Sitios predeterminados

ANEXO 10. COMENTARIOS DENTRO DEL CÓDIGO FUENTE QUE NO FUERON DEPURADOS

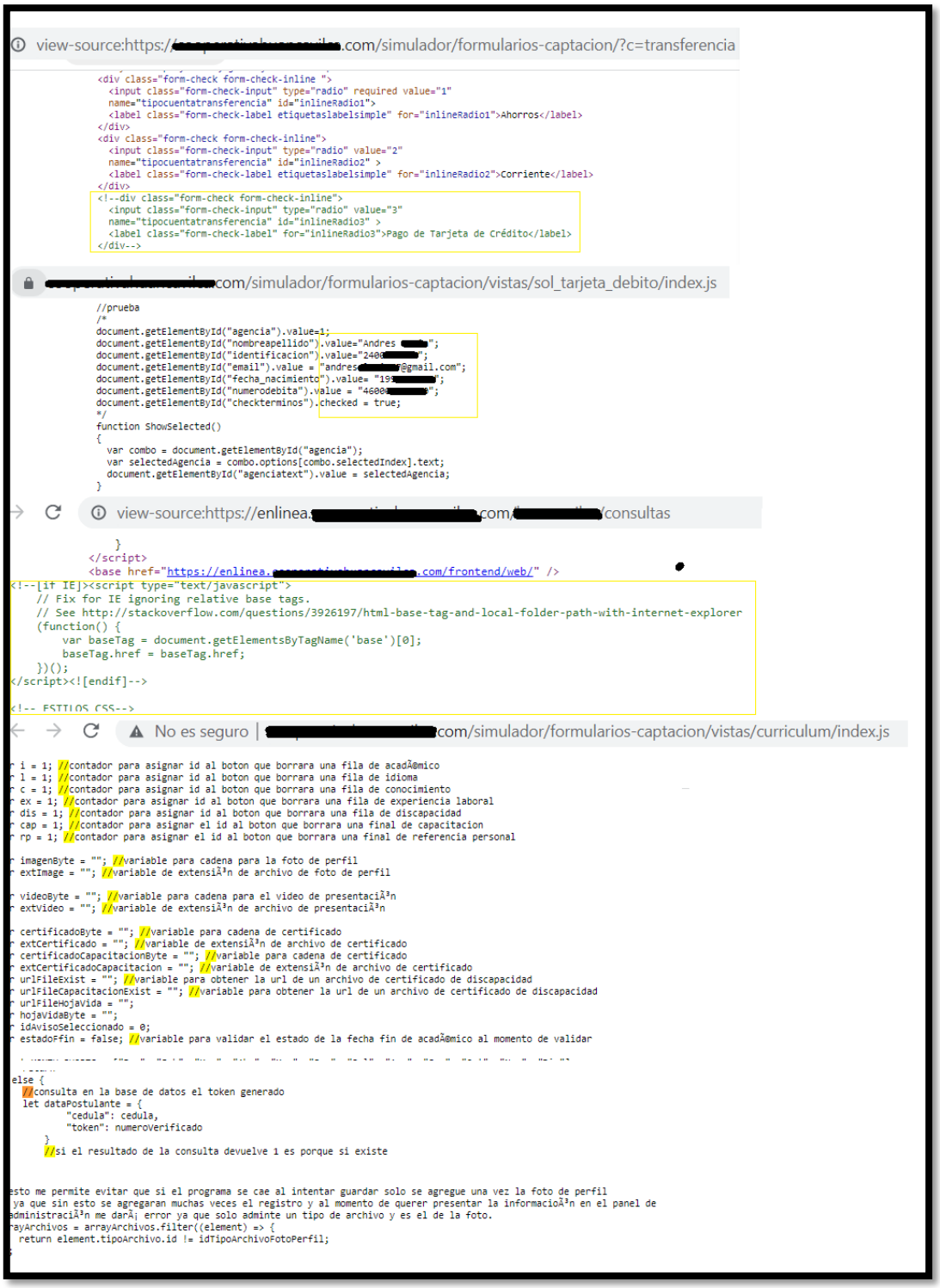


Ilustración 19 Comentarios con información que debió ser depurada al pasar al ambiente de producción

ANEXO 11. PRUEBA UTILIZANDO ROBOTS.TXT

Ilustración 20 Resultado de ejecutar robots.txt

ANEXO 12. PRUEBAS DE VERIFICACIÓN DE IDENTIDADES EN EL REGISTRO DE USUARIO

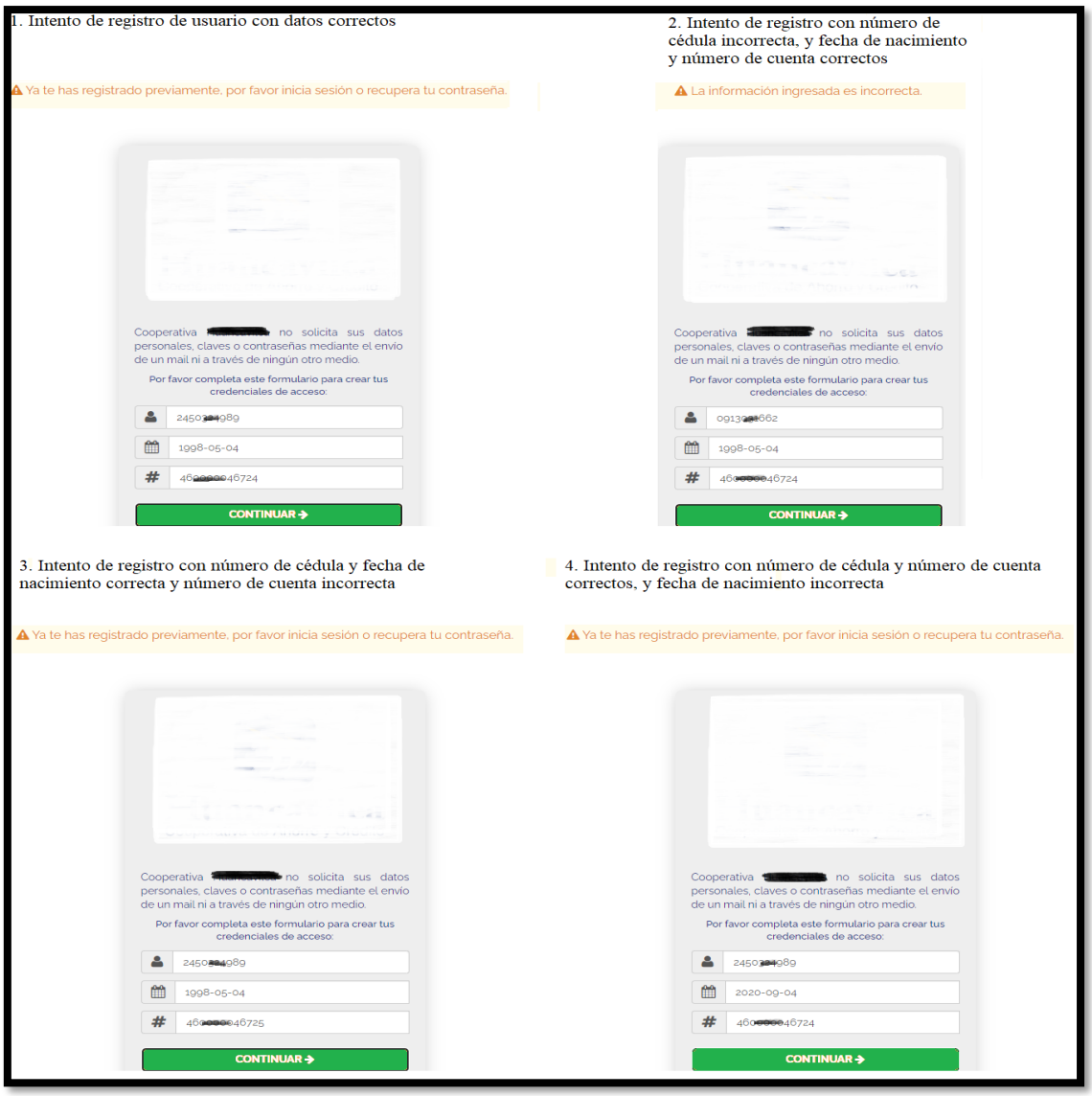


Ilustración 21 Pruebas de validación de identidad en registro de usuario

ANEXO 13. PRUEBA DE INICIO DE SESIÓN FALLIDO 3 VECES

Ilustración 22 Restricción de usuario luego de tres intentos fallidos

ANEXO 14. RECUPERACIÓN DE CONTRASEÑA

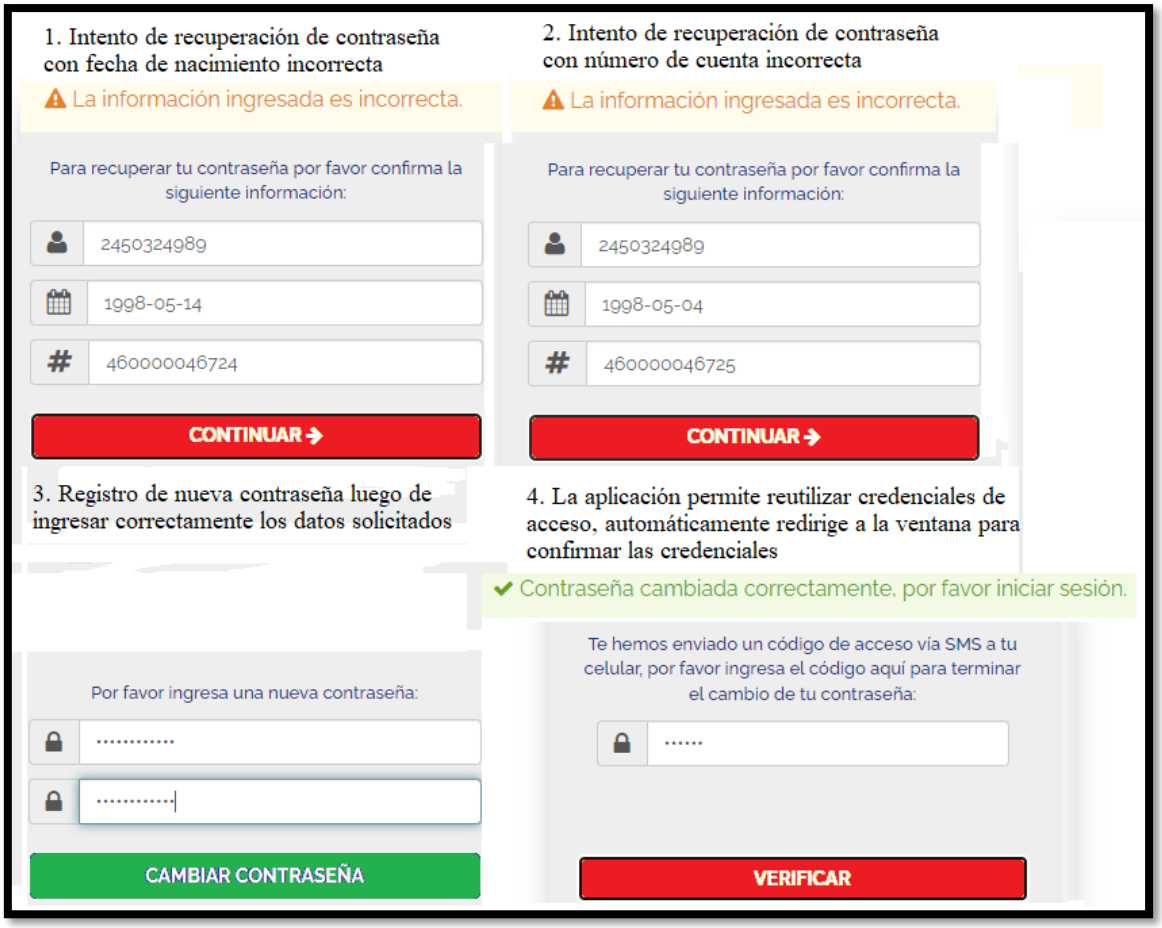


Ilustración 23 Recuperación de contraseña en la aplicación web

ANEXO 15. PRUEBA DE REFERENCIA DE OBJETOS DIRECTOS IDOR

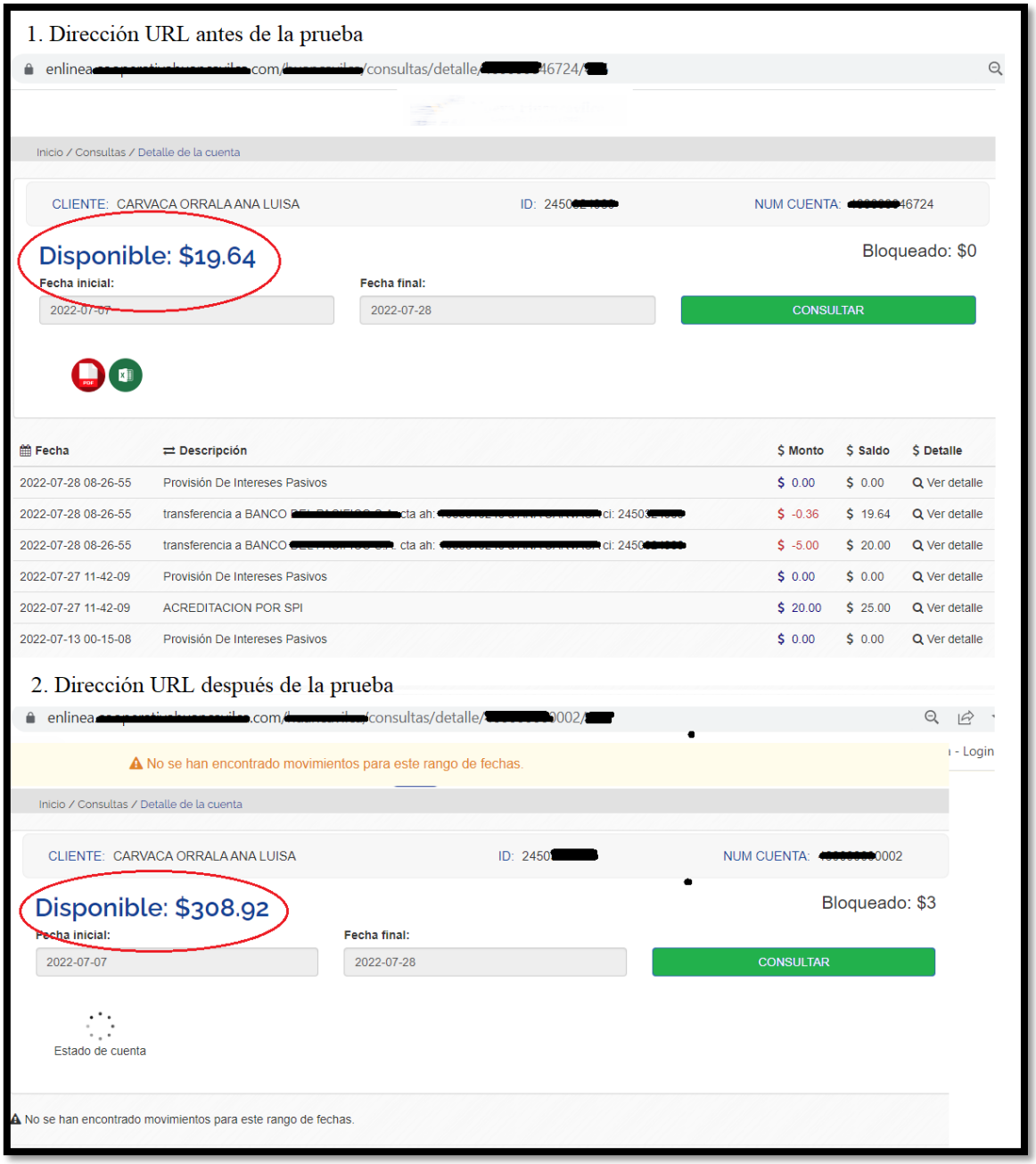


Ilustración 24 Visualización de información bancaria de otros usuarios

ANEXO 16. PRUEBA DE REFERENCIA DE OBJETOS DIRECTOS IDOR CON PROXY BURPSUITE

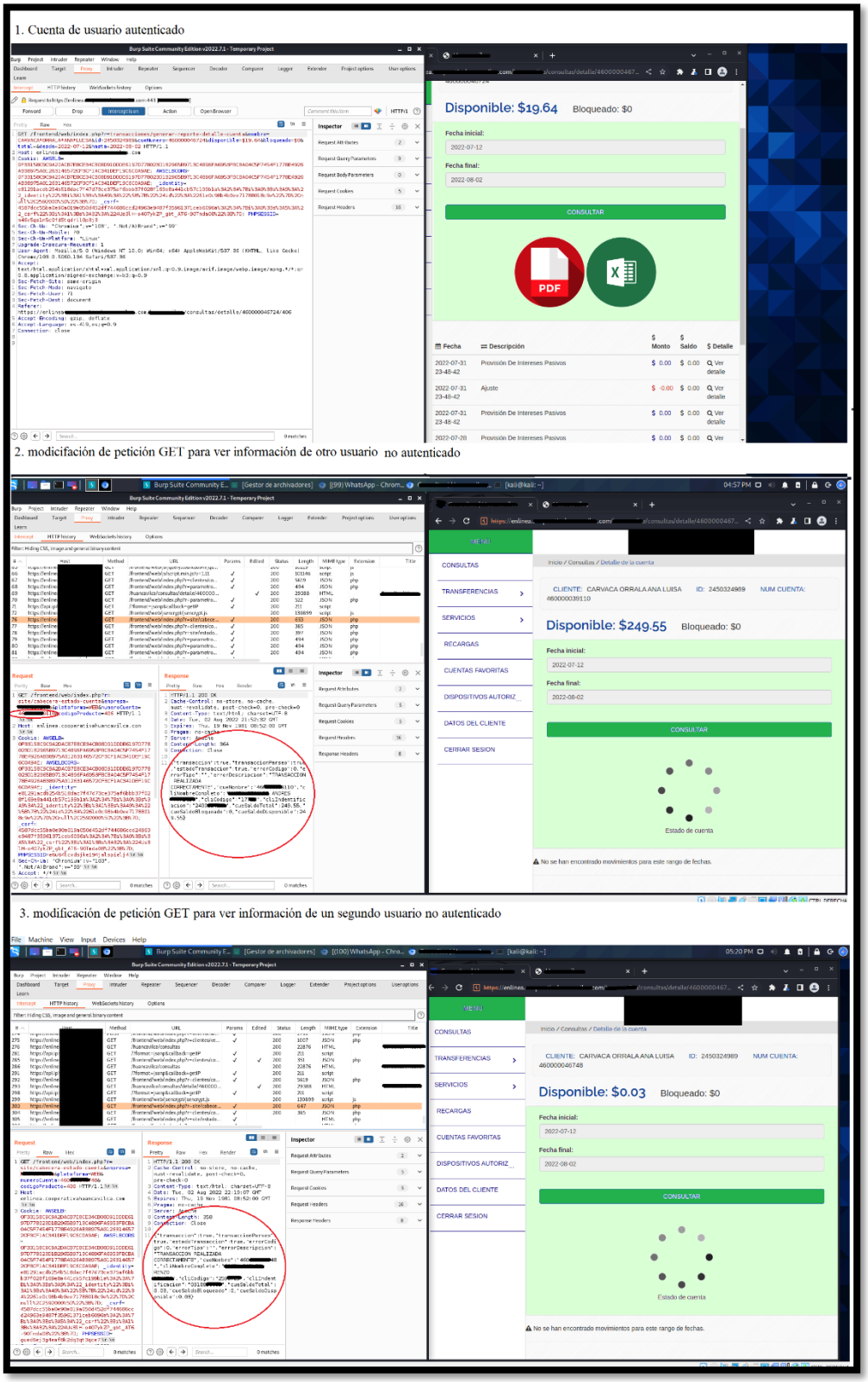


Ilustración 25 Prueba IDOR utilizando proxy BurpSuite

ANEXO 17. PRUEBA DE INYECCIÓN SQL CLÁSICA

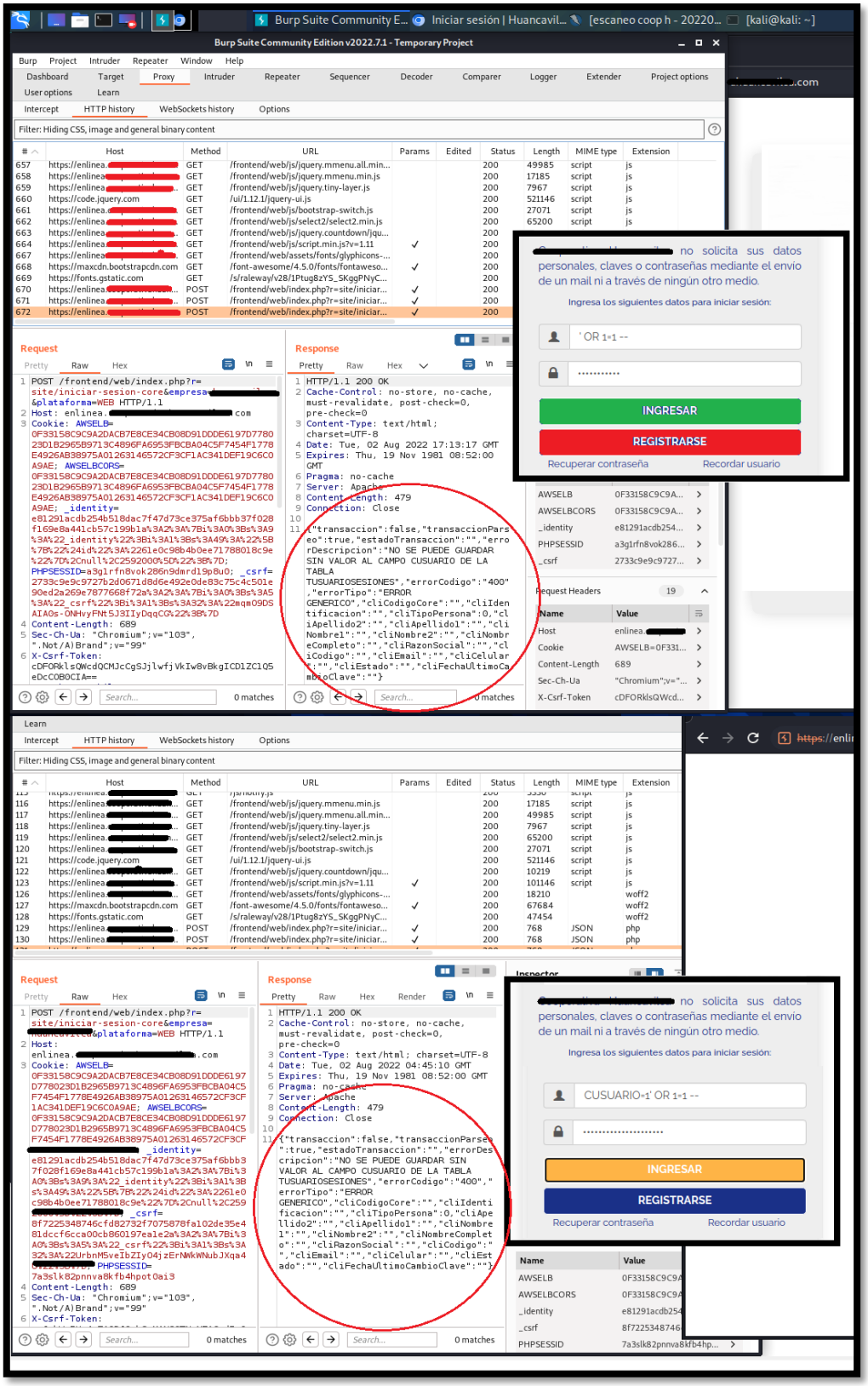


Ilustración 26 Prueba de inyección clásica en el formulario de inicio de sesión

ANEXO 18. PRUEBA DE INYECCIÓN SQL UTILIZANDO LA HERRAMIENTA SQLMAP AL SUBDOMINIO enlinea.sitiowenfinanciero.com/financiero/login

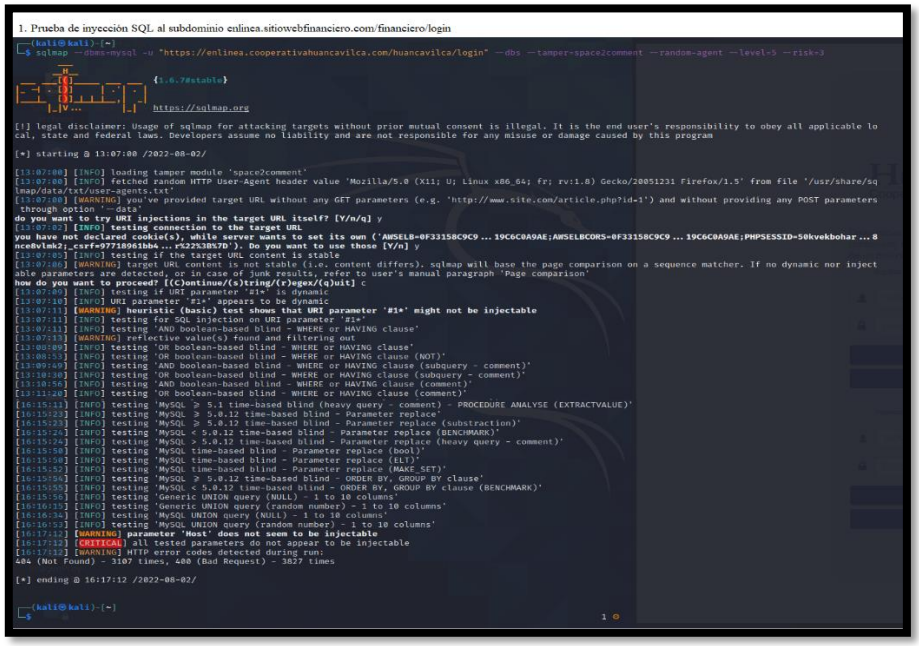


Ilustración 27 Prueba fallida de inyección SQL hacia el subdominio en línea

ANEXO 19. PRUEBA DE INYECCIÓN SQL UTILIZANDO LA HERRAMIENTA SQLMAP AL DOMINIO PRINCIPAL

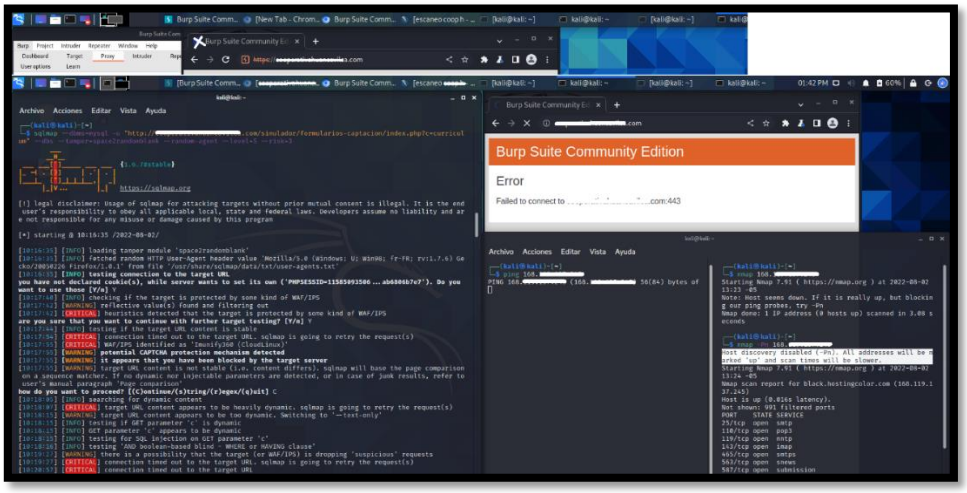


Ilustración 28 Prueba de inyección sobre el dominio

ANEXO 20. PRUEBAS SSRF

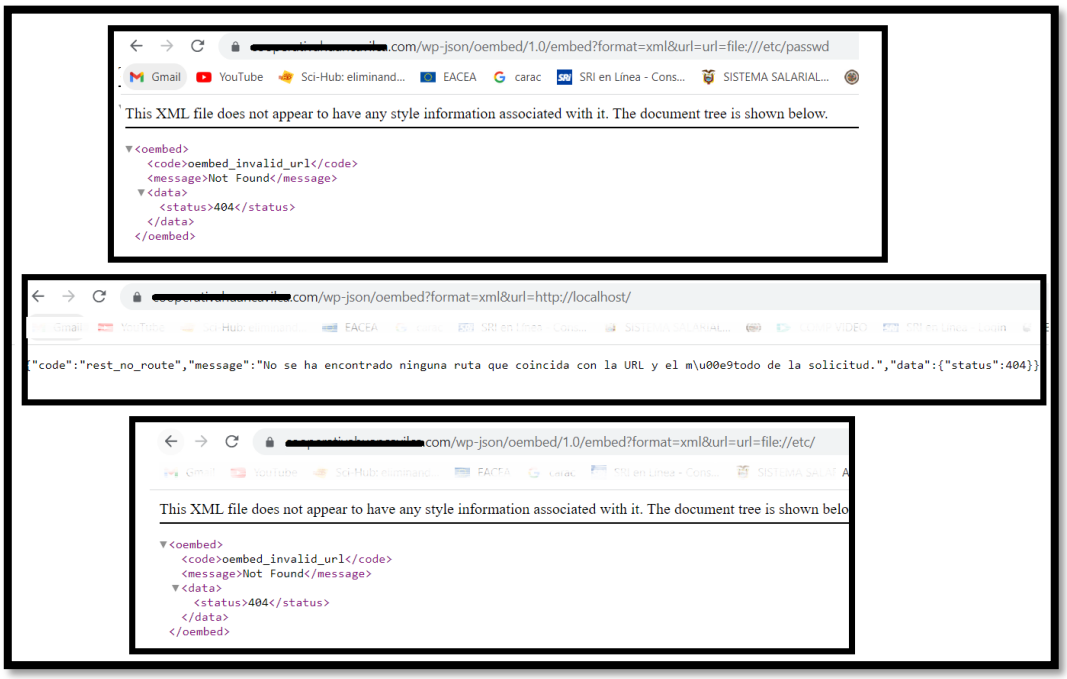


Ilustración 29 Prueba de falsificación de solicitudes al servidor

ANEXO 21. PRUEBAS PARA EVIDENCIAR EL DISEÑO INSEGURO

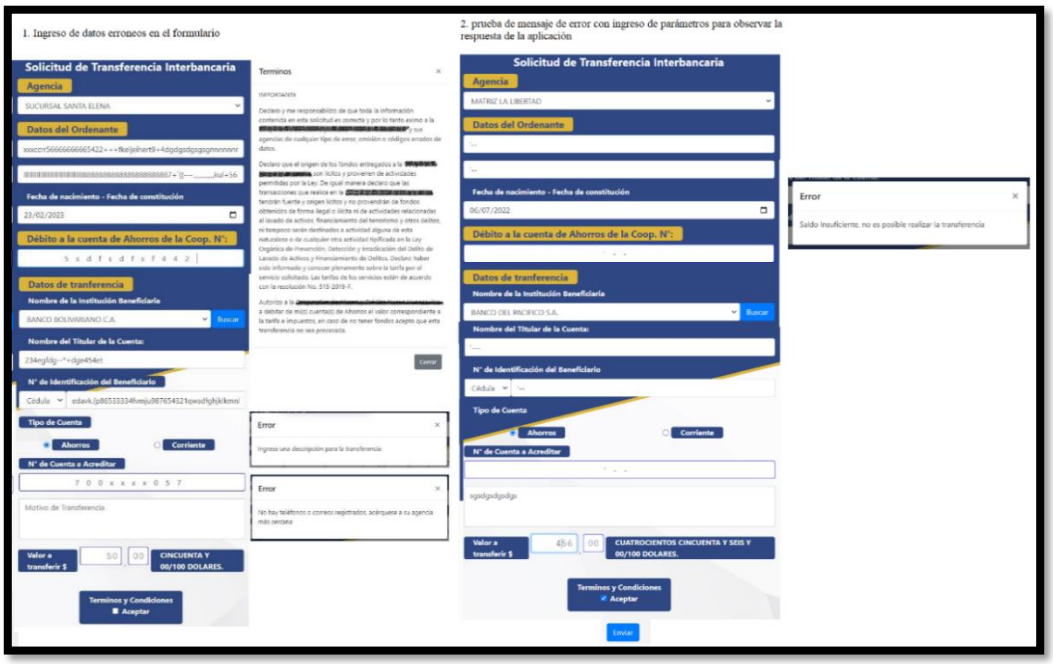


Ilustración 30 Ingreso de datos erróneos para visualizar los mensajes de error

ANEXO 22. PRUEBAS PARA EVIDENCIAR EL DISEÑO INSEGURO EN EL FORMULARIO DE INICIO DE SESIÓN

Ilustración 31 Mensaje de error revela información de los nombres de las tablas de la base de datos

ANEXO 23. REVISIÓN DE LA FUERZA CRIPTOGRÁFICA Y VALIDEZ DE LOS CERTIFICADOS DIGITALES PARA EL DOMINIO PRINCIPAL

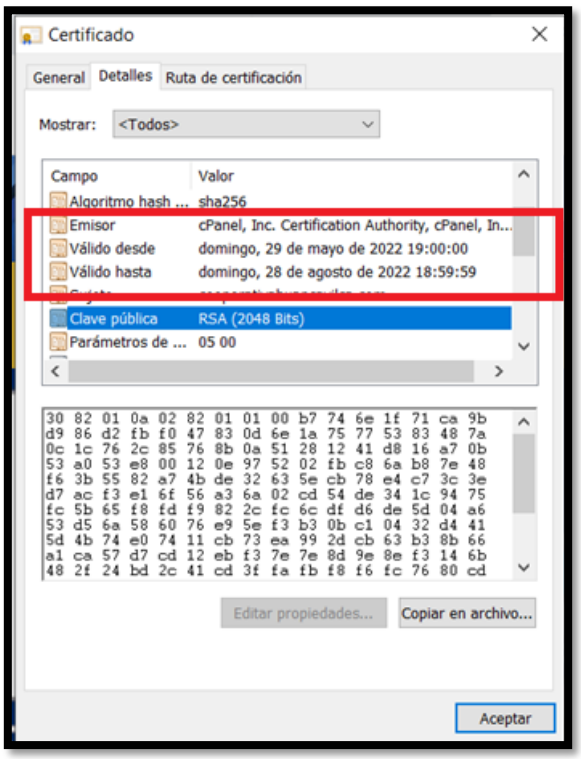


Ilustración 32 Certificado digital del subdominio "en línea"

ANEXO 24. REVISIÓN DE LA FUERZA CRIPTOGRÁFICA Y VALIDEZ DE LOS CERTIFICADOS DIGITALES PARA EL SUBDOMINIO “EN LINEA”

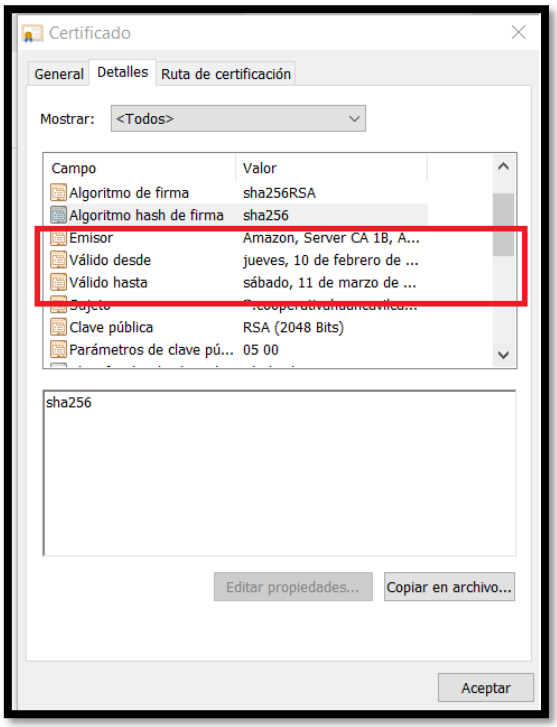


Ilustración 33 Certificado digitan para el subdominio "en línea"

ANEXO 25. PRUEBA DE FALLA DE INTEGRIDAD DE SOFTWARE Y DATOS

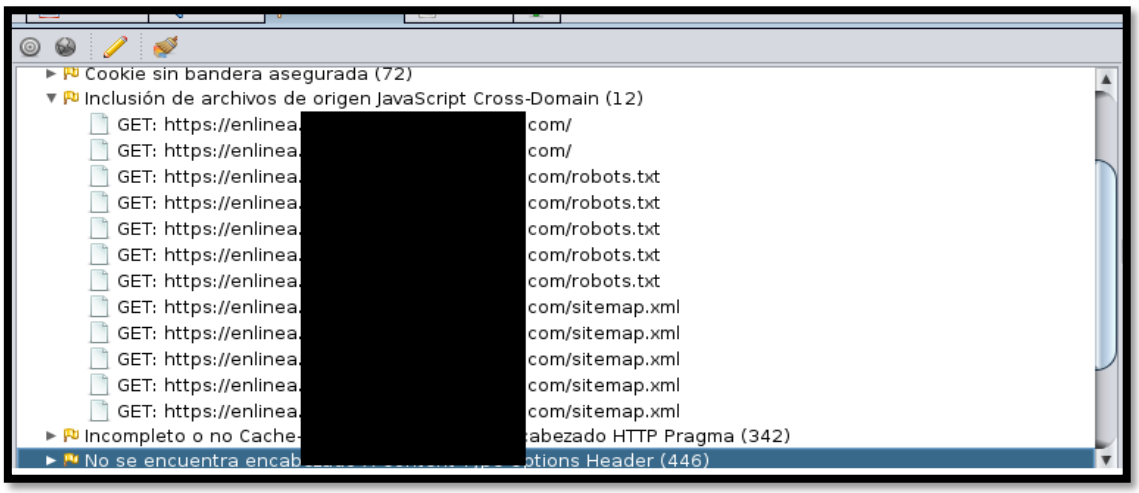


Ilustración 34 Vulnerabilidad de falla de integridad de datos detectada por la herramienta ZAP

ANEXO 26. INFORME FINAL DE PRUEBAS DE SEGURIDAD:

INFORME DE ANÁLISIS DE SEGURIDAD CONTROLADO EN APLICACIONES WEB DE UNA INSTITUCIÓN FINANCIERA

Responsable:

CARVACA ORRALA ANA LUISA

LA LIBERTAD - ECUADOR

2022

1. INTRODUCCIÓN

1.1.CONTROL DE VERSIONES

Versión	Descripción	Fecha	Autor
1.0	Informe de análisis de seguridad de aplicaciones web bajo el Top Ten de OWASP 2021	3 / 08 / 2022	Carvaca Orrala Ana Luisa

1.2.TABLA DE CONTENIDO

1.3.EL EQUIPO

Carvaca Orrala Ana Luisa - Estudiante de la carrera de Tecnologías de la Información de la Universidad Estatal Península de Santa Elena

1.4.ALCANCE

Se realizó un análisis de seguridad controlado sobre las aplicaciones web de la institución financiera para conocer qué tan seguras son ante los riesgos más comunes de seguridad de aplicaciones web. Las pruebas se realizaron en base a la Guía de pruebas de seguridad de aplicaciones web v4.0 y el Top Ten 2021 de OWASP descrito a continuación:

No.	OWASP Top Ten 2021
1	Control de Acceso Roto
2	Fallos de Cifrado
3	Inyección
4	Diseño Inseguro
5	Configuración de Seguridad Incorrecta
6	Componentes Vulnerables y Obsoletos
7	Fallas de Identificación y Autenticación
8	Fallas de Software e integridad de Datos
9	Fallas de Registro y Monitoreo
10	Falsificación de solicitudes del lado del servidor

Cuadro 1 Lista Top 10 de OWASP 2021

1.5.LIMITACIONES

El tiempo destinado para la ejecución de pruebas activas con herramientas de análisis de seguridad fue de cuatro días.

1.6.CRONOLOGÍA

El desarrollo de este análisis de seguridad tuvo un periodo de duración de aproximadamente tres meses, con fecha de inicio del 18 de mayo del 2022 y fecha de finalización el 3 de agosto del 2022, durante el periodo del 18 de mayo al 29 de julio se realizó la recopilación de información y pruebas manuales. Del periodo del 30 de julio al 2 de agosto se realizaron las pruebas activas con herramientas de escaneo de

vulnerabilidades de aplicaciones web, estas pruebas fueron realizadas en el ambiente de producción monitoreadas por el departamento de TI.

2. RESUMEN EJECUTIVO

El objetivo del análisis de seguridad es conocer qué tan segura son las aplicaciones web de la institución financiera ante las vulnerabilidades más importantes de aplicaciones web, y estimar la severidad de los riesgos encontrados que podrían poner en peligro el sistema o información crítica de sus usuarios.

La Superintendencia de Economía Popular y Solidaria dentro de las Normas de Control para las Entidades de los Sectores Financieros Popular y Solidario dentro de las "Recomendaciones para el manejo de información y administración de ciberseguridad en el Sector Financiero Popular y Solidario" establece que las instituciones financieras deben someter sus sistemas electrónicos al menos una vez al año a una revisión de la seguridad de sus activos mediante ejercicios prácticos y controlados, que simulen varios tipos de amenazas posibles, tales como ethical hacking, pentesting, entre otros; exponiendo a la infraestructura que soporta los servicios de la entidad a diferentes escenarios de nivel básico a avanzando en medida de lo posible.

Tras el análisis de seguridad se detecta que las aplicaciones web de la entidad financiera son vulnerables a cinco de los diez riesgos de la lista del Top 10 de OWASP 2021. Las vulnerabilidades encontradas serán abordadas con mayor detalle en orden de criticidad en la sección de hallazgos junto con recomendaciones para mitigarlas.

Estas vulnerabilidades corresponden a los siguientes riesgos del Top 10:

- A01: 2021 – Control de Acceso Roto
- A03: 2021 – Diseño Inseguro
- A05: 2021 – Configuración de Seguridad Incorrecta
- A07: 2021 – Fallas de Identificación y Autenticación
- A08: 2021 – Fallas de Software e Integridad de Datos

Se espera que una vez realizado el análisis de seguridad y presentado el informe, sean atendidas las vulnerabilidades encontradas con el fin de disminuir el riesgo de seguridad, queda a disposición del departamento de TI acoger las recomendaciones otorgadas.

3. HALLAZGOS

3.1.RESUMEN DE HALLAZGOS

En el siguiente cuadro "N" se utilizó para establecer un orden a la tabla, "ID" es el identificador otorgado a la vulnerabilidad antes del análisis de riesgo, "TOP 10" indica el riesgo perteneciente a la lista del OWASP Top 10 al que está relacionado la vulnerabilidad, "VULNERABILIDAD INVOLUCRADA" es el nombre de la vulnerabilidad encontrada durante las pruebas de penetración, y "NIVEL DE RIESGO" indica la severidad del riesgo global estimado para cada vulnerabilidad, ordenado del nivel más crítico al nivel bajo.

N	ID	RIESGO ASOCIADO	VULBERABILIDAD INVOLUCRADA	NIVEL DE RIESGO
1	v11	Fallas de integridad de datos y software	Inclusión de archivos de origen JavaScript Cross-Domain	Crítico
2	V4	Diseño inseguro	Cierre de sesión inadecuado permite recuperar la sesión luego de 10 minutos de inactividad	Crítico
3	V3	Diseño inseguro	Manejo inadecuado de errores revela mensajes de error demasiado informativos	Alto
4	V1	Control de acceso roto	El valor de un objeto se usa directamente para recuperar un registro de la base de Datos de otro usuario	Alto
5	V8	Configuración incorrecta de seguridad	Vulnerabilidad conocida sobre Cookies	Alto
6	V6	Configuración incorrecta de seguridad	Información sensible dentro de comentarios en el código fuente	Medio
7	V9	Fallas de identificación y autenticación	Mecanismo de desbloqueo permite reutilización de contraseñas	Bajo
8	V5	Configuración incorrecta de seguridad	Archivos y directorios de ejemplo conocidos	Bajo
9	V10	Fallas de identificación y autenticación	Todas las identidades registradas no son validadas	Bajo
10	V2	Diseño inseguro	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario	Bajo
11	V7	Configuración incorrecta de seguridad	Inferencia del esquema de nombres utilizado para el contenido publicado	Bajo

Cuadro 2 Lista de vulnerabilidades encontradas según la severidad del riesgo global

DETALLE DE LOS HALLAZGOS

Se utilizó la guía de valoración de riesgo propuesto en la guía de pruebas de seguridad de OWASP v3.0, el modelo estándar para calcular el riesgo es:

Riesgo= Probabilidad de ocurrencia * Impacto

Se utilizaron factores para poder puntuar la probabilidad de ocurrencia global e impacto técnico global. A continuación, se adjuntan tablas de referencia.

ID	NOMBRE DE LA VULNERABILIDAD INVOLUCRADA			
RIESGO	**FACTORES ASOCIADOS A LA VULNERABILIDAD**			
FACILIDAD DE DESCUBRIMIENTO	**Prácticamente imposible (1)**	**difícil (3)**	**fácil (7)**	**existen herramientas automatizadas disponibles (9)**
¿Es fácil descubrir esta vulnerabilidad?				
FACILIDAD DE EXPLOTACIÓN	**En teoría es posible explotarla (1)**	**difícil (3)**	**fácil (5)**	**existen herramientas automatizadas disponibles (9)**
¿Hasta qué punto es fácil para estos atacantes explotar esta vulnerabilidad?				
CONOCIMIENTO DE LA VULNERABILIDAD	**Desconocida (1)**	**oculta (4)**	**obvia (6)**	**se conoce de forma pública (9)**
¿Se trata de una vulnerabilidad muy conocida?				

Cuadro 3 Tabla de referencia para ponderar la probabilidad de ocurrencia de una vulnerabilidad

ID	NOMBRE DE LA VULNERABILIDAD INVOLUCRADA				
RIESGO	**FACTORES ASOCIADOS AL IMPACTO TÉCNICO**				
PÉRDIDA DE CONFIDENCIALIDAD	**Revelación mínima de datos no sensibles (2)**	**revelación mínima de datos críticos (6)**	**amplia revelación de datos no sensibles (6)**	**amplia revelación de datos críticos, todos los datos revelados (9)**	
¿Cuánta información podría ser revelada y cuán delicada es?					
PÉRDIDA DE INTEGRIDAD	**Mínimo datos ligeramente corruptos (1)**	**mínimos datos seriamente dañados (3)**	**gran cantidad de datos ligeramente dañados (5)**	**gran cantidad de datos seriamente dañados (7)**	**todos los datos totalmente corruptos (9)**
¿Cuántos datos se podrían corromper y cuanto sería el daño sufrido?					
PÉRDIDA DE DISPONIBILIDAD	**Mínimo número de servicios secundarios interrumpidos (1)**	**mínimo número de servicios primarios interrumpidos (5)**	**gran número de servicios secundarios interrumpidos (5)**	**gran número de servicios primarios interrumpidos (7)**	**todos los servicios perdidos (9)**
¿Cuántos servicios se pueden ver interrumpidos y cuán vitales son?					

Cuadro 4 Tabla de referencia para ponderar el impacto técnico de una vulnerabilidad

Para calcular la severidad global del riesgo fue necesario poner en conjunto la probabilidad de ocurrencia estimada y el impacto estimado por cada vulnerabilidad. Solo se necesitó comprender si la probabilidad de ocurrencia y el impacto es alta, media o baja según la escala del cero al nueve como lo muestra la tabla 4.

PROBABILIDAD DE OCURRENCIA Y NIVELES DE IMPACTO	
0 a < 3	BAJO
3 a < 6	MEDIO
6 a <9	ALTO

Cuadro 5 Rangos de probabilidad de ocurrencia y niveles de impacto

La severidad del riesgo global se determina según la probabilidad de ocurrencia por el impacto en la escala cualitativa del alta, media o baja, tal como se muestra en la siguiente tabla.

SEVERIDAD DEL RIESGO GLOBAL				
IMPACTO	ALTO	Medio	Alto	Crítico
	MEDIO	Bajo	Medio	Alto
	BAJO	Informativa	Bajo	Medio
		BAJO	MEDIO	ALTO
	PROBABILIDAD DE OCURRENCIA			

Cuadro 6 Tabla guía para estimar la severidad del riesgo global

3.1.1. V11. INCLUSIÓN DE ARCHIVOS DE ORIGEN JAVASCRIPT CROSS DOMAIN

Para estimar la probabilidad de ocurrencia global, en el factor de “FACILIDAD DE DESCUBRIMIENTO” se dio una ponderación de 9 ya que existen herramientas automatizadas que permiten descubrir esta vulnerabilidad, en “FACILIDAD DE EXPLOTACIÓN” se dio una ponderación de 3 debido a que, para explotar esta vulnerabilidad un actor malicioso deberá infectar código en archivos de fuentes “confiables”, y en “CONOCIMIENTO DE LA VULNERABILIDAD” se dio una ponderación de 9 ya existe el Common Weakness Enumeration CWE 829 asociado a esta vulnerabilidad.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Inclusión de archivos de origen JavaScript Cross-Domain	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	3	9
Probabilidad de ocurrencia global		7,00
VALORACIÓN		ALTO

Cuadro 7 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V11

Para estimar el impacto técnico global, en el factor de "PÉRDIDA DE CONFIDENCIALIDAD" se dio una ponderación de 6, "PÉRDIDA DE INTEGRIDAD" una ponderación de 7 y en "PÉRDIDA DE DISPONIBILIDAD" una ponderación de 7, ya que dependiendo del ataque se puede llegar a ejecutar códigos o comandos no autorizados que permitan la inyección de malware, exposición de información sensible, incluso otorgar privilegios que permitan tomar control con permisos de administrador.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Inclusión de archivos de origen JavaScript Cross-Domain	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	7	7
Impacto técnico global		6,67
VALORACIÓN		ALTO

Cuadro 8 Factores para calcular el impacto técnico sobre el riesgo V11

Severidad: Crítica

Recomendación: Asegúrese que los archivos de la fuente JavaScript que se estén utilizando sean solo de sus fuentes confiables, y las fuentes no pueden ser controladas por los usuarios finales de la aplicación. Para revisar más información del CWE 829 puede acceder en el siguiente enlace: https://cwe.mitre.org/data/definitions/829.html.

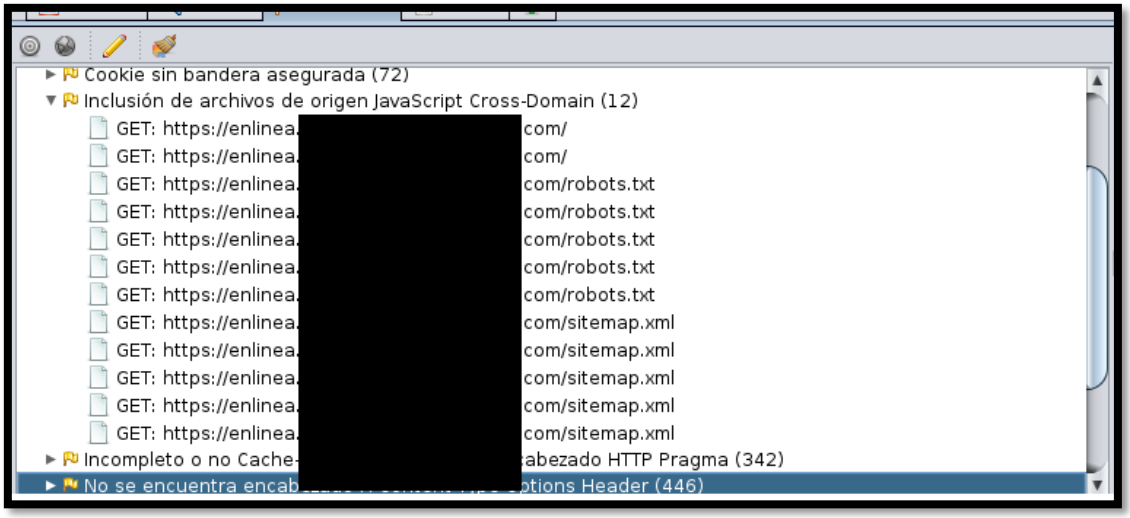


Figura 1 Dominios asociados con la vulnerabilidad JAVASCRIPT CROSS-DOMAIN

3.1.2. V4. CIERRE DE SESIÓN INADECUADO PERMITE RECUPERAR LA SESIÓN LUEGO DE 10 MINUTOS DE INACTIVIDAD

Para estimar la probabilidad de ocurrencia global, en el factor "FACILIDAD DE DESCUBRIMIENTO" se dio una ponderación de 7 ya que fue fácil probar esta vulnerabilidad cerrando las pestañas del navegador sin cerrar sesión adecuadamente y se lo realizó luego de diferentes tiempos para conocer el tiempo máximo de expiración asignada, en el factor "FACILIDAD DE EXPLOTACIÓN" se dio una ponderación de 5 y "CONOCIMIENTO DE LA VULNERABILIDAD" una ponderación de 6 ya que un atacante malicioso conoce que la mayoría de aplicaciones web no implementan los suficientes controles sobre la gestión de sesiones.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Cierre de sesión inadecuado	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	5	6
Probabilidad de ocurrencia global		6,00
VALORACIÓN		ALTO

Cuadro 9 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V4

Para estimar el impacto técnico, en el factor "PÉRDIDA DE CONFIDENCIALIDAD" se dio una ponderación de 9 ya que al recuperar la sesión de un usuario toda su

información bancaria queda expuesta, en el factor "PÉRDIDA DE INTEGRIDAD" se dio una ponderación de 5 y en "PÉRDIDA DE DISPONIBILIDAD" una ponderación de 5.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Cierre de sesión inadecuado	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
9	5	5
Impacto técnico global		6,33
VALORACIÓN		ALTO

Cuadro 10 Factores para calcular el impacto técnico sobre el riesgo V3

Severidad: Crítica

Recomendación: Para mejorar la gestión de sesiones puede implementar un estándar para mejorar la gestión de sesiones de sus aplicaciones. OWASP ofrece el "Estándar de verificación de seguridad en Aplicaciones", en el que comparte una lista de dieciocho requisitos de verificación de gestión de sesiones para mantener la seguridad de aplicaciones.

Para visualizar el estándar puede acceder en el siguiente enlace: https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

3.1.3. V3. MANEJO INADECUADO DE ERRORES REVELA MENSAJES DE ERROR DEMASIADO INFORMATIVOS COMO NOMBRE DE CAMPOS Y NOMBRES DE TABLAS DE LA BASE DE DATOS

Para estimar la probabilidad de ocurrencia, en el factor "FACILIDAD DE DESCUBRIMIENTO" se dio una ponderación de 7 ya que solo fue necesario un intento de inicio de sesión incorrecto para que la aplicación me muestre el mensaje de error, en el factor "FACILIDAD DE EXPLOTACIÓN" pese a que la información del mensaje de error es crítica, se intentó realizar un ataque de inyección SQL, pero no fue exitoso, sin embargo es posible explotarla. En el factor "CONOCIMIENTO DE LA

VULENERABILIDAD” se dio una ponderación de 9 ya que existe un CWE asociado a esta vulnerabilidad.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Manejo inadecuado de errores revela mensajes de error demasiado informativos como nombre de campos y nombres de tablas de la base de datos	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	1	9
Probabilidad de ocurrencia global		5.67
VALORACIÓN		MEDIO

Cuadro 11 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V3

Para estimar el impacto técnico, en el factor “PERDIDA DE CONFIDENCIALIDAD” se dio una ponderación de 9 ya que el mensaje de error muestra el nombre de la tabla y campo de la base de datos de inicio de sesión, en el factor “PÉRDIDA DE INTEGRIDAD” se dio una ponderación de 7 y en el factor “PÉRDIDA DE DISPONIBILIDAD” se dio una ponderación de 5 ya que en el caso de ser explotada se podrían corromper los datos y el daño podría desencadenar servicios primarios interrumpidos.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Manejo inadecuado de errores revela mensajes de error demasiado informativos como nombre de campos y nombres de tablas de la base de datos	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
9	7	5
Impacto técnico global		7.00
VALORACIÓN		ALTO

Cuadro 12 Factores para calcular el impacto técnico sobre el riesgo V3

Severidad: Alta

Recomendación: Asegurarse que los mensajes de error solo muestren la información mínima necesaria para el usuario. Para conocer más sobre el CWE asociado puede acceder al siguiente enlace: https://cwe.mitre.org/data/definitions/209.html

Figura 2 Mensaje de error revela información de los nombres de las tablas de la base de datos

3.1.4. V1. EL VALOR DE UN OBJETO SE USA DIRECTAMENTE PARA RECUPERAR UN REGISTRO DE LA BASE DE DATOS DE OTRO USUARIO

Para estimar la probabilidad de ocurrencia, al factor "FACILIDAD DE DESCUBRIMIENTO" se le dio una ponderación de 7 ya se fue suficiente modificar la URL al identificar que el objeto que utilizada era el número de cuenta del usuario autenticado. En el factor "FACILIDAD DE EXPLOTACIÓN" se dio una ponderación de 5 debido a que solo fue necesario un proxy para interceptar la petición, modificarla y obtener los datos de otros usuarios. En el factor "CONOCIMIENTO DE LA VULNERABILIDAD" se dio una ponderación de 9 ya que existe un CWE asociado a esta vulnerabilidad.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	El valor de un parámetro se usa directamente para recuperar un registro de la base de Datos de otro usuario	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	5	9
Probabilidad de ocurrencia global		7.00
VALORACIÓN		ALTO

Cuadro 13 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V1

Para estimar el impacto técnico, al factor "PÉRDIDA DE CONDIFENCIALIDAD" se dio una ponderación de 6, ya que la información personal de otros usuarios fue expuesta, el factor "PÉRDIDA DE INTEGRIDAD" se le dio una ponderación de 3 y al factor "PÉRDIDA DE DISPONIBILIDAD" una ponderación de 1, ya que la aplicación permitió ver la información de otros usuarios, pero no modificarla, tampoco se vieron servicios comprometidos, sin embargo es posible utilizar la información para realizar otro tipo de ataques.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	El valor de un parámetro se usa directamente para recuperar un registro de la base de Datos de otro usuario	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	3	1
Impacto técnico global		4.33
VALORACIÓN		MEDIO

Cuadro 14 Factores para calcular el impacto técnico sobre el riesgo V1

Severidad: Alta

Recomendación: Evite utilizar patrones simples o números secuenciales para hacer referencia a objetos, cifre la información sensible en tránsito para que un atacante malicioso no pueda ver la información en texto plano. Para conocer más sobre el CWE asociado, puede acceder al siguiente enlace: https://cwe.mitre.org/data/definitions/639.html

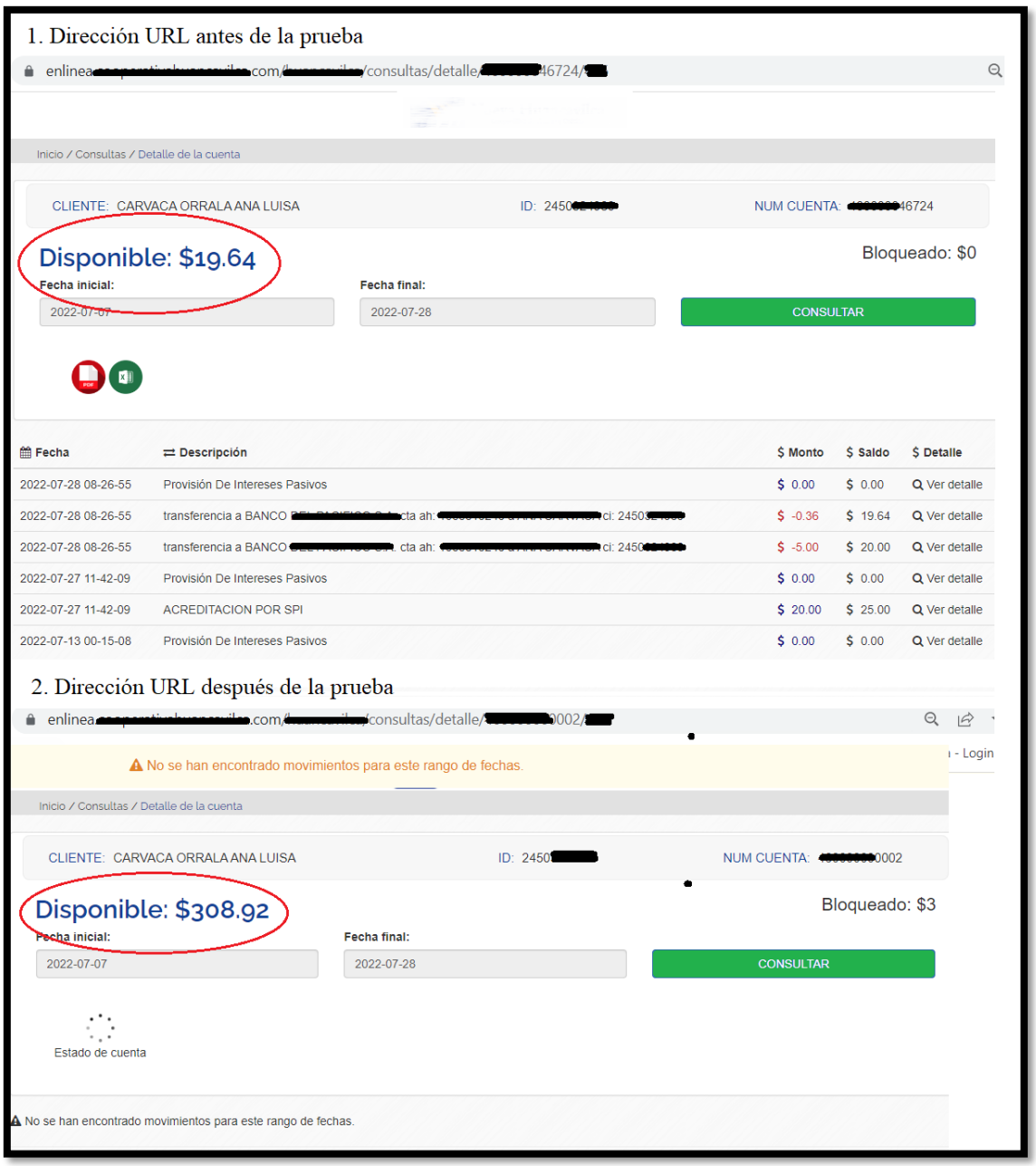


Figura 3 Visualización de información bancaria de otro usuario

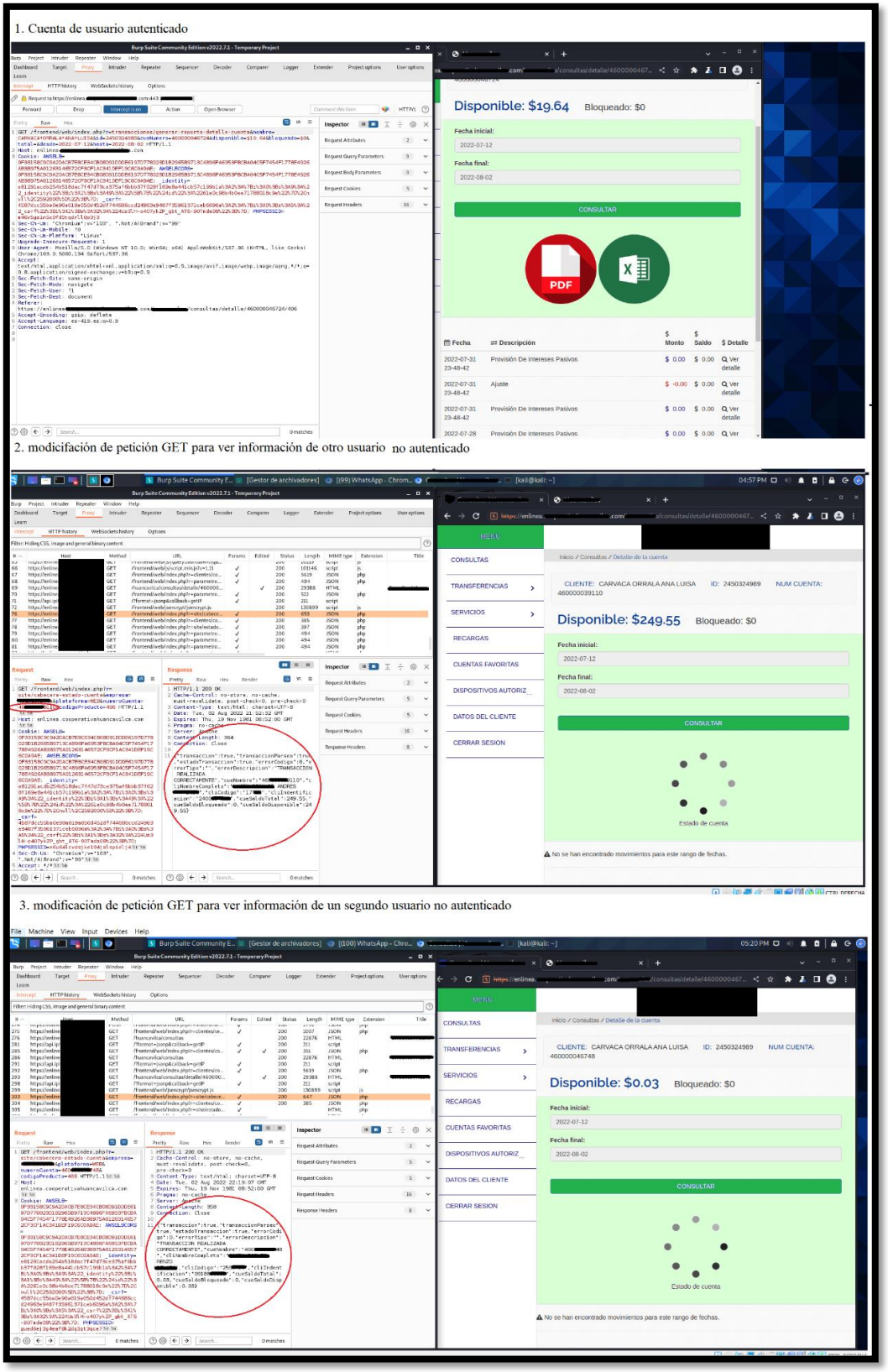


Figura 4 Prueba IDOR utilizando proxy BurpSuite

3.1.5. V8. VULNERABILIDAD CONOCIDA SOBRE COOKIES

Para estimar la probabilidad de ocurrencia, en el factor "FACILIDAD DE DESCUBRIMIENTO" se dio una ponderación de 9 ya que existen herramientas automatizadas para detectar esta vulnerabilidad, en "FACILIDAD DE EXPLOTACIÓN" se dio una ponderación de 3 ya que, para poder explotarla el atacante deberá insertar un script malicioso. Al factor "CONOCIMIENTO DE LA VULNERABILIDAD" se le dio una valoración de 9 ya que existen CWE asociados a esta vulnerabilidad, los cuales son el CWE 16, CWE 614 y CWE 1004.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Vulnerabilidad conocida sobre Cookies	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	3	9
Probabilidad de ocurrencia global		7,00
VALORACIÓN		ALTO

Cuadro 15 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V8

Para estimar el impacto, al factor "PÉRDIDA DE CONFIDENCIALIDAD" se le dio una ponderación de 6, al factor "PÉRDIDA DE INTEGRIDAD" una ponderación de 5 y "PÉRDIDA DE DISPONIBILIDAD" una ponderación de 1, ya que en caso de que el script malicioso pueda ser ejecutado en la aplicación entonces la cookie será accesible y podrá ser transmitida a otro sitio. Si esta es una cookie de sesión entonces el secuestro de sesión podría ser posible.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Vulnerabilidad conocida sobre Cookies	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	5	1
Impacto técnico global		4,00
VALORACIÓN		MEDIO

Cuadro 16 Factores para calcular el impacto técnico sobre el riesgo V8

Severidad: Alta

Recomendación: Asegurarse que la bandera HttpOnly esté establecida para todas las cookies, puede revisar información sobre HttpOnly en el siguiente enlace: https://owasp.org/www-community/HttpOnly y para conocer más información sobre el CWE asociado puede visitar los siguientes enlaces:

https://cwe.mitre.org/data/definitions/16.html
https://cwe.mitre.org/data/definitions/614.html
https://cwe.mitre.org/data/definitions/1004.html

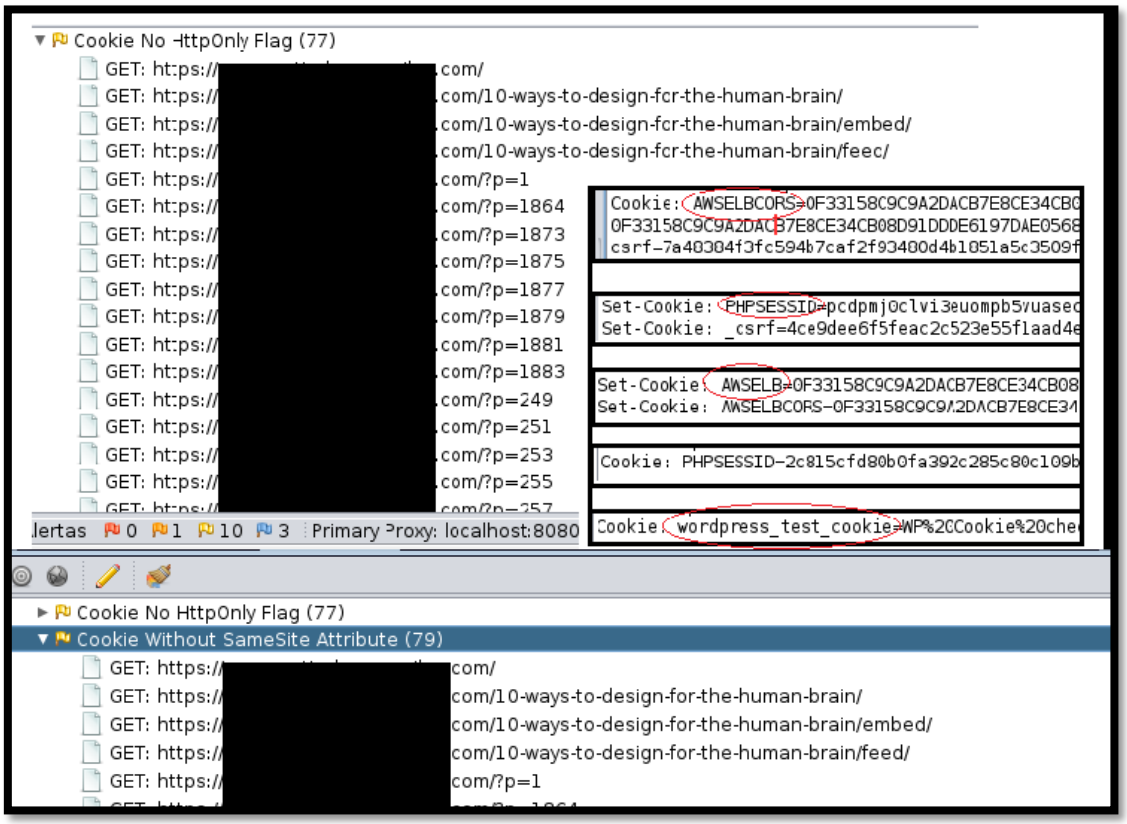


Figura 5 Cookies con nombres predeterminados que revelan el marco utilizado

3.1.6. V6. INFORMACIÓN SENSIBLE DENTRO DE COMENTARIOS EN EL CÓDIGO FUENTE

Para estimar la probabilidad de ocurrencia, al factor "FACILIDAD DE DESCUBRIMIENTO" se le dio una ponderación de 7 ya que fue fácil encontrar estos comentarios dentro del código fuente, al factor "FACILIDAD DE EXPLOTACIÓN" se

le asignó una ponderación de 3 y a “CONOCIMIENTO DE LA VULNERABILIDAD” una ponderación de 4.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Información sensible dentro de comentarios en el código fuente	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	3	4
Probabilidad de ocurrencia global		4,67
VALORACIÓN		MEDIO

Cuadro 17Factores para calcular la probabilidad de ocurrencia sobre el riesgo V6

Para estimar el impacto técnico, al factor “PÉRDIDA DE CONFIDENCIALIDAD” se le asignó una ponderación de 6 por la información sensible encontrada, en el factor “PÉRDIDA DE INTEGRIDAD” una valoración de 5 y a “PÉRDIDA DE DISPONIBILIDAD” una ponderación de 1.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Información sensible dentro de comentarios en el código fuente	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	5	1
Impacto técnico global		4,00
VALORACIÓN		MEDIO

Cuadro 18 Factores para calcular el impacto técnico sobre el riesgo V6

Severidad: Media

Recomendación: Eliminar todos los comentarios que muestren información sensible dentro del código fuente.

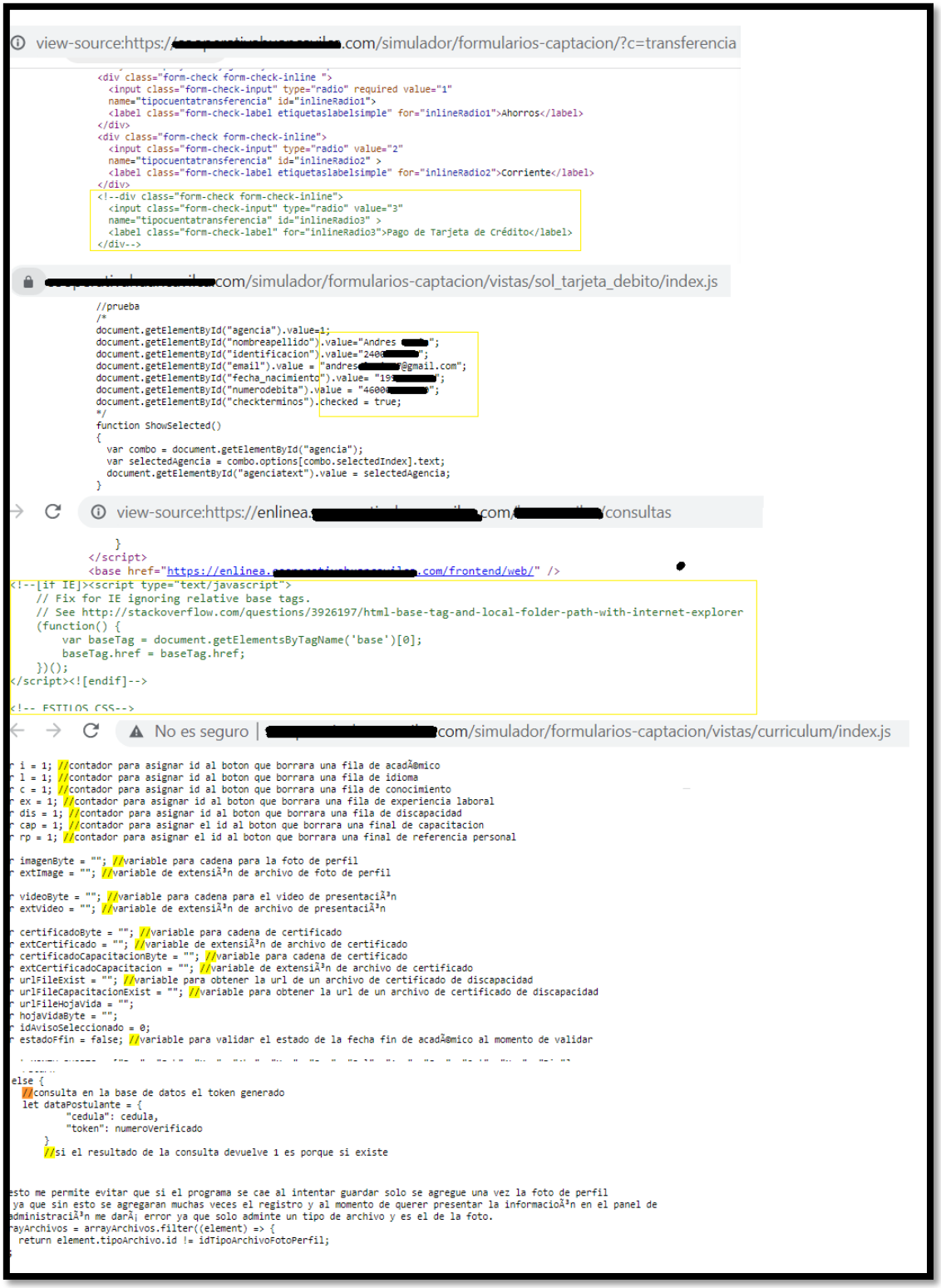


Figura 6 Comentarios con información que debió ser depurada al pasar al ambiente de producción

3.1.7. V10. TODAS LAS IDENTIDADES REGISTRADAS NO SON VALIDADAS

Para estimar la probabilidad de ocurrencia, al factor "FACILIDAD DE DESCUBRIMIENTO" se le dio una ponderación de 7 ya que bastó con hacer pruebas manuales sobre el formulario de registro de usuario, el factor "FACILIDAD DE EXPLOTACIÓN" se le dio una ponderación de 1 y a "CONOCIMIENTO DE LA VULNERABILIDAD" se le dio una ponderación de 4 ya que es una vulnerabilidad muy explotada.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Todas las identidades registradas no son validadas	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	1	4
Probabilidad de ocurrencia global		4,00
VALORACIÓN		MEDIO

Cuadro 19 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V10

Para estimar el impacto técnico, al factor "PÉRDIDA DE CONFIDENCIALIDAD" se le dio una ponderación de 2, "PÉRDIDA DE INTEGRIDAD" una valoración de 3, y "PÉRDIDA DE DISPONIBILIDAD" una valoración de 1, ya que ningún dato fue expuesto durante esta prueba, sin embargo, podría ser posible explotarla.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Todas las identidades registradas no son validadas	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	3	1
Impacto técnico global		2.00
VALORACIÓN		BAJO

Cuadro 20 Factores para calcular el impacto técnico sobre el riesgo V10

Severidad: Baja

Recomendación: Realizar la validación con al menos dos identidades, se recomienda con la identidad “Cédula” y “Número de cuenta”.

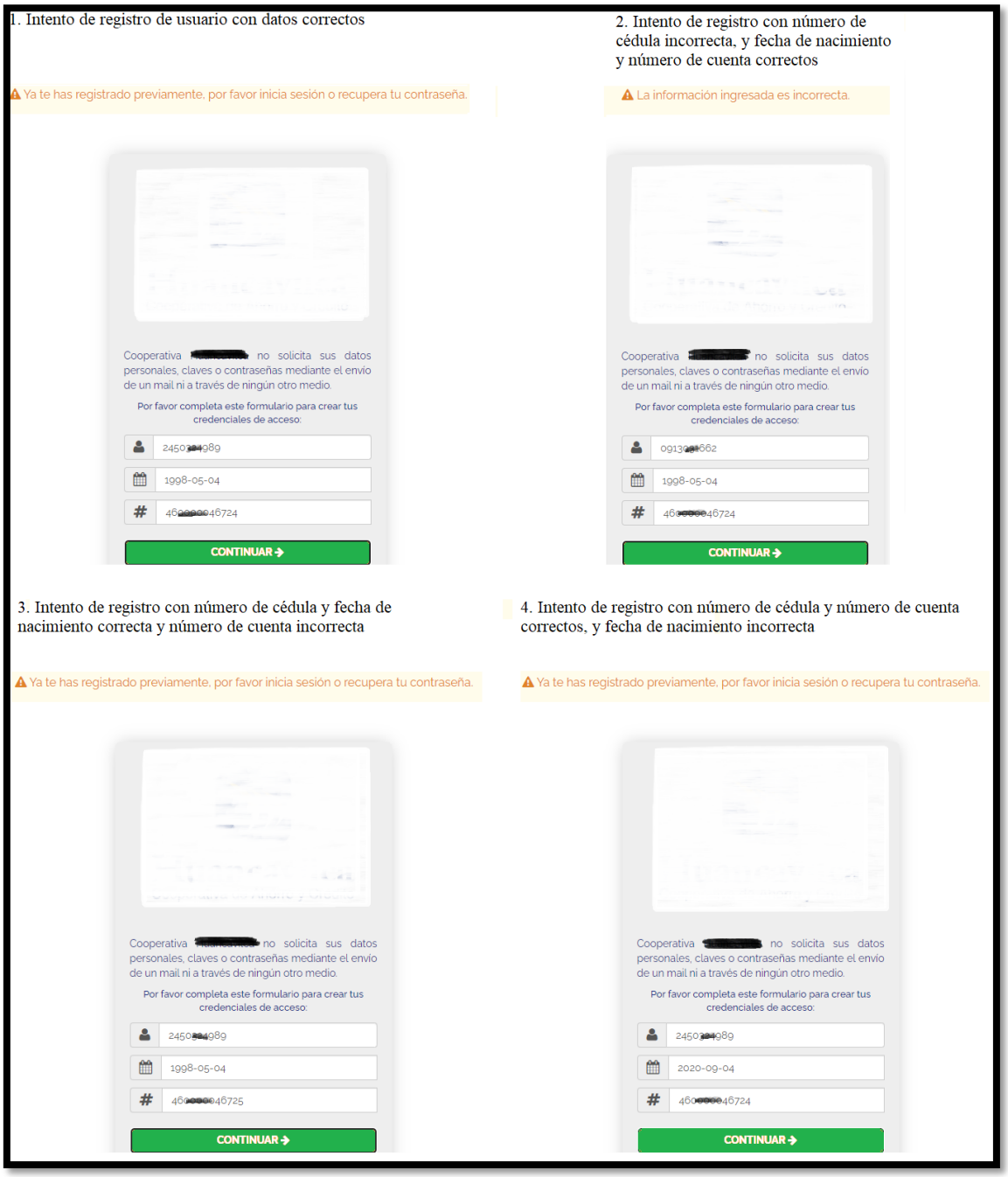


Figura 7 Pruebas de validación de identidad en registro de usuario

3.1.8. V9. MECANISMO DE DESBLOQUEO PERMITE REUTILIZACIÓN DE CONTRASEÑAS

Para Estimar la probabilidad de ocurrencia, al factor "FACILIDAD DE DESCUBRIMIENTO" se le dio una valoración de 7, "FACILIDAD DE EXPLOTACIÓN" una valoración de 3, y "CONOCIMIENTO DE LA VULNERABILIDAD" una valoración de 6, pese a que fue fácil descubrir que la aplicación permite la reutilización de contraseña, será difícil para un atacante conocerlo si no cuenta con credenciales de acceso.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Mecanismo de desbloqueo permite reutilización de contraseñas	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	3	6
Probabilidad de ocurrencia global		5.33
VALORACIÓN		MEDIO

Cuadro 21 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V9

Pasa estimar el impacto técnico, al factor "PÉRDIDA DE CONFIDENCIALIDAD" se le dio una valoración de 6, a "PÉRDIDA DE INTEGRIDAD" Y "PÉRDIDA DE DISPONIBLILIDAD" una valoración de 1.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Mecanismo de desbloqueo permite reutilización de contraseñas	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
6	1	1
Impacto técnico global		2,67
VALORACIÓN		BAJO

Cuadro 22 Factores para calcular el impacto técnico sobre el riesgo V9

Severidad: BAJA

Recomendación: Evite que los usuarios reutilicen credenciales antiguas o conocidas, también puede utilizar diccionarios de contraseñas conocidas para evitar ataques de fuerza bruta o de diccionario.

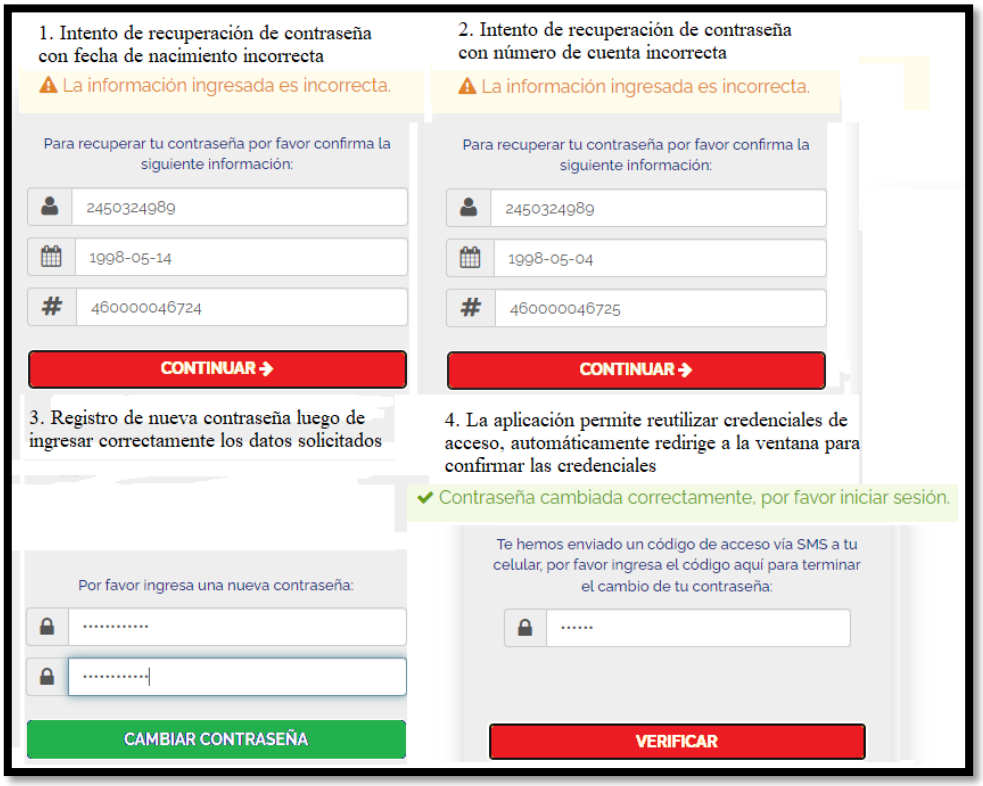


Figura 8 Recuperación de contraseña en la aplicación web

3.1.9. V5. ARCHIVOS Y DIRECTORIOS DE EJEMPLO CONOCIDOS

Para estimar la probabilidad de ocurrencia, en el factor "FACILIDAD DE DESCUBRIMIENTO" se dio una ponderación de 9 ya que se encontró una carpeta con todos los sitios predeterminados al navegar por el sitemap de la aplicación, al factor "FACILIDAD DE EXPLOTACIÓN" se le dio una ponderación de 1 y a "CONOCIMIENTO DE LA VULNERABILIDAD" una ponderación de 6, puesto que estos sitios predeterminados le brindan información de la aplicación en cuanto a estructura y diseño.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Archivos y directorios de ejemplo conocidos	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	1	6
Probabilidad de ocurrencia global		5,33
VALORACIÓN		MEDIO

Cuadro 23 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V5

Para estimar el impacto técnico, al factor "PÉRDIDA DE CONFIDENCIALIDAD" se le dio una ponderación de 2, a "PÉRDIDA DE INTEGRIDAD" una valoración de 1 y a "PÉRDIDA DE DISPONIBILIDAD" 1.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Archivos y directorios de ejemplo conocidos	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	1	1
Impacto técnico global		1,33
VALORACIÓN		BAJO

Cuadro 24 Factores para calcular el impacto técnico sobre el riesgo V5

Severidad: Baja

Recomendación: Oculte o elimine los sitios predeterminados de la aplicación web.

Figura 9 Sitios predeterminados

3.1.10. V2 LA APLICACIÓN NO VALIDA, FILTRA NI DESINFECTA LOS DATOS PROPORCIONADOS POR EL USUARIO

Para estimar la probabilidad de ocurrencia global, al factor "FACILIDAD DE DESCIBRIMIENTO" se le dio una valoración de 7 puesto que solo se llenó los formularios para poder descubrir esta vulnerabilidad, "FACILIDAD DE EXPLOTACIÓN" se le dio una ponderación de 1, y a "CONOCIMIENTO DE LA VULNERABILIDAD" una ponderación de 6.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
7	1	6
Probabilidad de ocurrencia global		4,67
VALORACIÓN		MEDIO

Cuadro 25 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V2

Para estimar el impacto técnico, al factor "PÉRDIDA DE CONFIDENCIALIDAD" se le dio una ponderación de 2, "PÉRDIDA DE INTEGRIDAD" una ponderación de 1 y a "PÉRDIDA DE DISPONIBILIDAD" una ponderación de 1.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	1	1
Impacto técnico global		1.33
VALORACIÓN		BAJO

Cuadro 26 Factores para calcular el impacto técnico sobre el riesgo V2

Severidad: Baja

Recomendación: Aplique validaciones en todos los formularios donde el usuario ingresa datos, limitando a que ingrese solo la información necesaria. No permita el ingreso de caracteres especiales.

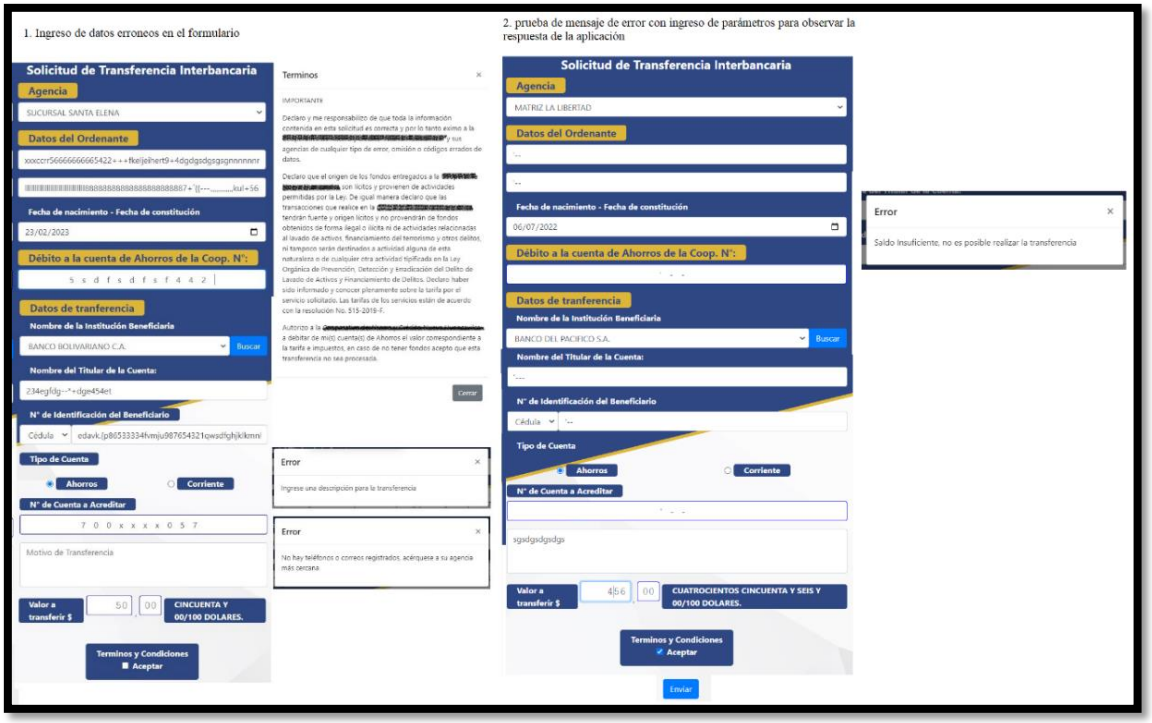


Figura 10 Ingreso de datos erróneos para visualizar los mensajes de error

3.1.11. V7. INFERENCIA DEL ESQUEMA DE NOMBRES UTILIZADO PARA EL CONTENIDO PUBLICADO

Para estimar la probabilidad de ocurrencia, al factor "FACILIDAD DE ESCUBRIMIENTO" se le dio una ponderación de 9, "FACILIDAD DE EXPLOTACIÓN" una ponderación de 3, y "CONOCIMIENTO DE LA VULNERABILIDAD" una ponderación de 1. Esta prueba trata de la estructura que utiliza la URL para acceder a una ruta de acceso en específico, muchas de ellas con direcciones o nombres obvias como /admin.

FACTORES ASOCIADOS A LA VULNERABILIDAD		
RIESGO	Inferencia del esquema de nombres utilizado para el contenido publicado	
FACILIDAD DE DESCUBRIMIENTO	**FACILIDAD DE EXPLOTACIÓN**	**CONOCIMIENTO DE LA VULNERABILIDAD**
9	3	1
Probabilidad de ocurrencia global		4,33
VALORACIÓN		MEDIO

Cuadro 27 Factores para calcular la probabilidad de ocurrencia sobre el riesgo V7

Para estimar el impacto técnico, el factor “PERDIDA DE CONFIDENCIALIDAD” tuvo una valoración de 2, “PÉRDIDA DE INTEGRIDAD” una valoración de 1, y “PERDIDA DE DISPONIBILIDAD” una valoración de 1.

FACTORES ASOCIADOS AL IMPACTO TÉCNICO		
RIESGO	Inferencia del esquema de nombres utilizado para el contenido publicado	
PÉRDIDA DE CONFIDENCIALIDAD	**PÉRDIDA DE INTEGRIDAD**	**PÉRDIDA DE DISPONIBILIDAD**
2	1	1
Impacto técnico global		1,33
VALORACIÓN		BAJO

Cuadro 28 Factores para calcular el impacto técnico sobre el riesgo V7

Severidad: Baja

Recomendación: Evite utilizar un esquema de nombres demasiado obvio que permita al atacante inferir en el nombre o ubicación de páginas no referenciadas como /admin.

1	https:// sitiowebfinanciero.com/solicitud-de-reclamo/	25	https:// sitiowebfinanciero.com/videos-concursos/
2	https:// sitiowebfinanciero.com/quienes-somos/	26	https:// sitiowebfinanciero.com/inscripcion-club-ahorro/
3	https:// sitiowebfinanciero.com/contactos/	27	https:// sitiowebfinanciero.com/club-del-ahorro/
4	https:// sitiowebfinanciero.com/depositos-a-plazo-fijo/	28	https:// sitiowebfinanciero.com/simulador-de-ahorros/
5	https:// sitiowebfinanciero.com/directivos/	29	https:// sitiowebfinanciero.com/huancavilca-en-linea/
6	https:// sitiowebfinanciero.com/proteccion-derecho-de-socios-informe/	30	https:// sitiowebfinanciero.com/ahorro-a-la-vista/
7	https:// sitiowebfinanciero.com/proteccion_derechos_socios/	31	https:// sitiowebfinanciero.com/credigrupo/
8	https:// sitiowebfinanciero.com/trabajeconnosotros/	32	https:// sitiowebfinanciero.com/la-hormiguita-saving/
9	https:// sitiowebfinanciero.com/solicitud-de-credito/	33	https:// sitiowebfinanciero.com/fondos-de-reserva/
10	https:// sitiowebfinanciero.com/credito-emergente/	34	https:// sitiowebfinanciero.com/plan-de-ahorro-decimos/
11	https:// sitiowebfinanciero.com/creditos-institucionales/	35	https:// sitiowebfinanciero.com/pago-de-servicios/
12	https:// sitiowebfinanciero.com/credinversion/	36	https:// sitiowebfinanciero.com/supa/
13	https:// sitiowebfinanciero.com/microcredito/	37	https:// sitiowebfinanciero.com/tarjeta-de-debito/

14	https:// sitiowebfinanciero.com/credito-de-consumo/	38	https:// sitiowebfinanciero.com/sistema-de-pagos-interbancarios/
15	https:// sitiowebfinanciero.com/formulario-quejas/	39	https:// sitiowebfinanciero.com/pagos-y-envio-de-dinero/
16	https:// sitiowebfinanciero.com/simulador-credito/	40	https:// sitiowebfinanciero.com/pago-de-nomina/
17	https:// sitiowebfinanciero.com/solicitud-de-tarjeta-de-debito/	41	https:// sitiowebfinanciero.com/cajero-automatico/
18	https:// sitiowebfinanciero.com/ruleta/	42	https:// sitiowebfinanciero.com/historia/
19	https:// sitiowebfinanciero.com/depositos-seguros-con-la-cosede/	43	https:// sitiowebfinanciero.com/recaudacion-movil/
20	https:// sitiowebfinanciero.com/solicitud_transferencia/	44	https:// sitiowebfinanciero.com/organismos-de-control/
21	https:// sitiowebfinanciero.com/mi-futuro-seguro/	45	https:// sitiowebfinanciero.com/ley-de-transparencia/
22	https:// sitiowebfinanciero.com/cuenta-juvenil/	46	https:// sitiowebfinanciero.com/organigrama/
23	https:// sitiowebfinanciero.com/cuenta-infantil/	47	https:// sitiowebfinanciero.com/balances/
24	https:// sitiowebfinanciero.com/videos-concursos-jovenes/	48	https:// sitiowebfinanciero.com/inicio-2/

Cuadro 29 Esquema de nombres utilizado

3.1.12. SEVERIDAD DEL RIESGO GLOBAL

A continuación, se muestra un mapa de calor sobre la severidad del riesgo global para brindar un mayor entendimiento de la criticidad de las vulnerabilidades encontradas.

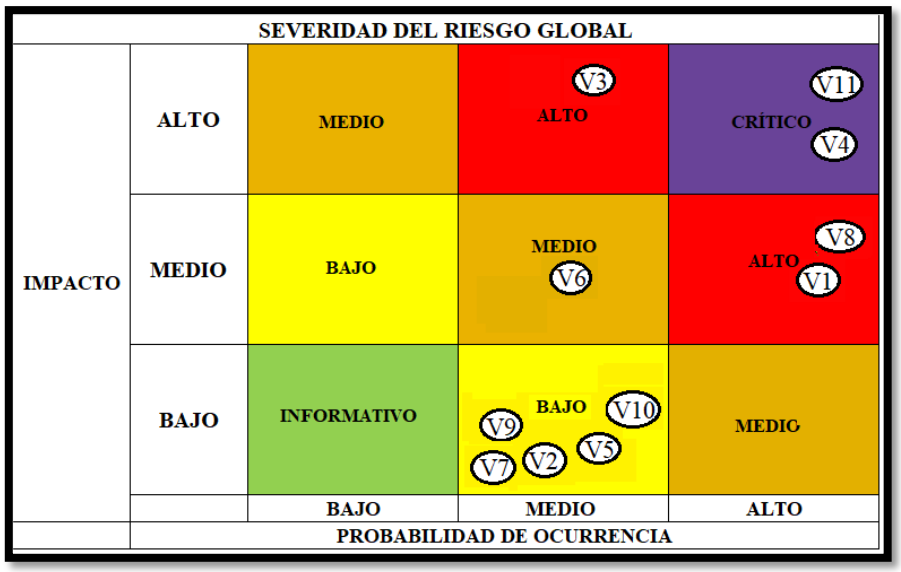


Figura 11 Severidad del riesgo global

La Libertad, 11 de octubre de 2022

CERTIFICADO ANTIPLAGIO
001-TUTOR IACS-2022

En calidad de tutor del trabajo de titulación denominado **"ANÁLISIS DE SEGURIDAD CONTROLADO EN APLICACIONES WEB DE UNA INSTITUCIÓN FINANCIERA UTILIZANDO HERRAMIENTAS DE CIBERSEGURIDAD Y BUENAS PRÁCTICAS DE OWASP"**, elaborado por la estudiante, **ANA LUISA CARVACA ORRALA**, egresada de la Carrera de Tecnologías de la Información, de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniera en Tecnologías de la Información, me permito declarar que una vez analizado en el sistema antiplagio URKUND, luego de haber cumplido los requerimientos exigidos de valoración, el presente proyecto ejecutado, se encuentra con 1% de la valoración permitida, por consiguiente se procede a emitir el presente informe.

Ouriginal

Document Information

Analyzed document	COMPONENTE TEORICO - ACO para impresión.pdf (D146165479)
Submitted	2022-10-11 22:07:00
Submitted by	
Submitter email	ana.carvacaorrala@upse.edu.ec
Similarity	1%
Analysis address	ouriginal.upse@analysis.urkund.com

Sources included in the report

SA	**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA / TESIS-BRENDA.docx** Document TESIS-BRENDA.docx (D132487381) Submitted by: ouriarc@upse.edu.ec Receiver: ouriarc.upse@analysis.urkund.com	1
SA	**INFORME FINAL TESIS - Bryan Muñoz.docx** Document INFORME FINAL TESIS - Bryan Muñoz.docx (D149410457)	1
SA	**informe OWASP.docx** Document informe OWASP.docx (D146667386)	2
SA	**tesis final 1.docx** Document tesis final 1.docx (D145145329)	1
SA	**G7OWASP.docx** Document G7OWASP.docx (D62229347)	2

Atentamente,

Ing. Coronel Suárez Iván Alberto, MSIA.
C.I.:0917255978
DOCENTE TUTOR