ANÁLISIS DE VULNERABILIDADES EN LOS PORTALES WEB PARA UNA ORGANIZACIÓN DEL SECTOR DE SERVICIOS FUNERARIOS.

José Ferney Nieto López, Andrés Iván Alarcón Ariza, Diego Alejandro Duarte Jiménez

Especialización en Seguridad Informática, Fundación Universitaria Compensar

Propuesta de Consultoría

Jaime Andrés Chaparro Sánchez

Director (a):

27 de mayo de 2024

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

ANÁLISIS DE VULNERABILIDADES EN LOS PORTALES WEB PARA UNA ORGANIZACIÓN DEL SECTOR DE SERVICIOS FUNERARIOS.

José Ferney Nieto López
Andrés Iván Alarcón Ariza
Diego Alejandro Duarte Jiménez

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista en Seguridad Informática

Director (a):

Ingeniero(a), Jaime Andrés Chaparro Sánchez

Codirector (a):

Ingeniería y Tecnología del Software:

Seguridad informática

Fundación Universitaria Compensar

Facultad de Ingeniería, Especialización en Seguridad Informática

Bogotá, Colombia

2024

Resumen

El presente documento describe el proceso de análisis de vulnerabilidades realizado en los portales web de clientes y empleados en una organización del sector de servicios funerarios, este análisis se realizará mediante la aplicación OWASP ZAP, reconocida por su eficacia en la detección de amenazas de seguridad en aplicaciones web, entregando así un informe detallado que documente todos los hallazgos identificados. El mismo, contendrá recomendaciones para abordar y mitigar las brechas de seguridad.

Este análisis de vulnerabilidades se llevará a cabo siguiendo las mejores prácticas recomendadas por la norma ISO 27002:2022, un estándar internacionalmente reconocido en gestión de seguridad de la información.

Palabras clave: Obsolescencia, Vulnerabilidades, Owasp, Análisis, estándares, buenas prácticas.

Abstract

This document describes the vulnerability analysis process conducted on the client and employee web portals of an organization in the funeral services sector, this analysis will be performed using the OWASP ZAP application, recognized for its effectiveness in detecting security threats in web applications, thus delivering a detailed report documenting all the findings identified. The report will contain recommendations to address and mitigate the security breaches.

This vulnerability analysis will be carried out following the best practices recommended by ISO 27002:2022, an internationally recognized standard in information security management.

Keywords: Obsolescence, Vulnerabilities, Owasp, Analysis, standards, good practices.

Contenido

PÁG.

RESUMEN **3**

INTRODUCCIÓN **5**

ANTECEDENTES Y JUSTIFICACIÓN 6

FORMULACIÓN DEL PROBLEMA 7

OBJETIVO GENERAL 7

Objetivos Específicos *7*

ALCANCES Y LIMITACIONES 7

1. MARCO TEÓRICO **9**

1.1 SEGURIDAD DE APLICACIONES WEB 10

1.2 ANÁLISIS DE VULNERABILIDADES 10

1.3 OWASP ZAP 10

1.4 NORMATIVAS Y ESTÁNDARES 11

1.5 GESTIÓN DEL RIESGO 11

2. DISEÑO METODOLÓGICO **12**

2.1 CONFIGURACIÓN Y PREPARACIÓN: 12

2.2. ESCANEO DE VULNERABILIDADES: 13

2.3. ENTREGA DE REPORTE: 13

3. RESULTADOS LOGRADOS **14**

4. CONCLUSIONES Y RECOMENDACIONES **19**

4.1 CONCLUSIONES 19

4.2 RECOMENDACIONES 20

5. BIBLIOGRAFÍA **21**

Introducción

Este documento presenta el análisis de vulnerabilidades que se llevará a cabo en una organización del sector de servicios funerarios, centrándose en el portal web destinado a clientes y empleados. Esta evaluación se ha diseñado en cumplimiento con las normas de seguridad de la información ISO 27002:2022, con el objetivo de evaluar e identificar las posibles brechas de seguridad que actualmente puedan existir en los portales web.

En el entorno actual de amenazas digitales en constante evolución, la seguridad de la información es muy importante. La empresa como parte de su compromiso continuo con la protección de los activos digitales y la confidencialidad de la información de los clientes y partes interesadas, desea realizar una revisión de sus entornos web.

Esta evaluación abarca aspectos clave, como la identificación del estado actual de los portales web críticos y el análisis exhaustivo de sus vulnerabilidades y amenazas. Los resultados ofrecerán una visión detallada de la situación actual de los portales, identificando las oportunidades de mejora en la evaluación realizada. Además, se proporcionarán recomendaciones detalladas y un plan de acción con el fin de abordar las debilidades identificadas y avanzar cuidadosamente en la construcción de los nuevos portales web, Esto permitirá a la empresa tomar decisiones informadas y estratégicas para fortalecer su postura en seguridad frente a los portales web.

Este proceso de evaluación y mejora es un reflejo del compromiso de la organización con la seguridad de la información y su enfoque en cumplir con los estándares internacionales. Agradecemos a todos los involucrados en este esfuerzo y confiamos en que este documento sirva como guía esencial para la gestión continuada de la seguridad de la información.

Antecedentes y Justificación

A continuación, se proporciona una visión completa y profunda de los portales web actuales en una organización del sector de servicios funerarios. Esto incluye una descripción detallada de los servicios, software y, estructura de los portales. En esta evaluación detallada se entenderán los activos en juego, sus capacidades y limitaciones. A partir de esta visión general, la compañía estará mejor preparada para tomar decisiones informadas y estratégicas sobre el futuro de los portales clientes y empleados.

Por este motivo la organización debe garantizar que sus portales web cumplan con los más altos estándares en seguridad de la información, de acuerdo con los definidos en las normas ISO 27000 (NormasISO.org, 2023). Esto no solo busca prevenir posibles pérdidas de credibilidad, datos y recursos financieros, sino también salvaguardar la confianza de sus clientes y socios comerciales, así como mantener su competitividad en un entorno empresarial cada vez más exigente y tecnológicamente avanzado.

En vista del creciente número de incidentes de hackeo en organizaciones públicas y privadas de acuerdo con la información suministrada por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2022 en donde informan que: "*El Ministerio de Tecnologías de la Información y las Comunicaciones a través del Equipo de Respuesta a Emergencias Cibernéticas de Colombia -COLCERT, ha recibido en el último mes y medio 36 reportes de incidentes de ciberseguridad siendo la suplantación de sitios web, con 19 reportes…*" es esencial que la organización. esté preparada para abordar y mitigar las vulnerabilidades reportadas por los fabricantes e identidades especializadas en el campo de la seguridad. Esto implica no solo la capacidad de identificar y corregir las vulnerabilidades de manera oportuna, sino también implementar medidas proactivas para fortalecer constantemente las defensas de seguridad de la organización.

La organización cuenta con una amplia base de clientes, superando los 165.000, así mismo, más de 25 sedes distribuidas a nivel nacional y más de 300 empleados. Entre algunos de estos, se encuentran entidades de gran importancia como la Policía Nacional, la Fiscalía General de la Nación, la DIAN, el INPEC, y otras más. Estos clientes confían en la empresa para garantizar la seguridad y la privacidad de sus datos personales. Es su derecho contar con un entorno en línea seguro y protegido donde puedan acceder y gestionar su información de manera confiable.

Por otro lado, de acuerdo con el reporte de ataques recopilado por los firewalls de la compañía en los últimos 6 meses, se observa un total de 172 intentos de ataques dirigidos

específicamente a los portales web de la organización. Este hallazgo representa una señal de alarma significativa, indicando la posibilidad latente de que estos intentos de intrusión se materialicen en ataques reales contra los portales web de la empresa.

Formulación del Problema

La organización reconoce la obsolescencia tecnológica que enfrenta en la actualidad, la cual genera múltiples limitaciones al no poder acceder a las ultimas funcionalidades y parches de seguridad más recientes, afectando directamente al funcionamiento de los portales web, comprometiendo la operatividad de la compañía y su capacidad de crecimiento a largo plazo.

La falta de una infraestructura actualizada impide la implementación de las mejores prácticas recomendadas por los fabricantes, como las actualizaciones de software y compatibilidad con aplicaciones o sistemas operativos.

Considerando la obsolescencia tecnológica que enfrenta la organización y su interés en proteger sus portales web, surge la pregunta crucial: **¿Puede este escaneo de vulnerabilidades realmente identificar las brechas de seguridad existentes en estos portales?**

Objetivo General

Realizar un análisis de vulnerabilidades enfocado en seguridad de la información en los portales web de clientes y empleados en una organización del sector de servicios funerarios.

Objetivos Específicos

- Diseñar la metodología para el análisis de vulnerabilidades, enfocada en la identificación de posibles brechas de seguridad en los portales web de la organización.
- Confirmar que OWASP ZAP es la herramienta idónea para el escaneo de vulnerabilidades, reconocida por su eficacia en la detección de brechas de seguridad en diversos sitios web.
- Identificar las recomendaciones técnicas generales que ayuden a la organización a abordar y mitigar las vulnerabilidades detectadas en los portales web.

Alcances y Limitaciones

Alcance

Este documento presenta el proyecto para el análisis de vulnerabilidades en los portales web de clientes y empleados en una organización del sector de servicios funerarios, por medio de la herramienta OWASP ZAP, con el fin de identificar posibles brechas de seguridad, que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Como resultado, se entregará un informe con sugerencias y medidas preventivas para mitigar los riesgos identificados.

El análisis de vulnerabilidades propuesto en este proyecto es una etapa inicial dentro de un macroproyecto. Dicho macroproyecto tiene como objetivo principal migrar la infraestructura tecnológica a la nube, con el fin de abordar los problemas de obsolescencia del hardware actual.

Limitaciones

1. La entrega de los resultados podría retrasarse debido a la complejidad de las pruebas, la disponibilidad de recursos o cualquier otro factor imprevisto.

2. Dado que las pruebas deben ser no intrusivas para no afectar la operación de la compañía, puede que algunas vulnerabilidades no se detecten o no se obtengan resultados completos por limitaciones técnicas o de acceso.

3. Aunque se identifiquen vulnerabilidades durante las pruebas, es posible que algunas de ellas no tengan una solución inmediata o que su mitigación requiera acciones adicionales que no estén dentro del alcance del proyecto.

4. Si el cliente restringe el acceso a ciertos recursos por motivos de confidencialidad, podría limitar la capacidad de realizar las pruebas.

5. Los resultados detallados del análisis de vulnerabilidades, que contienen información confidencial, no se incluirán en este documento para preservar la integridad de la compañía. En cambio, serán entregados directamente a la misma.

1. Marco teórico

En el entorno digital actual, caracterizado por la creciente amenaza de ataques cibernéticos y violaciones de seguridad, las organizaciones enfrentan el desafío de proteger la confidencialidad, integridad y disponibilidad de sus sistemas y datos. Las aplicaciones web, debido a su naturaleza abierta y disponibilidad pública, representan un vector de ataque crítico que requiere medidas proactivas de identificación y mitigación de vulnerabilidades. (Stuttard, 2007) En este contexto, el uso de herramientas como OWASP Zed Attack Proxy (ZAP) es fundamental para realizar un análisis integral de vulnerabilidades y mejorar la postura de seguridad de una organización. (The OWASP Foundation, s.f.)

La ciberseguridad se rige por principios fundamentales como la confidencialidad, la integridad, la disponibilidad, la autenticación y la gestión de riesgos (Whitman & Mattord, 2017). Estos conceptos básicos sientan las bases para crear un sistema de seguridad sólido. Las herramientas de análisis de vulnerabilidades como las de OWASP ZAP y similares, desempeñan un papel fundamental en la evaluación y el fortalecimiento de estos aspectos críticos de la seguridad al identificar debilidades que podrían comprometer la confidencialidad de los datos, la integridad de los sistemas o la disponibilidad del servicio (Dowd, McDonald , & Schuh , 2006).

Las pruebas de penetración, el hacking ético, la seguridad en entornos de nube y el marco legal y regulatorio aplicable, son elementos son fundamentales para comprender el panorama completo de la seguridad de la información y abordar de manera efectiva los desafíos y riesgos que enfrentan las organizaciones, haciendo énfasis también en el sector financiero. Por ejemplo, las empresas que operan en la nube deben implementar medidas de seguridad adicionales y las herramientas de escaneo de vulnerabilidades pueden ayudar a identificar y mitigar los riesgos específicos de los entornos de nube (Armbrust, y otros, 2010).

Por lo tanto y de acuerdo con lo anterior, podemos concluir que según (Hicken, 2023) “El análisis de vulnerabilidades con las herramientas y recursos de OWASP ha demostrado ser efectivo para que empresas de diversos sectores mejoren la seguridad de sus aplicaciones web y mitiguen los riesgos de ciberataques y filtraciones de datos”.

1.1 Seguridad de Aplicaciones Web

La seguridad de las aplicaciones web se refiere a las medidas y controles implementados para proteger las aplicaciones y los sitios web de amenazas y ataques maliciosos. Este es un aspecto crítico debido a la naturaleza abierta de las aplicaciones web y la creciente sofisticación de los ciberataques.

Las aplicaciones web enfrentan una amplia gama de amenazas. Es por esto por lo que el Open Web Application Security Project (OWASP) ha identificado las diez vulnerabilidades más críticas y comunes en las aplicaciones web, conocidas como OWASP Top 10 (The OWASP Foundation, s.f.).

Para mitigar estos riesgos, es importante adoptar prácticas de desarrollo seguras y un ciclo de vida de desarrollo de software seguro (S-SDLC). Esto incluye integrar controles de seguridad en las primeras etapas de desarrollo, realizar pruebas de seguridad continuas y aplicar actualizaciones y parches de seguridad de manera oportuna (Whitman & Mattord, 2017).

1.2 Análisis de Vulnerabilidades

La evaluación de vulnerabilidades es un proceso sistemático y proactivo para identificar y evaluar vulnerabilidades y vulnerabilidades en sistemas, aplicaciones o redes informáticas. Existen diferentes tipos de pruebas de penetración, como las pruebas de caja negra (sin conocimiento interno), las pruebas de caja blanca (con acceso al código fuente) y las pruebas de caja gris (conocimiento parcial).

Existen varias metodologías y estándares reconocidos para el análisis de vulnerabilidad, como las pautas de OWASP, el proceso de pruebas de penetración (PTES) del Instituto Nacional de Estándares y Tecnología (NIST) y las mejores prácticas de la industria (Instituto Nacional de Estándares y Tecnología (NIST)., s/f).

1.3 OWASP ZAP

OWASP Zed Attack Proxy (ZAP) es una herramienta de código abierto desarrollada por una organización a nivel mundial sin fines de lucro llamada OWASP (Open Worldwide Application Security Project. OWASP se dedica a mejorar la seguridad del software, y ZAP es uno de los productos destacados de su amplio conjunto de herramientas (The OWASP Foundation, s.f.).

ZAP está diseñado específicamente para probar aplicaciones web. Tiene capacidades de escaneo activo y pasivo, detección de vulnerabilidades, fuzzing y pruebas de seguridad avanzadas, facilitando la identificación de agujeros de seguridad en las aplicaciones web. Además, proporciona informes detallados y recomendaciones para mitigar los riesgos detectados.

OWASP ZAP está meticulosamente diseñada para detectar vulnerabilidades en conformidad con el famoso OWASP Top 10, una lista comprensiva de las principales vulnerabilidades de seguridad en aplicaciones web identificadas por la comunidad de seguridad. Al alinearse con este estándar reconocido a nivel mundial, ZAP se convierte en una herramienta confiable para identificar y mitigar las amenazas más críticas que enfrentan las aplicaciones web modernas (The OWASP Foundation, s.f.).

1.4 Normativas y Estándares

ISO/IEC 27002:2022 es un código de mejores prácticas ampliamente aceptado para la gestión de la seguridad de la información. Establece principios y controles para asegurar la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27002:2022(E), 2022).

El cumplimiento de estas reglas y estándares es esencial para que las organizaciones fortalezcan su seguridad, protejan sus activos de información y cumplan con los requisitos legales y reglamentarios aplicables.

1.5 Gestión del Riesgo

La gestión de riesgos de seguridad de la información es el proceso sistemático de identificar, analizar, evaluar y abordar los riesgos a los que están expuestos los activos de información de una organización, esto permite a las organizaciones tomar medidas para reducir la probabilidad y el impacto de posibles incidentes de seguridad (ISO/IEC 27005:2018(E)., 2022). Existen estándares reconocidos como ISO 27005, NIST SP 800-30 y CRAMM que proporcionan metodologías y pautas para implementar un proceso eficaz de gestión de riesgos de seguridad.

2. Diseño Metodológico

En este capítulo, se presenta el diseño metodológico elaborado para la ejecución del proyecto, el cual está estructurado en varias fases, desde la planificación inicial hasta la entrega de recomendaciones técnicas generales.

2.1 Configuración y Preparación:

En esta fase, se configura y se prepara el entorno de OWASP ZAP para el escaneo. Esto incluye configurar el proxy del navegador para interceptar y analizar el tráfico web, establecer las opciones de escaneo y configurar cualquier autenticación necesaria para acceder al sitio.

Se procede a descargar e instalar la herramienta OWASP ZAP en uno de los servidores de la compañía, específicamente en aquel que aloja los sitios web. Esto se realiza para agilizar el proceso. Una vez completada la instalación, es necesario ajustar algunos parámetros para personalizar el informe que la herramienta genera.

Pasos para realizar una ejecución de un escaneo automatizado.

- Iniciar OWASP ZAP y hacer clic en la pestaña “Inicio rápido”.
- Clic en el botón de Escaneo automatizado.
- Se ingresa la URL completa de la aplicación web que se desea analizar y se da clic en “Atacar” para iniciar el escaneo.

Una vez se ejecuten los pasos anteriores empezará el análisis del sitio web seleccionado. Esto puede hacerse utilizando el modo de "Spider" (araña), que sigue los enlaces dentro del sitio web para descubrir nuevas páginas y funcionalidades.

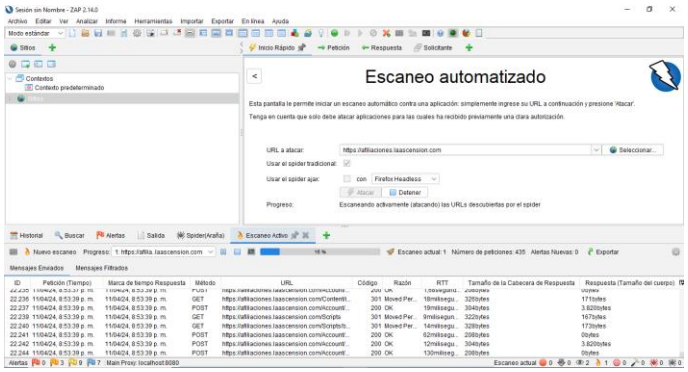


Ilustración 1. Imagen de la herramienta OWASP ZAP escaneo automatizado.

2.2. Escaneo de vulnerabilidades:

Una vez que el sitio web ha sido explorado, OWASP ZAP puede llevar a cabo un exhaustivo escaneo de vulnerabilidades en todas las páginas y funcionalidades descubiertas. Esto nos permite obtener un informe detallado de todas las posibles vulnerabilidades presentes en el sitio, así como la gravedad de cada brecha de seguridad y las soluciones recomendadas para su corrección, reducción o mitigación del impacto.

2.3. Entrega de Reporte**:**

Basándonos en los resultados detallados del análisis, proporcionaremos a la organización un informe exhaustivo que documente los hallazgos descubiertos, junto con recomendaciones generales y pertinentes para abordar y reducir las brechas de seguridad identificadas. Este informe no solo destacará las vulnerabilidades encontradas, sino que también ofrecerá soluciones concretas y estratégicas para fortalecer la postura de seguridad de la organización y mitigar los riesgos potenciales.

Para lograr el objetivo de detectar, enumerar y abordar la mayor cantidad posible de vulnerabilidades de seguridad, es esencial aplicar de manera efectiva la metodología OWASP. Esta acción asegurará la protección de las aplicaciones y la información confidencial de los usuarios.

Es fundamental reconocer que la seguridad es un proceso continuo; por lo tanto, las aplicaciones deben someterse a evaluaciones regulares para detectar y corregir nuevas vulnerabilidades antes de que puedan ser aprovechadas por posibles atacantes. La correcta implementación de la priorización de vulnerabilidades también resulta crucial, dado que permite clasificarlas según su gravedad, nivel de explotación y otros criterios relevantes para la seguridad. Esto posibilita tomar decisiones informadas acerca de qué vulnerabilidades abordar primero y qué medidas de seguridad adoptar para proteger de manera efectiva el sistema o la aplicación.

3. Resultados logrados

Se realizó el escaneo de vulnerabilidades a los portales web de clientes y empleados de la organización con la herramienta OWASP ZAP, herramienta de seguridad para probar y evaluar la seguridad de aplicaciones web. Esta herramienta nos generó un reporte detallado del escaneo de las vulnerabilidades presentadas por estos dos portales web.

Reporte de vulnerabilidad y seguridad Portal Empleados.

La siguiente tabla representa un resumen de las vulnerabilidades del portal empleados de la organización, reportadas por la herramienta OWASP ZAP. La primera tabla representa las vulnerabilidades detectadas junto con la descripción y nivel de riesgo.

Tabla 1. Resumen de vulnerabilidades web de portal empleados por categoría herramienta OWASP ZAP.

Vulnerabilidad detectada	Descripción	Nivel de riesgo
Ausencia de fichas (tokens) Anti- Falsificación de Petición en Sitios Cruzados	Solicitud falsa entre sitios que engaña a la víctima para realizar acciones no deseadas en un sitio web sin su conocimiento. Explota la confianza de la aplicación en el usuario y se diferencia de los ataques XSS, aunque pueden tener similitudes. También se conoce como ataque con un solo clic, montaje de sesión y otros términos.	Medio
CSP: Directiva de Comodín en la Política de Seguridad de Contenido	Capa adicional de seguridad que detecta y previene ataques, como XSS e inyección de datos, utilizados para robo de datos y distribución de malware. CSP utiliza encabezados HTTP para declarar fuentes de contenido permitidas, como JavaScript, CSS, imágenes, etc., protegiendo los sitios web contra amenazas.	Medio
Cabecera de la Política de Seguridad de Contenido (CSP) no configurada	Capa de seguridad que previene ataques como XSS e inyección de datos, utilizados para robar datos o distribuir malware. CSP usa encabezados HTTP para permitir a los propietarios de sitios web especificar fuentes de contenido permitidas, como JavaScript, CSS, imágenes, etc., protegiendo así sus sitios contra amenazas.	Medio
Falta de cabecera Anti-Clickjacking	La respuesta carece de medidas de seguridad como la Política de Seguridad de Contenido y X-Frame-Options para prevenir ataques de 'ClickJacking'.	Medio
Librería JS Vulnerable	Una librería JavaScript vulnerable puede causar, inyección de código malicioso, pérdida de datos, exposición de información sensible y riesgo de ataques de día cero en una aplicación web.	Medio
Revelación de Errores de la Aplicación	La página muestra un mensaje de error que puede exponer datos confidenciales, como la ubicación del archivo que causó un error no controlado, lo que podría facilitar futuros ataques a la aplicación web. Sin embargo, es posible que sea un falso positivo si el mensaje de error se encuentra en una página de documentación.	Bajo

Cookie Without Secure Flag	Se ha creado una cookie sin la marca de seguridad, lo que permite el acceso a la cookie a través de conexiones no cifradas, lo que puede ser un riesgo para la seguridad.	Bajo
Cookie sin el atributo SameSite	Se ha configurado una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud "entre sitios". El atributo SameSite es una contramedida eficaz contra la falsificación de solicitudes entre sitios, la inclusión de secuencias de comandos entre sitios y los ataques de sincronización.	Bajo
Inclusión de Archivos Fuente de JavaScript de Diferentes Dominio	La página incluye uno o más archivos de script de un dominio de terceros.	Bajo
Divulgación de la marca de hora - Unix	Una marca de tiempo ha sido divulgada por el servidor de la aplicación/el navegador - Unix	Bajo
El servidor revela información a través del encabezado de respuesta HTTP "X-Powered-By".	El servidor web/aplicaciones filtra información de la versión a través del encabezado de respuesta HTTP "Servidor". Esto podría facilitar a los atacantes la identificación de posibles vulnerabilidades en el servidor web/aplicaciones.	Bajo
El Servidor Filtra Información de la Versión a través del Campo de Cabecera HTTP 'Server'	HTTP Strict Transport Security (HSTS) es una política de seguridad web que obliga a los navegadores y otros agentes de usuario a utilizar conexiones HTTPS seguras al interactuar con un servidor web. Esto se hace superponiendo HTTP a TLS/SSL. HSTS es un protocolo estandarizado por el IETF y se especifica en RFC 6797.	Bajo
Cabecera de Seguridad de Transporte Estricto no Configurada	Falta configurar el encabezado Anti-MIME-Sniffing X-Content-Type-Options en 'nosniff'. Esto evita que navegadores más antiguos, como Internet Explorer y Chrome, realicen un rastreo MIME en la respuesta, lo que podría mostrar el contenido de una manera diferente a la declarada. Las versiones más recientes de Firefox usan el tipo de contenido declarado en lugar de realizar el rastreo MIME	Bajo
X-Content-Type-Options Header Missing	El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que podría provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto al declarado.	Bajo
Divulgación de información - Comentarios sospechosos	La respuesta contiene comentarios sospechosos que podrían ser útiles para un atacante. Esto incluye no solo los comentarios, sino todo el contenido de los scripts o archivos.	Informativo
Modern Web Application	La aplicación parece ser moderna, y para explorarla automáticamente, el Ajax Spider puede ser más efectivo que el enfoque estándar.	Informativo
Re-examine Cache-control Directives	El control de caché no está bien configurado o falta, lo que puede permitir que el contenido se almacene en caché en el navegador y servidores proxy. Mientras que esto puede ser deseado para recursos estáticos como CSS, JS e imágenes, se debe realizar una revisión para asegurarse de que no se almacene en caché ningún contenido sensible o confidencial.	Informativo
Session Management Response Identified	Se encontró un token de gestión de sesión en la respuesta. El campo 'Otra información' contiene un conjunto de tokens de encabezado utilizados para la administración de sesiones basada en encabezados. Si el contexto de la solicitud utiliza la "Detección automática" de	Informativo

	administración de sesiones, esta regla adaptará la administración de sesiones para utilizar los tokens identificados.	
User Controllable HTML Element Attribute (Potential XSS)	Verificación de la entrada del usuario para detectar posibles vulnerabilidades de XSS en parámetros de la cadena de consulta y datos POST. Se requiere revisión adicional para evaluar la explotabilidad.	Informativo

Fuente: Resultados Escaneo OWASP ZAP

Nivel de riesgo	Número de Alertas
Alto	0
Medio	5
Bajo	9

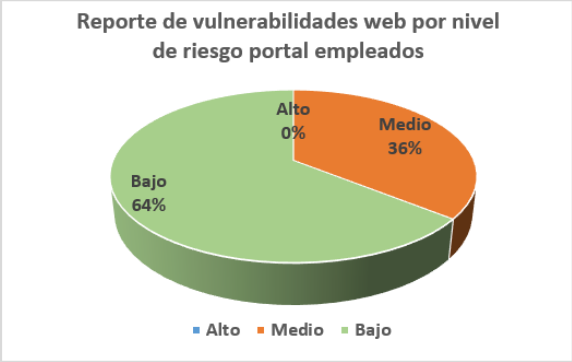


Ilustración 2. Gráfica de reporte de vulnerabilidades web por nivel de riesgo para el portal empleados.

De acuerdo con el resultado de escaneo de vulnerabilidades web con la herramienta OWASP ZAP mostrado en la tabla No.1, se determinó que el portal web empleados de la organización tiene una vulnerabilidad baja de un 64%, el daño que causan los ataques a este nivel no producen impacto significativo al portal web, sin embargo, un 36% del portal tiene vulnerabilidad media con vulnerabilidades como Ausencia de fichas (tokens) Anti- Falsificación de Petición en Sitios Cruzados , Cabecera de la Política de Seguridad de Contenido (CSP) no configurada, Falta de cabecera Anti-Clickjacking y otras mencionadas en la tabla No.1 que pueden llevar a la explotación de la seguridad del sitio, pérdida de datos, y compromiso de la integridad y la privacidad de usuarios.

También se evidencia que el portal web no tiene ninguna amenaza de nivel alto, lo que significa que no se han identificado vulnerabilidades críticas o amenazas significativas que representen un riesgo inminente para la seguridad de la aplicación web.

Notas del autor:

La anterior información presentada se expone a modo informativo para mostrar los resultados generales sin entrar en detalle o especificaciones para proteger la confidencialidad de la organización.

Reporte de vulnerabilidad y seguridad Portal Clientes.

La siguiente tabla representa el resumen de las vulnerabilidades de portal de clientes de la organización reportadas por la herramienta OWASP ZAP, esta tabla muestra la vulnerabilidad detectada, junto con la descripción, el nivel de riesgo y el número de instancias de vulnerabilidades encontradas en el portal web.

Tabla 2. Resumen de vulnerabilidades web de portal clientes por categoría herramienta OWASP ZAP.

Vulnerabilidad detectada	Descripción	Nivel de riesgo
Cabecera de la Política de Seguridad de Contenido (CSP) no configurada	CSP es una capa de seguridad que previene ataques como XSS e inyección de datos al permitir a los propietarios de sitios web declarar fuentes de contenido permitidas, como JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados, evitando la carga de contenido no deseado.	Medio
Configuración X-Frame-Options mal formada	Una cabecera X-Frame-Option está presente en la repuesta pero su valor configurado no es correcto.	Medio
Cookie sin bandera segura	Se ha configurado una cookie sin el indicador seguro, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.	Bajo
Cookie sin el atributo SameSite	La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra ataques de 'ClickJacking'.	Bajo
Inclusión de archivos fuente JavaScript entre dominios	La página incluye uno o más archivos de script de un dominio de terceros.	Bajo
Divulgación de la marca de hora - Unix	Una marca de tiempo ha sido divulgada por el servidor de la aplicación/el navegador - Unix	Bajo
El servidor expone su versión a través del encabezado de respuesta HTTP "Servidor".	El servidor revela información de versión en su encabezado "Servidor" de las respuestas HTTP, lo que podría ayudar a los atacantes a encontrar vulnerabilidades en el servidor web.	Bajo
Encabezado de seguridad de transporte estricto no establecido	HTTP Strict Transport Security (HSTS) es una política de seguridad web que obliga a los navegadores a utilizar conexiones seguras HTTPS con el servidor web, proporcionando una capa adicional de seguridad. Está definido en el estándar RFC 6797 del IETF.	Bajo
Divulgación de información - Comentarios sospechosos	La respuesta contiene comentarios sospechosos que podrían ser útiles para un atacante, incluyendo scripts y archivos en la evaluación.	Informativo
Reexaminar las directivas de control de caché	Falta o configuración incorrecta del encabezado de control de caché, lo que permite el almacenamiento en caché por parte de navegadores y servidores proxy. Puede ser intencional para activos estáticos como CSS, JS o imágenes, pero se debe revisar para evitar el almacenamiento en caché de contenido confidencial.	Informativo

Respuesta de gestión de sesión identificada	Se encontró un token de gestión de sesión en la respuesta. La "Otra información" incluye tokens de encabezado utilizados para la administración de sesiones basada en encabezados. En contextos con administración de sesión automática, esta regla ajusta el uso de los tokens detectados.	Informativo
Agente de usuario Fuzzer	Compara diferencias en respuestas al cambiar el User Agent (por ejemplo, a versiones móviles o como motor de búsqueda). Analiza el código de estado y el hash del cuerpo de respuesta respecto a la respuesta original.	Informativo
Atributo de elemento HTML controlable por el usuario (Posible XSS)	Esta verificación analiza la entrada del usuario en los parámetros de la cadena de consulta y los datos POST en busca de posibles vulnerabilidades de XSS (cross-site scripting), lo que requiere revisión adicional para evaluar su explotabilidad.	Informativo

Fuente: Resultados Escaneo OWASP ZAP

Nivel de riesgo	Número de Alertas
Alto	0
Medio	2
Bajo	6

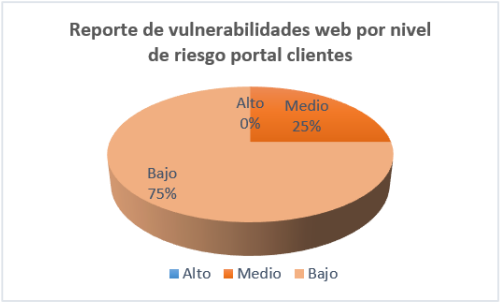


Ilustración 3. Gráfica de reporte de vulnerabilidades web por nivel de riesgo para el portal empleados.

De acuerdo con el resultado del escaneo de vulnerabilidades web del portal clientes de la organización con la herramienta OWASP ZAP, mostrado en la tabla No.2, se determinó que el portal web de clientes tiene una vulnerabilidad baja del 75%. Los ataques a este nivel no producen un impacto significativo en el portal web. Sin embargo, un 25% del portal tiene vulnerabilidades medias con alertas como "Cabecera Content Security Policy (CSP) no configurada" y "Configuración X-Frame-Options mal formada", mencionadas en la tabla No.2 que pueden exponer al portal web y a los usuarios a amenazas de seguridad significativas que pueden llevar a la explotación de la seguridad del sitio, pérdida de datos y compromiso de la integridad y la privacidad de los usuarios.

Notas del autor:

La anterior información presentada se expone a modo informativo para mostrar los resultados generales sin entrar en detalle o especificaciones para proteger la confidencialidad de la organización.

4. Conclusiones y recomendaciones

4.1 Conclusiones

El proyecto de análisis de vulnerabilidades en los portales web de la organización del sector de servicios funerarios ha proporcionado una visión del estado de seguridad de los portales tanto para empleados como para clientes.

A través del uso de la herramienta OWASP ZAP, reconocida mundialmente por su eficacia y confiabilidad para detectar y mitigar las amenazas más críticas que enfrentan las aplicaciones web modernas, se logró la identificación de varias vulnerabilidades con diferentes niveles de riesgo. Este hallazgo destaca la importancia de abordar y mitigar estos riesgos para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información.

Para el portal de empleados, se encontró que el 64% de las vulnerabilidades son de nivel bajo, mientras que el 36% restante son de nivel medio y para el portal de clientes muestra un panorama similar, con el 75% de las vulnerabilidades clasificadas como de nivel bajo y el 25% como de nivel medio. Aunque las vulnerabilidades de nivel bajo tienen un impacto limitado, las de nivel medio presentan riesgos significativos que pueden comprometer la seguridad del portal y la privacidad de los usuarios. Es crucial abordar estas vulnerabilidades para garantizar un entorno seguro y confiable para los empleados.

En resumen, el análisis de vulnerabilidades ha identificado áreas críticas de mejora en los portales web de la organización. Es fundamental que la compañía tome medidas para abordar y corregir estas vulnerabilidades, siguiendo las recomendaciones y mejores prácticas proporcionadas en el informe. Esto garantizará que los portales sean seguros, confiables y capaces de proteger la información sensible de la organización y de sus usuarios.

4.2 Recomendaciones

Implementar mecanismos para reforzar la seguridad de los portales web, como lo son:

- Tokens anti-falsificación de petición (CSRF).
- Políticas de seguridad de contenido (CSP) para mitigar los riesgos de XSS y la inyección de datos maliciosos.
- Configurar adecuadamente las cabeceras de seguridad para prevenir ataques de Clickjacking y proteger la integridad del sitio web.
- Mantener actualizadas las bibliotecas y dependencias en el código del sitio web.
- Revisar y corregir los mensajes de error.
- Configurar correctamente las cookies.

Así mismo, se debe realizar un seguimiento continuo de las vulnerabilidades identificadas, se recomienda establecer un proceso de mejora continua de la seguridad de los portales web. Esto incluye realizar escaneos periódicos de vulnerabilidades, actualizar regularmente las políticas de seguridad y mantener al equipo de seguridad informado sobre las últimas amenazas y mejores prácticas de seguridad.

Al implementar estas recomendaciones, la organización podrá mejorar significativamente la seguridad de sus portales web y proteger la confidencialidad, integridad y disponibilidad de la información de la empresa y sus usuarios.

5. Bibliografía

(16 de Diciembre de 2022). Obtenido de Ministerio de Tecnologías de la Información y las Comunicaciones: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., & ... & Zaharia, M. (2010). *A view of cloud computing. .* Communications of the ACM, 53(4), 50-58.

Dowd, M., McDonald , J., & Schuh , J. (2006). *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities.* Addison Wesley Professional.

Hicken, A. (Octubre de 2023). *Cómo aprender OWASP e impulsar la seguridad de sus aplicaciones*. Obtenido de https://es.parasoft.com/blog/getting-started-with-owasp/

Instituto Nacional de Estándares y Tecnología (NIST). (s/f). *Penetration Testing Execution Standard (PTES).* Obtenido de https://www.nist.gov/itl/applied-cybersecurity/nice/penetration-testing-execution-standard

ISO/IEC 27002:2022(E). (2022). *Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información.* ISO.

ISO/IEC 27005:2018(E). (2022). *Tecnología de la información - Técnicas de seguridad - Gestión de riesgos en seguridad de la información.* ISO.

NormasISO.org. (2023). Obtenido de ISO 27000: clave para seguridad de la información: https://normasiso.org/norma-iso-27000/

Stuttard, D. &. (2007). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* Wiley.

The OWASP Foundation. (s.f.). *OWASP Zed Attack Proxy (ZAP) Official Documentation.* Obtenido de https://www.zaproxy.org/docs/

Whitman, M., & Mattord, H. (2017). *Principles of information security (6th ed.).* CENGAGE Learning Custom Publishing.