PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ESCUELA DE INFORMATICA E INTELIGENCIA ARTIFICIAL

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN TECNOLOGIAS DE LA INFORMACIÓN

“ANÁLISIS DE VULNERABILIDADES A LOS SISTEMAS INFORMATICOS DE LA EMPRESA INGENIO AZUCARERO DEL NORTE DE COMPAÑÍA DE ECONOMÍA MIXTA “IANCEM” BASADO EN LA METODOLOGÍA OWASP”

DIEGO FERNANDO GUERRA OLMEDO

TUTOR: MGS. DAVID NARVAEZ

IBARRA – ECUADOR

FEBRERO – 2025

Ibarra, 12 de Febrero del 2025

CERTIFICACÍON TUTOR

En mi calidad de Tutor del Trabajo de titulación titulado:

“Análisis de Vulnerabilidades a los Sistemas Informáticos de la Empresa Ingenio Azucarero del Norte de Compañía de Economía Mixta “IANCEM” basado en la Metodología OWASP, presentado por el estudiante Diego Fernando Guerra Olmedo con cédula de ciudadanía N° 1004172746, para obtener el Título de Ingeniero en Tecnologías de la Información.

Certifico que el trabajo cumple con todos los parámetros establecidos, mediante el cual el estudiante demuestra el desarrollo de competencias en el campo de conocimiento de su profesión con un nivel de argumentación coherente, para ser sometido a la evaluación por parte de los lectores.

Adicionalmente, se adjunta el certificado de porcentaje de originalidad de TURNITIN.


3/2/25, 7:30 Turnitin - Informe de Originalidad - Tesis Guerra Diego

Turnitin Informe de Originalidad

Procesado el: 27-ene.-2025 07:39 -05
Identificador: 2572680657
Número de palabras: 16406
Entregado: 1

Tesis Guerra Diego Por DIEGO FERNANDO GUERRA OLMEDO

Índice de similitud
4%

Similitud según fuente
Internet Sources: 3%
Publicaciones: 0%
Trabajos del estudiante: 2%

(f):__
Mgs. David Narváez
TUTOR DE TRABAJO
C.C.: 1002868378

PAGINA DE APROBACIÓN DEL TRIBUNAL

El tribunal examinador, aprueba el presente trabajo en nombre de la Pontificia Universidad Católica del Ecuador Ibarra:

(f):

Mgs. David Narváez

C.C.: 1002868378

Diego Fernando Baroja Llanos

Firmado digitalmente por Diego Fernando Baroja Llanos
DN: cn=Diego Fernando Baroja Llanos gn=Diego Fernando Baroja Llanos c=EC Ecuador l=E.C Ecuador o=Docente ou=Docente e=diegofer369i@gmail.com
Motivo:Soy el autor de este documento
Ubicación:
Fecha:2025-02-14 15:46-05:00

(f):……

Msc. Diego Baroja

C.C.: 1002402061

(f):……

Ms. Darwin Pillo

C.C.: 1003319660

ACTA DE CESIÓN DE DERECHOS

Yo, *Diego Fernando Guerra Olmedo*, declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: "Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones a título gratuito y oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia".

Ibarra, _____

(f):_____

Diego Fernando Guerra Olmedo

C.C.: 1004172746

AUTORIA

Yo, Diego Fernando Guerra Olmedo, portador de la cedula de ciudadanía N° 1004172746, declaro que el presente trabajo de investigación es de total responsabilidad del autor@, y eximo expresamente a la Pontificia Universidad Católica del Ecuador Ibarra de posibles reclamos o acciones legales.

(f): 

Diego Fernando Guerra Olmedo

C.C.: 1004172746.

DECLARACIÓN Y AUTORIZACIÓN

Yo Diego Fernando Guerra Olmedo, con CC: 1004172746, autor del trabajo de grado intitulado: "ANÁLISIS DE VULNERABILIDADES A LOS SISTEMAS INFORMÁTICOS DE LA EMPRESA INGENIO AZUCARERO DEL NORTE DE COMPAÑÍA DE ECONOMÍA MIXTA "IANCEM" BASADO EN LA METODOLOGÍA OWASP", previo a la obtención del título profesional de ("INGENIERO EN TECNOLOGIAS DE LA INFORMACION", en la Escuela de Informática e Inteligencia Artificial.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador Sede- Ibarra, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador Sede Ibarra a difundir a través de sitio web de la Biblioteca de la PUCESI el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ibarra, (día, mes y año)

(f.)…….
Diego Fernando Guerra Olmedo

C.C.: 1004172746

DEDICATORIA Y AGRADECIMIENTOS

Quiero agradecer primeramente a Dios por ayudarme a cumplir una meta mas en mi vida, por siempre darme la fuerza para seguir, nunca dejarme solo y por siempre estar a mi lado las veces que lo necesite.

A mis padres Edwin Rene Guerra Pinto y Sylvia Margarita Olmedo Paz por darme su apoyo incondicional, también por ser un pilar fundamental en mi vida, por siempre haberme inculcado el camino del bien y por darme un ejemplo de perseverancia y dedicación que es lo que me inspira a superar cada obstáculo que se presenta en mi vida y la fuerza que me dan para superar cada una de mis metas.

También quiero agradecer a mi familia y amigos quienes han estado a mi lado en cada paso de mi carrera, los cuales me han brindado su aliento, su apoyo y su comprensión en los momentos mas desafiantes de este viaje

Finalmente quiero agradecer a una persona más, que no estuvo en el inicio de mi carrera, pero si está en el final, ella es mi novia María Paula. Quiero agradecerle por estar conmigo, por apoyarme, por impulsarme a cada día ser mejor persona y un mejor hombre, también por darme su amor y cariño y por siempre estar a mi lado y no alejarse de mí, quiero celebrar este y mas logros a su lado, quiero decirle que la amo y que ella ha sido el mejor regalo que me ha dado la vida.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el panorama empresarial actual, caracterizado por una creciente dependencia de la tecnología, las empresas del sector productivo se enfrentan a desafíos sin precedentes en materia de ciberseguridad. IANCEM, una empresa líder en la comercialización de azúcar en el norte de Ecuador, no es una excepción a esta realidad. A pesar de haber modernizado recientemente sus instalaciones para optimizar la producción y cumplir con rigurosas normas ambientales, IANCEM se encuentra en una posición vulnerable en lo que respecta a la seguridad de sus sistemas informáticos.

La presente investigación surge de la necesidad crítica de evaluar y fortalecer la postura de seguridad de IANCEM en el entorno digital. Aunque la empresa ha implementado medidas de seguridad en sus sistemas informáticos, estas no han sido sometidas a una validación exhaustiva para determinar su efectividad frente a la creciente sofisticación de los ciberataques. Esta brecha en la validación representa un riesgo significativo para la integridad de los datos, la continuidad operativa y, en última instancia, la reputación de la empresa en un mercado cada vez más competitivo y consciente de la seguridad.

El objetivo principal de este estudio es realizar un análisis comprehensivo y meticuloso de los sistemas informáticos de IANCEM, utilizando como marco de referencia la metodología OWASP (Open Web Application Security Project). Esta elección metodológica no es arbitraria; OWASP se ha establecido como un estándar de facto en la industria de la seguridad informática, ofreciendo un enfoque estructurado y actualizado para la identificación, evaluación y mitigación de riesgos de seguridad en los sistemas.

El análisis se centrará en la detección y evaluación de una amplia gama de vulnerabilidades potenciales, con especial énfasis en aquellas que han demostrado ser particularmente críticas en entornos empresariales similares. Entre estas, se prestará especial atención a:

Inyecciones SQL: Una vulnerabilidad clásica pero aún prevalente que puede permitir a los atacantes manipular o extraer datos sensibles de las bases de datos.

Fallos en la gestión de sesiones: Deficiencias que podrían permitir a atacantes suplantar la identidad de usuarios legítimos, comprometiendo la confidencialidad y la integridad de las operaciones.

Configuraciones inadecuadas de seguridad: Errores en la configuración de servidores, aplicaciones o frameworks que pueden dejar puertas abiertas a intrusiones.

Cross-Site Scripting (XSS): Vulnerabilidades que permiten la inyección de scripts maliciosos en cada uno de los sistemas que son visualizadas por otros usuarios.

Exposición de datos sensibles: Fallos en la protección de información crítica durante su almacenamiento o transmisión.

Falta de control de acceso robusto: Debilidades en los mecanismos de autenticación y autorización que podrían permitir accesos no autorizados.

La metodología OWASP no solo guiará la identificación de estas vulnerabilidades, sino que también proporcionará un marco para su priorización basada en el impacto potencial y la probabilidad de explotación. Este enfoque permitirá a IANCEM abordar primero las amenazas más críticas, optimizando así la asignación de recursos en sus esfuerzos de mitigación.

Además de la identificación de vulnerabilidades, esta investigación se propone ofrecer un informe técnico y otro administrativo donde se pueda sustentar el proceso de testeo de los sistemas y las vulnerabilidades encontradas en estos, además estos informes contendrán las recomendaciones concretas y accionables para la mitigación de los riesgos detectados. Estas recomendaciones se basarán en las mejores prácticas de la industria y se adaptarán específicamente al contexto operativo de IANCEM, considerando factores como su infraestructura tecnológica existente, recursos disponibles y requisitos regulatorios específicos del sector azucarero en Ecuador.

Esta investigación no solo busca abordar las vulnerabilidades inmediatas en los sistemas informáticos de IANCEM, sino que también aspira a establecer un precedente para la mejora continua de la seguridad cibernética en la empresa. Al adoptar un enfoque

proactivo y basado en estándares internacionales como OWASP, IANCEM no solo protegerá sus activos digitales críticos, sino que también reafirmará su compromiso con la innovación, la excelencia operativa y la responsabilidad corporativa en la era digital.

Este esfuerzo posicionará a IANCEM como un líder no solo en la producción y comercialización de azúcar, sino también en la adopción de prácticas de seguridad cibernética avanzadas en el sector agroindustrial ecuatoriano. El impacto de esta investigación, por lo tanto, se extenderá más allá de los límites de la empresa, contribuyendo potencialmente a elevar los estándares de seguridad en toda la industria.

PALABRAS CLAVE

Ciberseguridad, Sistemas Informáticos, OWASP, OWASP ZAP, Validación de seguridad, vulnerabilidades, Inyección SQL, Gestión de sesiones, Cross-Site Scripting (XSS), Datos sensibles, Control de acceso, Mitigación, Informes técnicos, Agroindustrial.

ABSTRACT

In today's business landscape, characterized by an increasing dependence on technology, companies in the productive sector face unprecedented cybersecurity challenges. IANCEM, a leading sugar trading company in northern Ecuador, is no exception to this reality. Despite having recently modernized its facilities to optimize production and comply with rigorous environmental standards, IANCEM is in a vulnerable position when it comes to the security of its web systems.

This investigation arises from the critical need to assess and strengthen IANCEM's security posture in the digital environment. Although the company has implemented security measures on its web systems, these have not been subjected to thorough validation to determine their effectiveness against the increasing sophistication of cyberattacks. This gap in validation represents a significant risk to data integrity, operational continuity, and ultimately the company's reputation in an increasingly competitive and security-conscious market.

The main objective of this study is to perform a comprehensive and meticulous analysis of IANCEM web systems, using the OWASP (Open Web Application Security Project) methodology as a reference framework. This methodological choice is not arbitrary; OWASP has established itself as a de facto standard in the IT security industry, offering a structured and up-to-date approach to the identification, assessment and mitigation of security risks in web applications.

The analysis will focus on the detection and assessment of a wide range of potential vulnerabilities, with special emphasis on those that have proven to be particularly critical in similar business environments. Among these, special attention will be paid to:

SQL injections: A classic but still prevalent vulnerability that can allow attackers to manipulate or extract sensitive data from databases.

Session management flaws: Deficiencies that could allow attackers to impersonate legitimate users, compromising the confidentiality and integrity of operations.

Inadequate security configurations: Errors in the configuration of servers, applications or frameworks that can leave doors open to intrusions.

Cross-Site Scripting (XSS): Vulnerabilities that allow the injection of malicious scripts into web pages viewed by other users.
Exposure of sensitive data: Failures in the protection of critical information during storage or transmission.
Lack of robust access control: Weaknesses in authentication and authorization mechanisms that could allow unauthorized access.

The OWASP methodology will not only guide the identification of these vulnerabilities, but will also provide a framework for their prioritization based on potential impact and likelihood of exploitation. This approach will allow IANCEM to address the most critical threats first, thus optimizing the allocation of resources in its mitigation efforts.

In addition to the identification of vulnerabilities, this research aims to offer concrete and actionable recommendations for mitigating the risks detected. These recommendations will be based on industry best practices and tailored specifically to IANCEM's operational context, considering factors such as its existing technological infrastructure, available resources, and regulatory requirements specific to the sugar sector in Ecuador.

This research not only seeks to address immediate vulnerabilities in IANCEM's web systems, but also aims to set a precedent for continuous improvement of cybersecurity in the company. By adopting a proactive approach based on international standards such as OWASP, IANCEM will not only protect its critical digital assets, but will also reaffirm its commitment to innovation, operational excellence, and corporate responsibility in the digital age.
This effort will position IANCEM as a leader not only in the production and marketing of sugar, but also in the adoption of advanced cybersecurity practices in the Ecuadorian agro-industrial sector. The impact of this research will therefore extend beyond the boundaries of the company, potentially contributing to raising security standards across the industry.

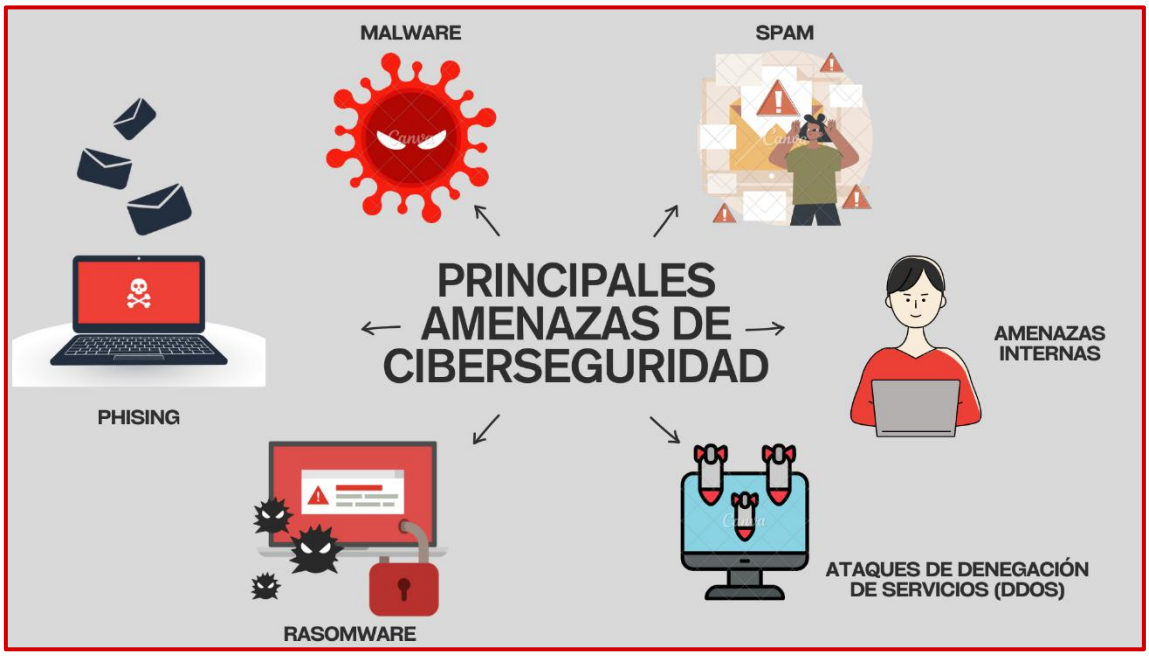
KEY WORDS

Cybersecurity, Computer Systems, OWASP, OWASP ZAP, Security validation, vulnerabilities, SQL injection, Session management, Cross-Site Scripting (XSS), Sensitive data, Access control, Mitigation, Technical reports, Agroindustrial.

INTRODUCCION

En la era digital actual, la ciberseguridad se ha convertido en un pilar fundamental para la supervivencia y el éxito de las empresas en todos los sectores. La creciente dependencia de los sistemas informáticos y las plataformas web para las operaciones diarias ha ampliado significativamente la superficie de ataque, exponiendo a las organizaciones a una variedad de amenazas cibernéticas cada vez más sofisticadas.

Figura 1
Principales Amenazas de la Ciberseguridad



Fuente: Santos, J. (2024, 21 octubre). principales amenazas de ciberseguridad para empresas y cómo prevenirlas. Deltaprotect. https://www.deltaprotect.com/blog/amenazas-de-ciberseguridad

La agroindustria comprende las actividades económicas relacionadas con la producción y comercialización agrícola, siendo fundamental para la economía de muchos países, especialmente en América Latina. Este sector no solo incluye la producción en fincas, sino también empresas que fabrican maquinaria agrícola, suministran insumos, y producen agroquímicos. Además, emplea a gran parte de la población en países como Brasil, Argentina y México. La agroindustria es clave para la seguridad alimentaria, el desarrollo económico y la sostenibilidad, aunque enfrenta desafíos como la emisión de

gases de efecto invernadero, lo que impulsa la innovación en prácticas agrícolas. (TOTVS LATAM, 2024)

Según (INCIBE, 2024) “La digitalización del sector agroalimentario aumenta su vulnerabilidad a ciberataques debido a la exposición de dispositivos conectados y una baja preparación en ciberseguridad, lo que lo convierte en un objetivo atractivo y crítico para ciberdelincuentes.”

Las empresas como el Ingenio Azucarero del Norte de Compañía de Economía Mixta "IANCEM", líder en la comercialización de azúcar en el norte de Ecuador, se encuentran en una encrucijada donde la modernización tecnológica y la seguridad cibernética deben converger para garantizar la integridad de sus operaciones y la protección de sus activos digitales.

IANCEM, en su búsqueda de optimización y eficiencia, ha implementado diversos sistemas web para gestionar sus procesos productivos y administrativos. Sin embargo, la rápida adopción de estas tecnologías no siempre va acompañada de una evaluación exhaustiva de los riesgos de seguridad asociados. Esta brecha entre la implementación tecnológica y la validación de seguridad representa un punto vulnerable que podría ser explotado por actores malintencionados.

En este contexto, la metodología OWASP (Open Web Application Security Project) se presenta como una herramienta invaluable para evaluar y fortalecer la postura de seguridad de las aplicaciones web. OWASP proporciona un marco de referencia ampliamente reconocido en la industria de la seguridad informática, ofreciendo un enfoque estructurado para la identificación, evaluación y mitigación de riesgos de seguridad en aplicaciones web.

El presente proyecto se enfoca en la aplicación rigurosa de la metodología OWASP para evaluar la seguridad de los sistemas web de IANCEM. Este análisis no solo busca identificar vulnerabilidades existentes, sino también categorizar y priorizar estos riesgos en función de su gravedad y potencial impacto en las operaciones de la empresa. Para llevar a cabo esta evaluación, se utilizará la herramienta OWASP ZAP, aplicando técnicas

de hacking ético para simular posibles vectores de ataque y descubrir debilidades en la infraestructura web de IANCEM.

La relevancia de este estudio trasciende el ámbito inmediato de IANCEM, ya que los hallazgos y recomendaciones resultantes pueden servir como un modelo para otras empresas del sector agroindustrial que enfrentan desafíos similares en la protección de sus activos digitales. Al abordar proactivamente las vulnerabilidades de seguridad, IANCEM no solo fortalecerá su propia postura de ciberseguridad, sino que también establecerá un precedente de buenas prácticas en un sector cada vez más dependiente de la tecnología.

Este proyecto culminará con el desarrollo de una propuesta integral que resumirá los resultados de la evaluación de vulnerabilidades y proporcionará recomendaciones concretas para mejorar la seguridad de los sistemas web de IANCEM. Estas recomendaciones se basarán en las mejores prácticas de la industria y se adaptarán específicamente al contexto operativo de IANCEM, considerando factores como su infraestructura tecnológica existente, recursos disponibles y requisitos regulatorios específicos del sector azucarero en Ecuador.

En última instancia, este esfuerzo busca no solo proteger los activos digitales críticos de IANCEM, sino también impulsar una cultura de seguridad cibernética proactiva dentro de la organización. Al adoptar un enfoque sistemático y basado en estándares internacionales para la evaluación y mejora de la seguridad web, IANCEM se posicionará como un líder en la adopción de prácticas de seguridad cibernética avanzadas en el sector agroindustrial ecuatoriano, contribuyendo así a elevar los estándares de seguridad en toda la industria.

OBJETIVO GENERAL

Evaluar la seguridad de los sistemas informáticos de la empresa "IANCEM" utilizando la metodología OWASP para identificar y abordar posibles vulnerabilidades y contribuir a fortalecer la seguridad cibernética de la organización.

OBJETIVOS ESPECÍFICOS

- Aplicar la metodología OWASP para categorizar y priorizar las vulnerabilidades identificadas en función de su gravedad y riesgo.

- Analizar detalladamente las vulnerabilidades en los sistemas web de la empresa utilizando la herramienta de OWASP ZAP aplicando técnicas de hacking ético.

- Presentar una propuesta integral que resuma los resultados de la evaluación de vulnerabilidades y las recomendaciones para mejorar la seguridad de los sistemas web de la empresa.

VARIABLE DEPENDIENTE

En esta investigación, la variable dependiente se define como las vulnerabilidades identificadas y evaluadas en los sistemas web de IANCEM. Estas vulnerabilidades representan el resultado del análisis de seguridad realizado con base en la metodología OWASP y el uso de herramientas como OWASP ZAP.

La variable dependiente se mide a través de factores clave como la cantidad de vulnerabilidades detectadas, su clasificación según la severidad (crítica, alta, media o baja) y su impacto potencial en la confidencialidad, integridad y disponibilidad de la información sensible de la empresa.

Este enfoque permite evaluar el estado actual de la seguridad en los sistemas web de IANCEM, proporcionando una base para priorizar las acciones correctivas y garantizar la protección de los activos digitales de la organización frente a amenazas potenciales.

ALCANCE DEL PROYECTO

El alcance de esta investigación se centra en el análisis de las vulnerabilidades presentes en los sistemas informáticos de la empresa IANCEM, que gestiona información crítica relacionada con los diferentes procesos en la producción de azúcar.

Para los sistemas informáticos de IANCEM incluye la identificación ***de*** vulnerabilidades mediante herramientas como OWASP ZAP, enfocándose en detectar amenazas como inyecciones de código, configuraciones inadecuadas de acceso y exposición de datos sensibles. Posteriormente, se realizará una evaluación de riesgos, clasificando cada vulnerabilidad según su severidad y probabilidad de explotación, considerando tanto el impacto técnico como comercial en la empresa. Con base en estos hallazgos, se desarrollarán recomendaciones prácticas alineadas con las mejores prácticas de seguridad informática para mitigar o eliminar los riesgos detectados.

Este análisis no contempla la implementación directa de las soluciones propuestas ni la corrección de las vulnerabilidades identificadas. En su lugar, se prioriza la elaboración de un informe detallado que incluya:

Límites del análisis:

- El análisis se enfoca exclusivamente en los sistemas informáticos en uso en la empresa IANCEM.
- No se incluyen pruebas en dispositivos personales, redes externas a la empresa o entornos fuera del alcance directo de sus operaciones.

- Las soluciones recomendadas no serán implementadas como parte del presente trabajo; dichas acciones dependerán de la decisión y capacidad técnica de la empresa.

Con este alcance, se busca proporcionar a la empresa una visión integral del estado de seguridad de sus sistemas, permitiendo priorizar recursos y esfuerzos para la protección de la información crítica y el fortalecimiento de sus defensas contra amenazas cibernéticas.

CAPITULO 1

ESTADO DEL ARTE

En este capítulo, se presenta el estado del arte y los conceptos básicos acerca del análisis de vulnerabilidades el cual tiene como objetivo explorar el panorama en el cual se va a trabajar sin antes primero hablar de la empresa y el entorno en el que se va a desarrollar el proyecto de tesis.

Según (*Ingenio Azucarero del Norte Compañía de Economía Mixta Iancem Perfil de Compañía - Ecuador | Finanzas y Ejecutivos Clave | EMIS*, s. f.):

> El Ingenio Azucarero del Norte Compañía de Economía Mixta Iancem, ubicado en Ibarra, es la primera industria azucarera en Imbabura, instalada en 1908. Los orígenes del Ingenio se remontan a 1964, cuando las Cajas de Previsión Social deciden instalarlo y contratan a las compañías FIVES LILLE CAIL y Granda Centeno. En 1966, una vez terminada la obra, se vende el Ingenio a la compañía TAINA, pero en 1977 se le embarga debido a que no pudo cumplir con los compromisos adquiridos con el IESS. En 1985, se forma la Empresa de Economía Mixta Ingenio Azucarero del Norte, con el aporte del IESS, cañicultores de Imbabura y Carchi, accionistas privados y trabajadores de la compañía. El Ingenio es la empresa agroindustrial más importante de Imbabura y Carchi, con proveedores y programas de cultivo de 4600 hectáreas de caña de azúcar.

En el contexto de una creciente digitalización del sector agroindustrial, empresas como IANCEM se enfrentan a nuevos y complejos desafíos en materia de seguridad informática. La transformación digital que experimenta este sector ha traído consigo no solo mejoras en eficiencia y productividad, sino también un aumento significativo en los riesgos cibernéticos.

La naturaleza de las operaciones en empresas como IANCEM, que involucran tanto procesos industriales como gestión de datos sensibles de proveedores y clientes, las convierte en objetivos potenciales para ciberdelincuentes. La combinación de sistemas de control industrial, redes corporativas y plataformas de comercio electrónico crea un ecosistema digital complejo que requiere una protección integral.

Según (INCIBE, 2024)

> Las amenazas más comunes en este sector incluyen ataques de rasomware dirigidos a empleados, explotación de sistemas de control industrial mal configurados, vulnerabilidades en aplicaciones web obsoletas y ataques de ransomware. Cada una de estas amenazas puede tener consecuencias graves, desde la interrupción de operaciones hasta la pérdida de datos críticos o daños a la reputación de la empresa.

La creciente sofisticación de los ciberataques, junto con la expansión de la superficie de ataque debido a la adopción de nuevas tecnologías, subraya la importancia crítica de implementar estrategias de seguridad informática robustas y adaptativas en empresas como IANCEM. Estas estrategias no solo deben enfocarse en proteger la integridad de las operaciones, sino también en salvaguardar la confianza de los grupos interesados y cumplir con las cada vez más exigentes regulaciones en materia de protección de datos y seguridad cibernética.

En este contexto, las vulnerabilidades, especialmente en los sistemas web, se convierte en una práctica esencial. Permite a las empresas identificar proactivamente puntos débiles en su infraestructura digital antes de que puedan ser explotados por actores malintencionados. Para una empresa como IANCEM, líder en su sector y con una larga trayectoria, mantener una postura de seguridad sólida no es solo una medida preventiva, sino también una declaración de compromiso con la excelencia operativa y la responsabilidad corporativa en la era digital.

Este enfoque en la seguridad informática no solo protege los activos digitales de la empresa, sino que también contribuye a su competitividad y sostenibilidad a largo plazo en un mercado cada vez más consciente de los riesgos cibernéticos.

Para lo cual el proyecto se realizó bajo la metodología OWASP, según (Arsys, 2024) “OWASP es una comunidad global de voluntarios y expertos en seguridad informática. Su misión es mejorar la seguridad de las aplicaciones web mediante la concienciación, la educación y la promoción de las mejores prácticas de seguridad.”

OWASP ha desarrollado diversas guías, herramientas y metodologías para ayudar a organizaciones a mejorar la seguridad de sus sistemas, siendo la más conocida el OWASP Top 10, que proporciona un listado de las vulnerabilidades más críticas que afectan a las aplicaciones web.

1 ANTECENDETES

En los últimos años, la seguridad cibernética ha cobrado una importancia creciente dentro del ámbito empresarial, debido a la sofisticación y frecuencia de los ataques informáticos.

La investigación realizada por Jefferson Yacelga (2024) sobre vulnerabilidades en servidores empresariales de Cubosoft, utilizando las metodologías OWASP y PTES, es un claro ejemplo de cómo las auditorías de seguridad pueden revelar fallos críticos en la infraestructura tecnológica. A través de un proceso exhaustivo de pentesting, se detectaron vulnerabilidades desde configuraciones incorrectas hasta posibles inyecciones de código malicioso. Estos hallazgos subrayan la relevancia de adoptar una cultura organizacional de seguridad y una gestión proactiva de riesgos para mitigar amenazas. Además, la investigación no solo se limita a identificar las debilidades, sino que ofrece recomendaciones prácticas y validadas para reforzar la seguridad de los sistemas, lo que evidencia la necesidad de enfoques estructurados para enfrentar los desafíos cibernéticos actuales. Esta investigación aporta un análisis profundo sobre cómo las metodologías estandarizadas como OWASP y PTES pueden guiar la detección y mitigación de riesgos en un entorno digital cada vez más complejo.

La investigación realizada por Ruíz Cortés, Ricardo Alfonso, Ruíz Cortés y Jhon Carlos en 2024 sobre el sistema de inventarios Phoenix de una IPS de primer nivel utiliza la metodología OWASP y el estándar ISO 27001:2022 para evaluar su seguridad. Este estudio se enfoca en identificar vulnerabilidades críticas en un sistema basado en PHP y MySQL, detectando desde errores de configuración hasta fallos de protección de datos que podrían facilitar el acceso no autorizado. Mediante pruebas de pentesting en tres etapas: análisis del sistema, pruebas de seguridad, y propuestas de mitigación, se encontró que el sistema presentaba varias vulnerabilidades explotables. Este análisis resalta la importancia de aplicar políticas y procedimientos de seguridad, además de conceptos de PHVA y prácticas de ITIL, como medidas preventivas y correctivas.

1.1 MARCO TEÓRICO

1.1.1 ¿Qué es la seguridad informática?

Para definir el concepto de seguridad informática Aguilar (2024) señala que "La seguridad informática comprende un conjunto de herramientas, prácticas y procesos enfocados en garantizar la seguridad de la información confidencial. Por ejemplo, bases de datos personales, equipos tecnológicos, redes y programas de una empresa ante posibles ataques de ciberdelincuentes".

Según (Eliseo, 2024)

> Existen 4 pilares clave sobre los que se apoya la seguridad informática:
>
> - **Disponibilidad**. Los sistemas deben permitir el acceso a la información cuando el usuario lo requiera, sin perder de vista la privacidad.
> - **Confidencialidad**. La información solo debe ser accesible para las personas autorizadas.
> - **Integridad**. Los sistemas deben garantizar la integridad de la información, sin errores ni modificaciones.
> - **Autenticación**. La información que procede de un usuario debe verificarse para garantizar que es quien dice ser.

1.1.2 ¿Que es la ciberseguridad?

Lindemulder y Kosinski (2024) afirma que "La ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas."

1.1.3 ¿Que es la metodología OWASP?

La metodología OWASP (Open Web Application Security Project) se ha consolidado como un estándar en el ámbito de la seguridad informática, orientada a la identificación y mitigación de riesgos en aplicaciones y sistemas. Desde su fundación en 2001, OWASP ha trabajado activamente para detectar vulnerabilidades comunes y proporcionar

herramientas y guías que ayuden a los desarrolladores a mejorar la seguridad de sus aplicaciones.

Según (Team, 2024)

> OWASP comenzó como un proyecto de código abierto con el objetivo de alertar sobre las vulnerabilidades en las aplicaciones web. Con el tiempo, su enfoque se amplió para abarcar otras áreas tecnológicas, como las APIs, dispositivos móviles e IoT. La metodología OWASP proporciona guías y estándares que priorizan la ciberseguridad en las etapas de desarrollo de software, ofreciendo herramientas de acceso libre para probar vulnerabilidades. Aunque la ciberseguridad a menudo se ve comprometida por los tiempos ajustados de desarrollo, OWASP sigue siendo un recurso clave para las auditorías y mejoras en la seguridad de aplicaciones.

La metodología OWASP es integral porque no solo identifica riesgos, sino que también sugiere soluciones prácticas para prevenir y corregir vulnerabilidades antes de que puedan ser explotadas. Este enfoque ayuda a las empresas a implementar ciberseguridad proactiva, reduciendo tanto el riesgo como el impacto potencial de los ataques.

Entre los pilares de OWASP están sus guías de pruebas, las cuales abarcan desde pruebas de seguridad en aplicaciones web hasta móviles. Estas guías detallan cómo evaluar diferentes aspectos de la seguridad, como la autenticación, la gestión de sesiones y la autorización. Además, OWASP fomenta la colaboración global, atrayendo a profesionales de la ciberseguridad para que contribuyan con su experiencia, lo que asegura que las herramientas y recomendaciones estén alineadas con las mejores prácticas internacionales.

Un aspecto central de la metodología OWASP es el "Top 10 de OWASP", que prioriza las amenazas de seguridad más comunes y críticas, permitiendo a los desarrolladores enfocarse en las vulnerabilidades más importantes. Esta lista se actualiza periódicamente para reflejar las tendencias emergentes en ciberseguridad y asegurar que las organizaciones estén preparadas ante nuevas amenazas.

1.1.4 OWASP Top 10

El (OWASP, 2024) es uno de los pilares de la metodología, y sirve como una lista de control de las amenazas más importantes que las organizaciones deben abordar.

En la Tabla 1 se puede visualizar las vulnerabilidades más comunes y críticas según el OWASP Top 10:

Tabla 1

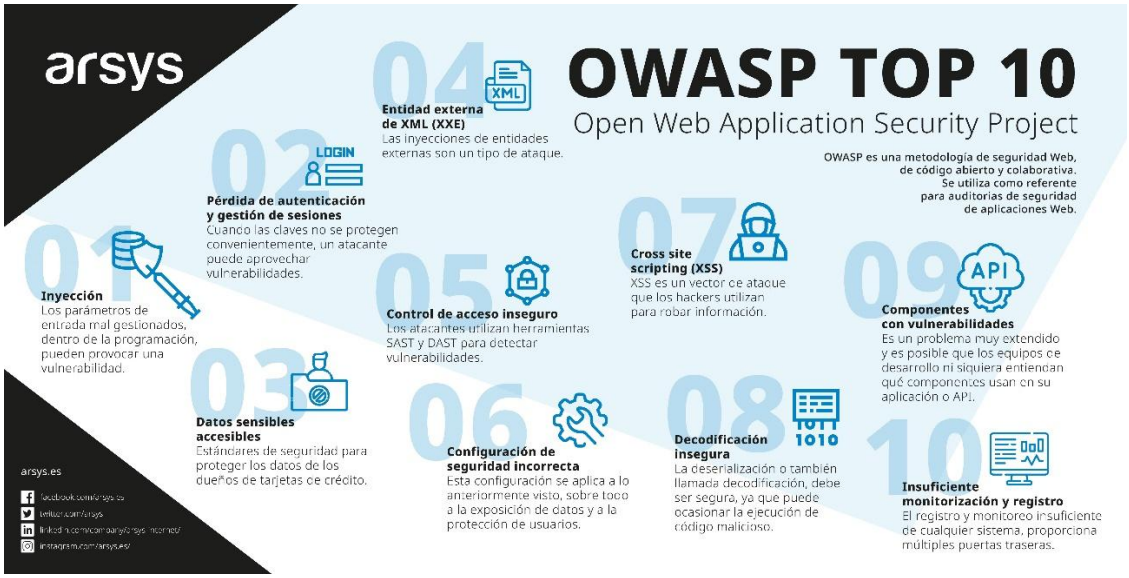
Matriz General de las Amenazas Mas Importantes Sobre la Metodología OWASP

Vulnerabilidad	Descripción	Impacto	Mitigación
Inyección (Injection)	Datos maliciosos enviados a un intérprete (SQL, NoSQL, OS) se ejecutan involuntariamente.	Acceso no autorizado a datos, modificación o eliminación de información, ejecución de comandos en el sistema.	Validar y sanitizar entradas, usar consultas preparadas, emplear ORM (Object Relational Mapping) y evitar concatenación directa en comandos SQL o similares.
Pérdida de control sobre autenticación (Broken Authentication)	Autenticación y gestión de sesiones deficientes permiten a atacantes comprometer cuentas de usuario.	Secuestro de cuentas, acceso no autorizado, robo de identidad.	Usar autenticación multifactor, contraseñas robustas, limitar duración de sesiones, rotar tokens de sesión y evitar exposición de tokens en URL.
Exposición de datos sensibles (Sensitive Data Exposure)	Información sensible (financiera, salud, PII) no está adecuadamente protegida.	Robo de identidad, fraude, pérdida de confidencialidad de datos críticos.	Implementar cifrado fuerte (AES, TLS) para datos en tránsito y almacenamiento, evitar almacenamiento innecesario y eliminar datos que ya no son necesarios.
Control de acceso roto (Broken Access Control)	Los atacantes eluden restricciones de acceso, actuando como usuarios legítimos o administradores.	Acceso y modificación no autorizada de datos, abuso de privilegios administrativos.	Configurar estrictamente controles de acceso, deshabilitar funciones innecesarias, aplicar reglas de validación y realizar auditorías de configuración.
Configuración incorrecta de seguridad (Security Misconfiguration)	Configuraciones por omisión o sin actualizar permiten vulnerabilidades.	Acceso no autorizado, exposición de datos sensibles, posibilidad de ataques de DoS.	Mantener configuración segura, aplicar parches y actualizaciones, eliminar funciones no utilizadas y asegurar configuraciones predeterminadas.
Componentes vulnerables y desactualizados (Vulnerable and Outdated Components)	Uso de bibliotecas o frameworks con vulnerabilidades conocidas.	Pérdida de datos, accesos no autorizados, posibles violaciones de seguridad y daño a la reputación.	Realizar escaneos de vulnerabilidades, actualizar componentes y frameworks regularmente, mantener

Vulnerabilidad	Descripción	Impacto	Mitigación
			un inventario actualizado de componentes y aplicar parches de seguridad.
Cross-Site Scripting (XSS)	Datos maliciosos inyectados permiten la ejecución de scripts en el navegador de otro usuario.	Robo de credenciales, manipulación de datos, redirección a sitios fraudulentos, pérdida de confianza en la aplicación.	Validar y sanitizar entradas de usuario, emplear encoding para HTML, CSS y JavaScript, evitar el uso de otros métodos peligrosos en el lado del cliente.
Deserialización insegura (Insecure Deserialization)	Datos deserializados sin validación permiten ejecutar código malicioso en la aplicación.	Acceso no autorizado, ejecución remota de código, alteración de comportamiento de la aplicación.	Validar datos deserializados, limitar los tipos de datos permitidos en la deserialización, usar formatos de serialización seguros y restringir el acceso a fuentes no confiables.
Uso insuficiente de registro y monitoreo (Insufficient Logging and Monitoring)	Falta de medidas de monitoreo impide detectar y responder a incidentes de seguridad a tiempo.	Acciones maliciosas no detectadas, demora en respuesta a incidentes, dificultad en investigación de incidentes.	Implementar registros de seguridad adecuados, establecer alertas de eventos críticos, monitorear actividades inusuales y realizar auditorías periódicas de los registros.
Uso de funciones criptográficas inseguras (Insecure Cryptographic Storage)	Uso de algoritmos de cifrado débiles o inexistentes para proteger datos sensibles.	Acceso no autorizado a datos confidenciales, robo de datos financieros y personales, posibilidad de ingeniería inversa.	Usar algoritmos de cifrado seguros (AES con claves de 256 bits), aplicar salting en contraseñas, evitar el almacenamiento de información sensible sin cifrado y emplear bibliotecas de cifrado actualizadas y confiables.

Nota: Elaboración propia adaptada de OWASP. (2024, septiembre). Los diez mejores de OWASP. https://owasp.org/www-project-top-ten/

Figura 2
Principales Amenazas en Base a OWASP TOP 10



Nota: Grafico extraído directamente de García, F. (2024, 16 octubre). OWASP: ¿Qué es y cómo usar esta metodología? Arsys. https://www.arsys.es/blog/owasp

1.1.5 Frameworks para llevar a cabo un pentesting o análisis de vulnerabilidades

En la Tabla 2 se presenta la comparativa de diferentes frameworks que se pueden usar para llevar a cabo un análisis de vulnerabilidades comparando sus pros y contras acerca del tema desarrollado:

Tabla 2
Matriz de Frameworks Utilizados en Análisis de Vulnerabilidades Basados en sus Pros y Contras.

Framework	Pros	Contras
Nmap	- Amplia funcionalidad para el escaneo de red. - Permite identificar servicios, puertos, sistemas operativos y equipos activos. - Adaptable mediante parámetros como -sV (versión del servicio) o -O (detectar OS).	- Requiere conocimientos avanzados para aprovechar todas sus funciones. - Salida basada en línea de comandos, lo cual puede ser menos amigable para principiantes. - Interfaces gráficas limitadas y menos recomendadas.

Framework	Pros	Contras
	- Disponible en múltiples sistemas operativos (Linux, Windows, Mac).	
Nessus	- Posee una extensa base de datos de vulnerabilidades conocidas en servicios. - Ofrece una interfaz gráfica intuitiva, ideal para principiantes. - Plugins específicos para identificar vulnerabilidades según los servicios activos. - Modo gratuito adecuado para uso hogareño.	- La versión profesional es de pago. - Escanear sin limitación de parámetros puede ser lento en entornos grandes. - Requiere configuración específica para analizar solo servicios relevantes.
Metasploit	- Potente base de datos de exploits para aprovechar vulnerabilidades encontradas. - Consola de línea de comandos msfconsole que permite automatizar tareas. - Buen enfoque para simular ataques reales y verificar el alcance de las vulnerabilidades. - Interfaz gráfica disponible para facilitar el aprendizaje.	- Curva de aprendizaje más pronunciada en comparación con otros frameworks. - Puede ser potencialmente destructiva si no se usa correctamente. - No se recomienda para principiantes sin conocimientos sólidos en ciberseguridad.
Damn Vulnerable Linux (DVL)	- Amplia gama de vulnerabilidades para experimentar en un entorno seguro. - Ideal para probar técnicas de hacking y fortalecer habilidades de seguridad.	- No está actualizado ni mantenido oficialmente. - Puede no reflejar vulnerabilidades modernas o sistemas actuales.
Kali Linux (antes Backtrack)	- Incluye herramientas avanzadas como Nmap, Nessus, Metasploit, y más. - Cubre múltiples categorías de análisis, desde recolección de datos hasta ataques de fuerza bruta y forense.	- Puede ser abrumadora para principiantes debido a la cantidad de herramientas. - Algunas herramientas requieren conocimientos avanzados para su uso efectivo.

Framework	Pros	Contras
	- Fácil de instalar como ISO o en entornos virtualizados (VMWare).	

Nota: Elaboración propia adaptada de Bortnik, S. (2024). Pruebas de penetración para principiantes: 5 herramientas para empezar. .Seguridad. https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

1.1.6 Contenido de la estructura en base a la documentación del análisis de vulnerabilidad

Como señala Jackson (2024)

> La documentación de un análisis de vulnerabilidades sigue una estructura clave para asegurar claridad y utilidad en la gestión de riesgos.

1.1.6.1 Descubrimiento de activos

Primero, se identifican todos los activos de TI que pueden ser vulnerables, como servidores, dispositivos de red y aplicaciones. Este inventario ayuda a establecer el alcance del análisis y asegura que no se omitan componentes importantes.

1.1.6.2 Identificación de vulnerabilidades

Se realizan pruebas de vulnerabilidad mediante herramientas automáticas y, en ocasiones, revisiones manuales para descubrir fallos en los sistemas. Aquí se detectan configuraciones inseguras, software desactualizado o problemas de codificación.

1.1.6.3 Documentación de vulnerabilidades

Cada vulnerabilidad se registra detalladamente, incluyendo su ubicación, impacto potencial y gravedad. Esto es fundamental para priorizar acciones, y permite crear un plan de remediación estructurado. Además, esta documentación es útil para auditorías y análisis futuros.

1.1.6.4 Recomendaciones y Plan de Remediación

Basándose en la gravedad de las vulnerabilidades, se desarrollan guías de corrección, como aplicar parches, reconfigurar sistemas o mejorar controles de seguridad. Esto se presenta en un formato claro y ordenado, con recomendaciones prácticas y plazos sugeridos para implementar las soluciones.

1.1.7 Implementación basada en la metodología OWASP

1.1.7.1 Identificar el riesgo

El primer paso consiste en reconocer las amenazas y vulnerabilidades específicas de la aplicación en cuestión. Para hacerlo, OWASP recomienda un análisis detallado de la infraestructura, datos, y configuraciones de la aplicación para detectar posibles puntos débiles que puedan ser explotados por atacantes.

1.1.7.2 Estimar la probabilidad

Aquí se analiza la posibilidad de que las amenazas identificadas se materialicen. OWASP sugiere considerar la frecuencia y los patrones históricos de los ataques y el contexto específico del entorno de la aplicación para definir una probabilidad de ocurrencia.

Tabla 3
Tabla de Estimación de Probabilidad de Cada Amenaza Encontrada.

ALTA	MEDIA	BAJA
Vulnerabilidad que si es explotada comprometería la seguridad de la información ocasionando un impacto negativo sobre la empresa. Debe solucionarse inmediatamente.	Vulnerabilidad que si es explotada tendría un impacto leve sobre la operativa del negocio. Puede solucionarse en un tiempo prudente.	Vulnerabilidad que si es explotada no ocasionaría mayores inconvenientes. Su solución no necesariamente será inmediata.

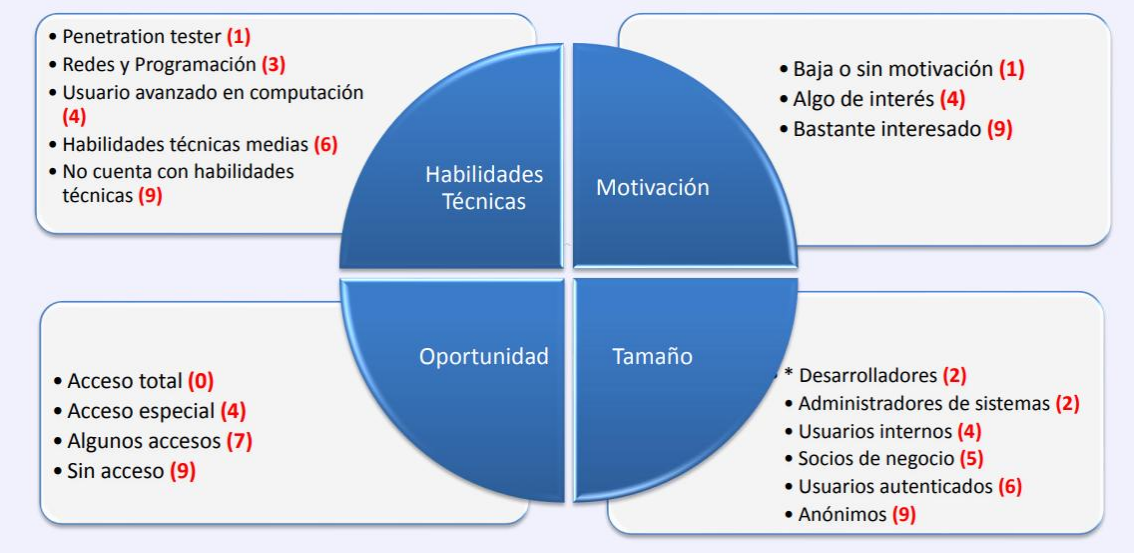
Nota: Elaboración adaptada de Machaca, A. (2024). ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP [Diapositivas].

https://wiki.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

1.1.7.3 Agentes de amenaza

Este punto examina los posibles actores detrás de cada amenaza, incluyendo tanto atacantes internos como externos. Se evalúa su nivel de habilidad, motivación y recursos, para estimar la capacidad del agente de explotar la vulnerabilidad.

Figura 3
Clasificación de los Agentes de Amenaza

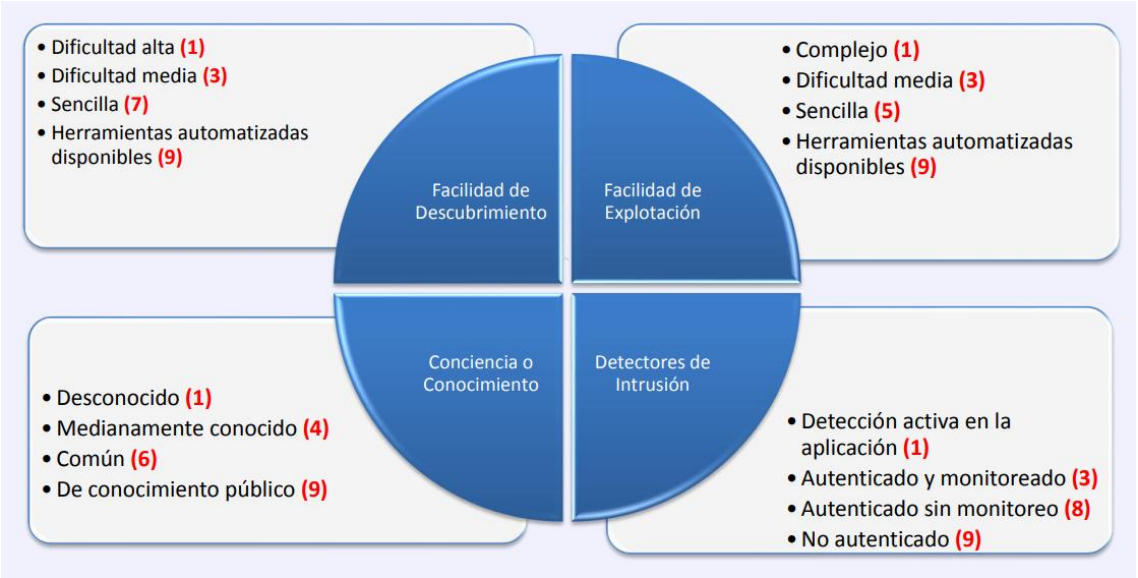


Nota: Grafico extraído directamente de Machaca, A. (2024). ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP [Diapositivas]. https://wiki.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

1.1.7.4 Vulnerabilidades

OWASP recomienda identificar cada vulnerabilidad que pueda estar presente en la aplicación. La evaluación de vulnerabilidades suele incluir auditorías de código, pruebas de penetración y herramientas de escaneo de seguridad para asegurar una detección exhaustiva.

Figura 4
Clasificación de las Vulnerabilidades



Nota: Grafico extraído directamente de Machaca, A. (2024). ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP [Diapositivas]. https://wiki.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

1.1.7.5 Estimar el impacto

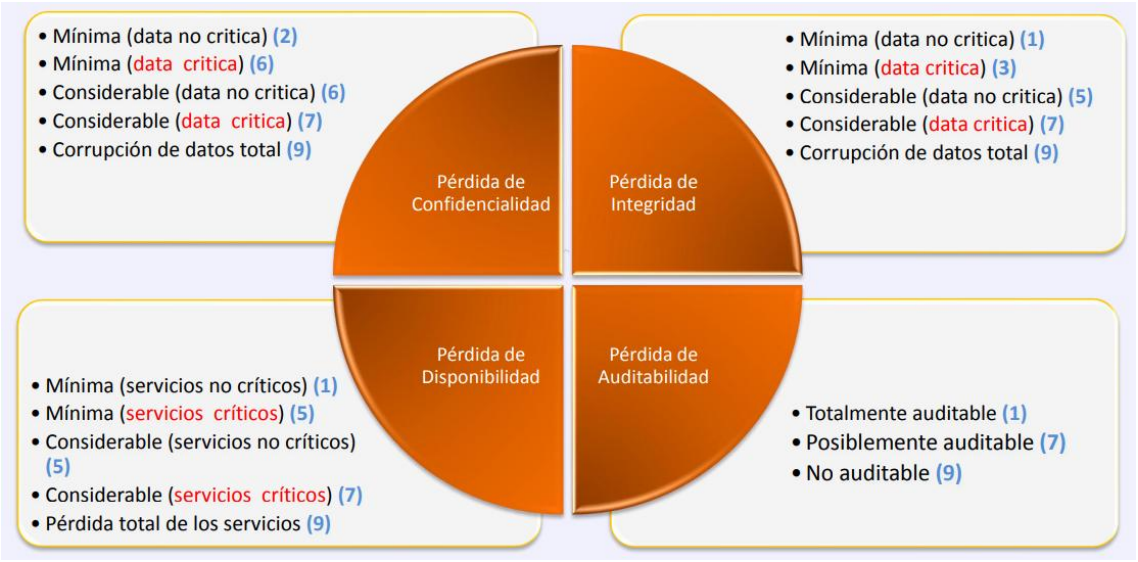
Este paso implica evaluar las posibles consecuencias de un ataque exitoso. OWASP sugiere considerar tanto los impactos técnicos como los de negocio para tener una visión clara de las posibles pérdidas o daños a la organización.

1.1.7.6 Impacto técnico

Evalúa el daño potencial en la infraestructura tecnológica y en los datos, como la pérdida de confidencialidad, integridad o disponibilidad de los sistemas y datos afectados.

Figura 5

Impacto Técnico de una Empresa en Cuestión de Vulnerabilidades



Nota: Grafico extraído directamente de Machaca, A. (2024). ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP [Diapositivas]. https://wiki.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

1.1.7.7 Impacto en el negocio

Aquí se miden las repercusiones en la organización, como pérdidas financieras, daños a la reputación, y problemas de cumplimiento normativo.

Figura 6
Clasificación de la Perdida Financieras en un Negocio

Nota: Grafico extraído directamente de Machaca, A. (2024). ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP [Diapositivas]. https://wiki.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

1.1.7.8 Determinar la severidad del riesgo

Este proceso permite priorizar los riesgos según su gravedad y enfocar recursos en aquellos que representan una amenaza crítica para la seguridad de la aplicación o el negocio.

Para calcular la severidad, OWASP sugiere asignar un nivel de probabilidad e impacto a cada riesgo, que luego se pueden combinar en una matriz de riesgos. La probabilidad se evalúa basándose en factores como la facilidad con que se podría explotar la vulnerabilidad y la frecuencia histórica de ataques similares. El impacto, por otro lado, considera las posibles consecuencias técnicas y de negocio, tales como la exposición de

datos sensibles, la pérdida de disponibilidad del sistema, o daños a la reputación de la organización.

Para determinar la severidad del riesgo, se debe trabajar con los siguientes valores:

1. Probabilidad de la ocurrencia de la amenaza.

2. Impacto generado sobre el negocio.

Tabla 4
Tabla Sobre el Nivel de Probabilidad e Impacto de Acuerdo a la Vulnerabilidad Encontrada.

NIVEL DE PROBABILIDAD E IMPACTO	
0 < 3	**BAJO**
3 < 6	**MEDIO**
6 a 9	**ALTO**

Nota: Elaboración adaptada de Machaca, A. (2024). ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP [Diapositivas]. https://wiki.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

1.1.7.9 Plan de acción

El último paso es la priorización de planes de acción para mitigar los riesgos más graves. OWASP sugiere que cada plan de acción tenga objetivos claros, incluyendo la implementación de medidas correctivas como parches, controles de acceso o ajustes de configuración para fortalecer la seguridad de la aplicación

1.1.8 Que es la herramienta OWASP ZAP

OWASP ZAP (Zed Attack Proxy) es una herramienta de seguridad de aplicaciones web de código abierto desarrollada por OWASP (Open Web Application Security Project), que ofrece a los profesionales de seguridad y a los desarrolladores una plataforma robusta para identificar y solucionar vulnerabilidades en aplicaciones web. OWASP ZAP se destaca por su facilidad de uso y su interfaz amigable, ideal tanto para principiantes como para expertos en ciberseguridad. (Comunnity Latam, 2023)

Esta herramienta actúa como un proxy intermediario entre el usuario y la aplicación web, analizando el tráfico y realizando pruebas de seguridad como escaneos activos y pasivos para detectar vulnerabilidades comunes. Entre las características clave de ZAP están la automatización de pruebas, las exploraciones dinámicas de sitios web, y las herramientas de interceptación y edición de solicitudes HTTP, lo que permite a los usuarios comprender mejor las debilidades en la infraestructura de su aplicación. (Comunnity Latam, 2023)

1.1.9 Funcionamiento de OWASP ZAP

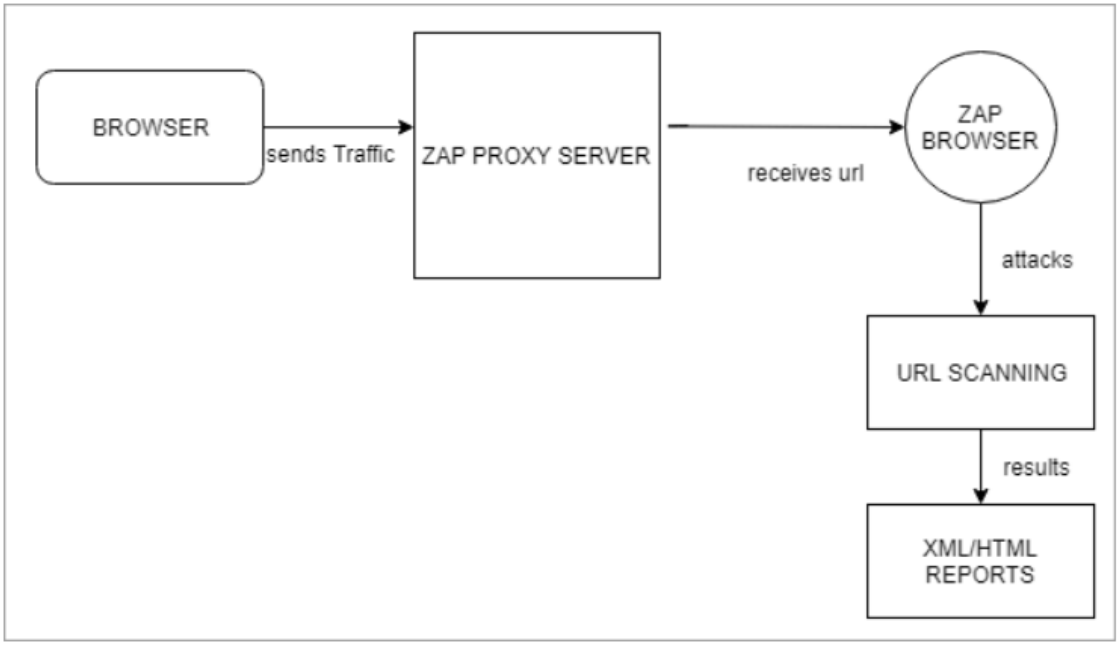
OWASP ZAP opera emulando un intermediario entre el usuario y la web application que se está examinando. Todas las peticiones y respuestas, mientras el usuario opera con la web application citada, se direccionan a través de ZAP. ZAP tiene la función de registrar cada interacción y luego examinarlas para localizar posibles fallos de seguridad. (Beschokov, 2024)

Como señala (Beschokov, 2024)

> ZAP tiene dos modos de operación: pasivo y activo. En el modo pasivo, ZAP se limita a registrar y examinar el tráfico que fluye entre la web application y el usuario sin alterar las peticiones y las respuestas. Este modo resulta útil para detectar fallos de seguridad de forma evidente pero no puede localizar problemas más sutiles que requieren de una interacción más directa.
>
> Por otro lado, en su modo activo, ZAP se implica en el proceso de forma más proactiva modificando las peticiones y respuestas para comprobar si la web application presenta vulnerabilidades. Esta implicación puede implicar inyectar

códigos dañinos en las peticiones o cambiar las respuestas para ver cómo reacciona la aplicación.

Figura 7
Funcionamiento General de la Herramienta OWASP ZAP



Nota: Grafico extraído directamente de Hernández, M. (2024, 12 noviembre). Escaneo de vulnerabilidades automático con OWASP ZAP. https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-autom%C3%A1tico-OWASP-ZAP

1.1.10 Herramientas que se usaran en el análisis de vulnerabilidades

1.1.10.1 Proxy para Interceptación

Descripción: Permite interceptar y analizar las solicitudes y respuestas HTTP entre el navegador y la aplicación web.

Uso: Ideal para entender cómo funciona la aplicación, manipular datos en tránsito, y detectar problemas como inyección de SQL o fallos en la autenticación.

1.1.10.2 Escáner Activo

Descripción: Realiza pruebas automáticas en busca de vulnerabilidades comunes como XSS, inyecciones y exposición de datos sensibles.

Uso: Utilízalo después de explorar la aplicación con el proxy para un análisis más profundo. Es una herramienta clave en un análisis de vulnerabilidades.

1.1.10.3 Escáner Pasivo

Descripción: Analiza automáticamente las solicitudes y respuestas HTTP capturadas por el proxy, sin interactuar directamente con la aplicación.

Uso: Ideal para identificar cabeceras de seguridad ausentes, configuraciones inseguras y problemas de exposición de datos sensibles.

1.1.10.4 Spidering

Descripción: Mapea automáticamente las páginas de la aplicación web explorando enlaces.

Uso: Útil para asegurar que todas las partes de la aplicación han sido analizadas. Complementa el escaneo activo y pasivo.

1.1.10.5 Fuzzing

Descripción: Envía datos malformados o inesperados para probar la robustez de la aplicación frente a entradas inválidas.

Uso: Úsalo para analizar formularios, parámetros y puntos de entrada en busca de vulnerabilidades no detectadas automáticamente.

1.1.10.6 Reporte de Vulnerabilidades

Descripción: Genera informes detallados sobre los hallazgos de seguridad.

Uso: Documenta los riesgos encontrados y las medidas correctivas necesarias para presentarlas al equipo de desarrollo o a la administración.

1.1.11 Herramienta de Nmap

1.1.11.1 ¿Qué es la herramienta Nmap?

La herramienta Nmap es la abreviatura de Network Mapper. Es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas. Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades (Shivanandhan, 2023).

1.1.11.2 ¿Por qué usar Nmap?

Según (Shivanandhan, 2023)

- Capacidad para reconocer rápidamente todos los dispositivos, incluidos servidores, enrutadores, conmutadores, dispositivos móviles, etc. en redes únicas o múltiples.

- Ayuda a identificar los servicios que se ejecutan en un sistema, incluidos los servidores web, los servidores DNS y otras aplicaciones comunes. Nmap también puede detectar versiones de aplicaciones con una precisión razonable para ayudar a detectar vulnerabilidades existentes.

- Nmap puede encontrar información sobre el sistema operativo que se ejecuta en los dispositivos. Puede proporcionar información detallada, como las versiones del sistema operativo, lo que facilita la planificación de enfoques adicionales durante las pruebas de penetración.

- Durante la auditoría de seguridad y el escaneo de vulnerabilidades, puedes usar Nmap para atacar sistemas usando scripts existentes del motor de scripting de Nmap.

- Nmap tiene una interfaz gráfica de usuario llamada Zenmap. Te ayuda a desarrollar mapeos visuales de una red para una mejor usabilidad y generación de informes.

CAPITULO II

MATERIALES Y METODOS

En este capítulo, se describen los procedimientos, técnicas y herramientas utilizadas para analizar las vulnerabilidades en los sistemas web de la empresa IANCEM. La investigación se centra en la seguridad de las aplicaciones web utilizando OWASP ZAP como herramienta principal para identificar y mitigar posibles riesgos. El objetivo principal es garantizar la protección de la información sensible de la empresa, mejorando la resiliencia frente a ataques cibernéticos y reduciendo las vulnerabilidades existentes.

2. Generalidades de la investigación

Esta investigación aborda un aspecto crítico en el ámbito de la ciberseguridad: el análisis de vulnerabilidades de las aplicaciones web utilizadas por la empresa IANCEM, dedicada a la comercialización de azúcar. Mediante el uso de OWASP ZAP, se busca identificar, clasificar y priorizar las vulnerabilidades más críticas, proponiendo estrategias efectivas para fortalecer la seguridad y minimizar el impacto de posibles ataques.

El enfoque adoptado combina el uso de metodologías reconocidas, como OWASP, y el análisis cualitativo. Esto permitió no solo identificar vulnerabilidades técnicas, sino también comprender el contexto y las implicaciones de estas en el negocio. A continuación, se describen las principales estrategias empleadas:

1. **Análisis con OWASP ZAP:** Se utilizó esta herramienta para realizar pruebas automatizadas y manuales de seguridad en las aplicaciones web, enfocándose en vulnerabilidades como inyección SQL, XSS, y control de acceso insuficiente.

2. **Enfoque cualitativo:** Comprendió el análisis detallado de los riesgos y amenazas, considerando aspectos técnicos y su impacto en los procesos de negocio.

2.1 Metodología

El análisis de seguridad se ejecuto basado en la metodología OWASP la cual esta desencadenada e implantada en la herramienta OWASP ZAP, por lo tanto, se proporciona una descripción detallada del proceso metodológico que se utilizo para analizar la seguridad de las plataformas de IANCEM.

Para llevar a cabo el análisis, se implementaron las siguientes tareas específicas:

1. Planificación y Alcance:

- Definir objetivos y límites del análisis
- Identificar sistemas y aplicaciones a evaluar
- Establecer cronograma y recursos

2. Recopilación de Información:

- Identificar tecnologías utilizadas
- Realizar reconocimiento pasivo y activo
- Documentar la arquitectura del sistema

3. Análisis de Vulnerabilidades:

- Realizar escaneos automatizados
- Revisar configuraciones
- Identificar vulnerabilidades conocidas

4. Explotación:

- Confirmar vulnerabilidades encontradas
- Evaluar impacto real
- Documentar vectores de ataque

5. Documentación de Hallazgos:

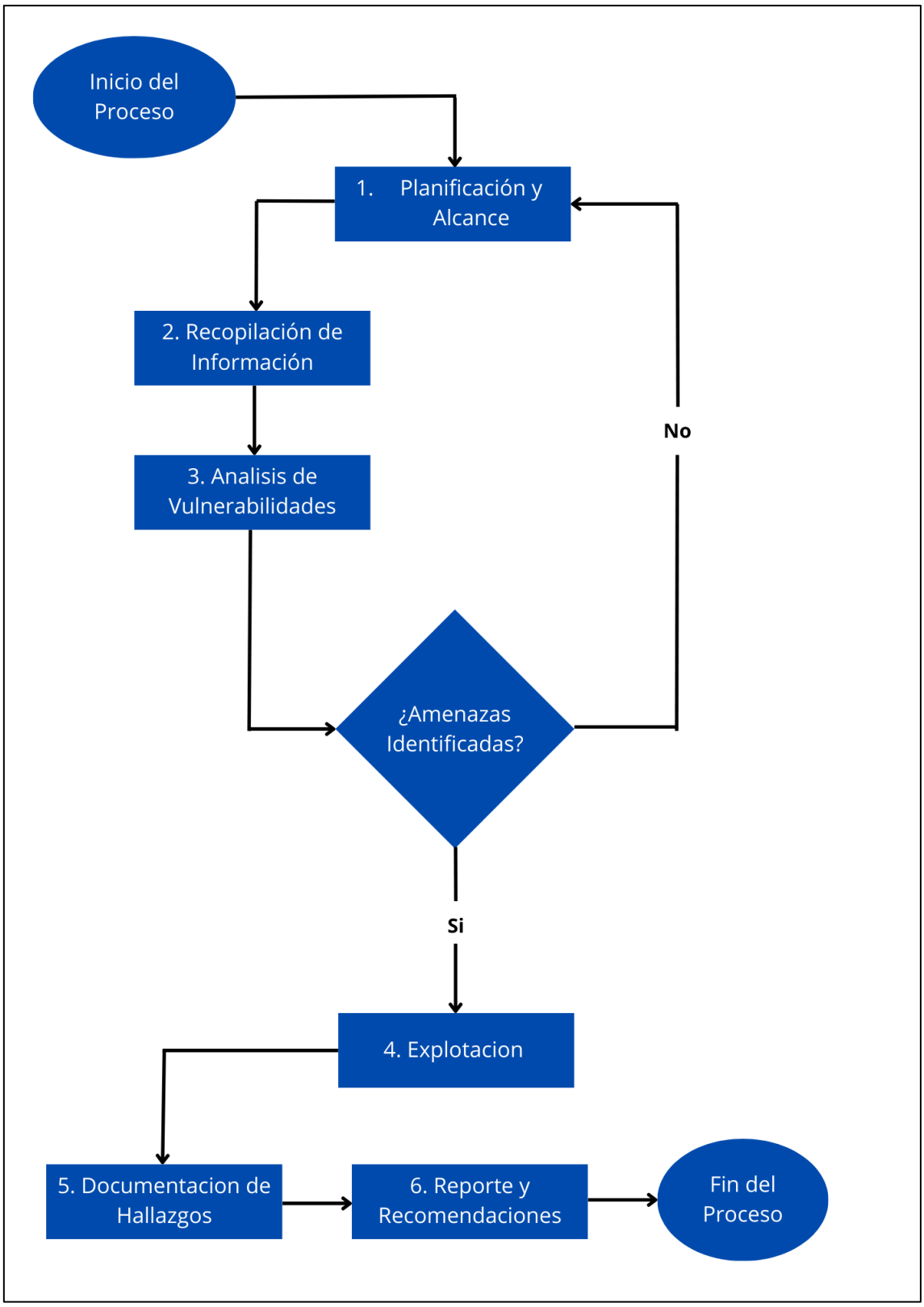
- Registrar todas las vulnerabilidades
- Clasificar por severidad
- Documentar pasos de reproducción

6. Reporte y Recomendaciones:

- Generar informe detallado
- Proponer soluciones específicas
- Priorizar acciones correctivas

Figura 8

Flujograma Sobre los Pasos Principales de la Metodología OWASP



Fuente: Grafico adaptado de OWASP. (2024a, enero 21). OWASP Web Security Testing Guide. https://owasp.org/

Para identificar los puertos abiertos y los posibles servicios en ejecución en las direcciones IP que no respondieron correctamente durante el análisis con OWASP ZAP, se utilizó la herramienta Nmap ampliamente reconocida en la industria de ciberseguridad para la identificación de servicios y puertos activos en sistemas objetivo. Este escaneo permitió obtener información detallada sobre el estado de los puertos y los servicios expuestos, facilitando la detección de configuraciones inseguras o servicios no autorizados que podrían representar vectores de ataque.

- **Configuración de instalación de OWASP ZAP**

Se configuró la herramienta OWASP ZAP, aprovechando su capacidad para realizar análisis dinámicos de seguridad sobre los sistemas informáticos. Esta herramienta permitió detectar vulnerabilidades críticas en los sistemas informáticos de la empresa.

- **Descarga e instalación de OWASP ZAP:**

OWASP ZAP fue descargado desde su sitio oficial e instalado en un equipo destinado exclusivamente para la realización de pruebas. Se configuraron los parámetros iniciales para garantizar su correcto funcionamiento en el entorno de red de IANCEM.

- **Configuración personalizada:**

Se integraron los componentes necesarios para habilitar análisis específicos. Esto incluyó:

- **Configuración de un proxy:** Para monitorear las interacciones entre los clientes y los servidores.
- **Integración con los sistemas evaluados:** Se proporcionaron las direcciones URL y los endpoints críticos de los servicios a evaluar.
- **Reglas de análisis personalizadas:** Basadas en los riesgos identificados previamente y en las recomendaciones de OWASP para sistemas informáticos.

- **Ejecución de pruebas:**

La herramienta fue utilizada accediendo a través de su interfaz en el puerto predeterminado `http://localhost:8080`. Durante la ejecución, se realizaron escaneos dinámicos completos, identificando vulnerabilidades relacionadas con:

- Inyecciones de código.
- Configuraciones de seguridad incorrectas.
- Exposición de datos sensibles.
- Autenticación y control de acceso.

- **Documentación de hallazgos:**

Los resultados de las pruebas fueron documentados utilizando las funcionalidades de generación de informes de OWASP ZAP, proporcionando un resumen detallado del tipo de vulnerabilidad, su severidad y las recomendaciones específicas de mitigación.

2.3 Aspectos clave del análisis

1. **Revisión de estándares OWASP:**

Se utilizó la metodología OWASP Top 10 para identificar las vulnerabilidades más comunes y críticas, alineando el análisis con las mejores prácticas reconocidas internacionalmente.

2. **Entrevistas con personal técnico:**

Se consultó con los desarrolladores de la empresa para entender los procesos de desarrollo y las prácticas actuales de seguridad en las aplicaciones web.

3. **Observación y análisis en profundidad:**

Se analizó la estructura de las aplicaciones web de IANCEM, incluyendo sus componentes, funcionalidad y configuraciones. Este paso fue esencial para identificar posibles puntos débiles.

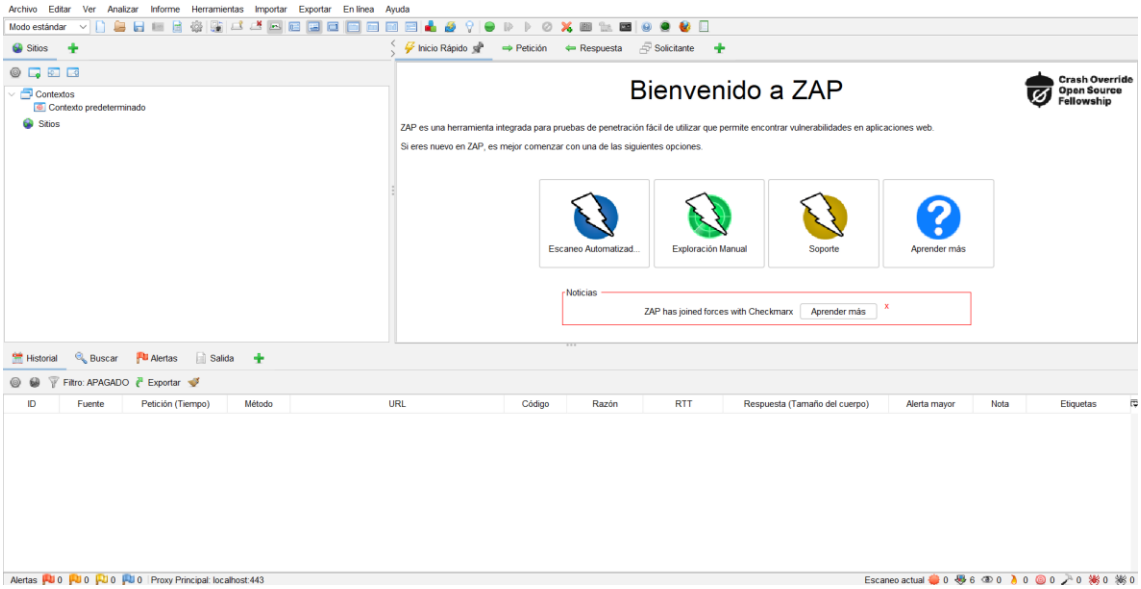
4. **Pruebas de penetración con OWASP ZAP:**

Se realizaron pruebas controladas para simular ataques y evaluar cómo responderían los sistemas ante amenazas reales.

5. **Análisis de riesgos:**

Se evaluaron los riesgos en términos de impacto técnico y comercial, priorizando las vulnerabilidades con base en su severidad y probabilidad de ocurrencia.

Figura 9
Herramienta de OWASP ZAP



Fuente: Diego Fernando Guerra

En la **Figura 8**, se muestra la herramienta OWASP ZAP. La cual será la encargada de llevar a cabo los análisis a los sistemas informáticos de la empresa IANCEM.

- **Descarga e Instalación de Nmap**

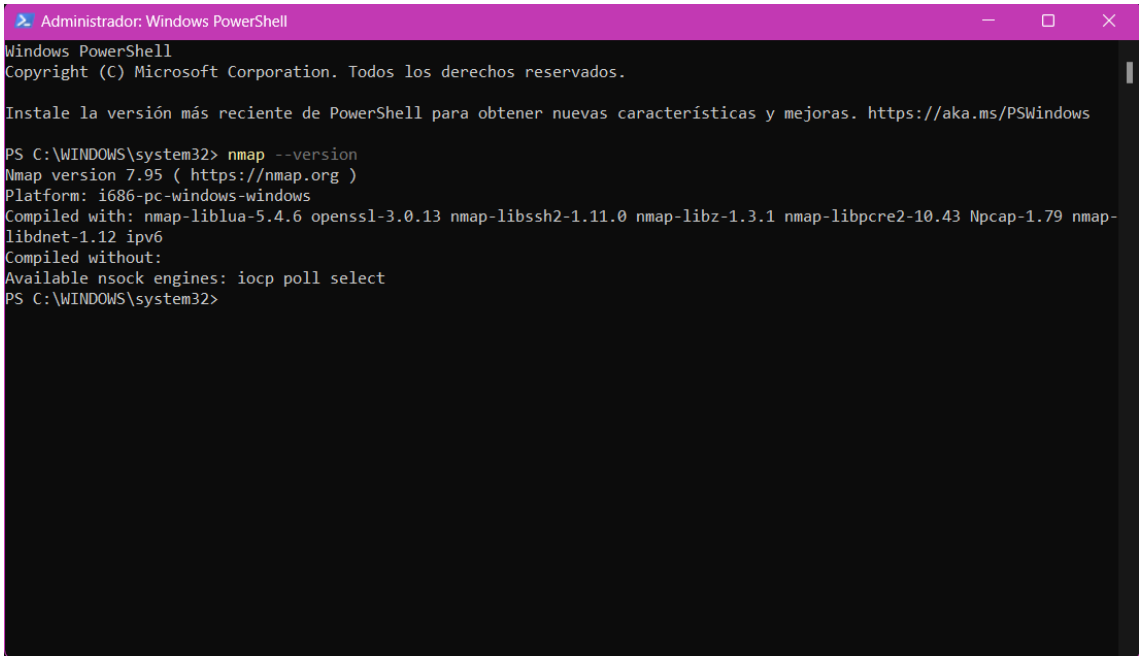
Nmap fue descargado desde su sitio oficial e instalado en un equipo configurado exclusivamente para las pruebas de seguridad. Durante la instalación, se habilitaron los módulos adicionales necesarios para realizar un análisis avanzado de la red interna y externa de IANCEM.

- **Configuración de instalación de Nmap**

Nmap fue implementado como herramienta clave para el escaneo y análisis de los sistemas de red de la empresa IANCEM. Gracias a su capacidad para descubrir servicios,

puertos abiertos y configuraciones inseguras, Nmap permitió identificar posibles vectores de ataque en la infraestructura tecnológica.

Figura 10
Herramienta de Nmap



Fuente: Diego Fernando Guerra

En la **Figura 9**, se presenta el resultado de la instalación de la herramienta Nmap en la cual podemos ver la plataforma en la que está instalada y la versión de esta misma también es la cual nos ayudara para analizar los puertos abiertos, los servicios en ejecución y la versión detectada de cada servicio.

CAPITULO III

RESULTADOS

Este capítulo presenta los resultados obtenidos del análisis de seguridad realizado a los sistemas informáticos de la empresa IANCEM, con el objetivo de identificar vulnerabilidades. El análisis se llevó a cabo siguiendo una metodología basada en las mejores prácticas de seguridad, utilizando herramientas como OWASP ZAP, que facilitó la identificación de fallos de seguridad en cada uno de los sistemas.

Los resultados obtenidos se presentan de manera detallada en matrices y tablas que permiten visualizar las vulnerabilidades encontradas, su severidad y su impacto potencial en la confidencialidad, integridad y disponibilidad de los sistemas de la empresa. Estos resultados sirven como base para priorizar las acciones correctivas y mejorar la seguridad de las plataformas web de IANCEM, asegurando la protección de la información sensible y fortaleciendo la infraestructura frente a posibles ciberataques.

Adicionalmente, se empleó la herramienta Nmap para realizar un escaneo detallado de la infraestructura de red de IANCEM. Nmap permitió identificar puertos abiertos, servicios en ejecución presentes en los sistemas analizados. Estos resultados complementaron el análisis general y proporcionaron información crítica para la implementación de medidas correctivas que fortalezcan la seguridad de la infraestructura tecnológica frente a amenazas externas e internas, a continuación, se presenta el listado de los servidores que se analizó:

- Servidor de nomina
- Servidor RP
- Servidor de base de datos y aplicaciones (Backup)
- Servidor virtualizado
- Servidor de archivos
- Servidor dns
- Active directory
- Servidor replicado (Esxi)
- Servidor de cámaras
- Servidor linux – ubuntu 22 de inteligencia artificial
- Servidor de aplicaciones principal

3. Clasificación de vulnerabilidades encontradas

Durante el análisis a los servidores de IANCEM se identificaron diferentes vulnerabilidades. Estas debilidades pueden facilitar ataques como la inyección de código malicioso, clickjacking y ejecución de scripts no autorizados, comprometiendo la confidencialidad, integridad y disponibilidad de los sistemas.

Figura 11

Servidor de Archivos

Alert type	Risk	Count
Metadatos de la Nube Potencialmente Expuestos	Alto	1 (20,0 %)
Cabecera Content Security Policy (CSP) no configurada	Medio	3 (60,0 %)
Falta de cabecera Anti-Clickjacking	Medio	3 (60,0 %)
Falta encabezado X-Content-Type-Options	Bajo	3 (60,0 %)
Aplicación Web Moderna	Informativo	3 (60,0 %)
Total		5

Fuente: OWASP ZAP

En la Figura 11, se puede observar las diferentes vulnerabilidades encontradas en el servidor de archivos las cuales están clasificadas por riesgo.

Figura 12

Servidor RP

Tipo de alerta	Riesgo	Contar
Cabecera Política de seguridad de contenidos (CSP) no configurada	Medio	4 (133,3 %)
Falta de cabecera Anti-Clickjacking	Medio	1 (33,3 %)
Falta encabezado X-Content-Type-Options	Bajo	1 (33,3 %)
Total		3

Fuente: OWASP ZAP

En la Figura 12 se presentan las vulnerabilidades identificadas en el Servidor RP. Las brechas de seguridad señaladas podrían ser explotadas para comprometer la integridad y disponibilidad del servidor.

Figura 13

Servidor DNS

Tipo de alerta	Riesgo	Contar
Cabecera Política de seguridad de contenidos (CSP) no configurada	Medio	15 (300,0 %)
Falta de cabecera Anti-Clickjacking	Medio	2 (40,0 %)
El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP	Bajo	16 (320,0 %)
Falta encabezado X-Content-Type-Options	Bajo	3 (60,0 %)
Divulgación de información - Comentarios sospechosos	Informativo	2 (40,0 %)
Total		5

Fuente: OWASP ZAP

En la Figura 13 se detalla las vulnerabilidades encontradas en el servidor DNS las cuales no son criticas, pero no dejan de ser vulnerabilidades que si llegan a ser detectadas pueden generar daños al servidor.

Figura 14

Servidor Active Directory

Tipo de alerta	Riesgo	Contar
Cabecera Content Security Policy (CSP) no configurada	Medio	15 (300,0 %)
Falta de cabecera Anti-Clickjacking	Medio	2 (40,0 %)
El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP	Bajo	16 (320,0 %)
Falta encabezado X-Content-Type-Options	Bajo	3 (60,0 %)
Divulgación de información - Comentarios sospechosos	Informativo	2 (40,0 %)
Total		5

Fuente: OWASP ZAP

En la Figura 14 Las fallas identificadas podrían facilitar accesos no autorizados, permitiendo modificaciones en la configuración de hardware y software que pueden afectar el rendimiento y la seguridad de la infraestructura.

Figura 15

Servidor Virtualizado (VMWARE Replicación)

Tipo de alerta	Riesgo	Contar
CSP: Directiva Comodín	Medio	3 (42,9 %)
CSP: script-src inseguro en línea	Medio	3 (42,9 %)
CSP: estilo-fuente-inseguro-en-línea	Medio	3 (42,9 %)
Archivo oculto encontrado (Archivo Oculto Encontrado)	Medio	4 (57,1 %)
Divulgación de información - Comentarios sospechosos	Informativo	11 (157,1 %)
Reexaminar las Directivas de Control de Caché	Informativo	2 (28,6 %)
Agente de usuario Fuzzer	Informativo	24 (342,9 %)
Total		7

Fuente: OWASP ZAP

En la Figura 15 expone las vulnerabilidades halladas en el **Servidor de Archivos**. Se resaltan los puntos débiles que podrían ser aprovechados para acceder o modificar información sensible almacenada, comprometiendo la confidencialidad y la integridad de los datos corporativos.

Figura 16

Servidor de Cámaras

Tipo de alerta	Riesgo	Contar
Cabecera Política de seguridad de contenidos (CSP) no configurada	Medio	3 (42,9 %)
Divulgación de Marcas de Tiempo - Unix	Bajo	93 (1.328,6 %)
Falta encabezado X-Content-Type-Options	Bajo	9 (128,6 %)
Aplicación Web Moderna	Informativo	1 (14,3 %)
Divulgación de información - Comentarios sospechosos	Informativo	6 (85,7 %)
Librería JS Vulnerable	Informativo	2 (28,6 %)
Agente de usuario Fuzzer	Informativo	22 (314,3 %)
Total		7

Fuente: OWASP ZAP

En la Figura 16 se presentan las vulnerabilidades identificadas en el Servidor DNS. Las deficiencias señaladas podrían ser explotadas para redirigir el tráfico de la red, facilitando ataques de phishing o intercepción de comunicaciones.

Figura 17

Servidor de Base de Datos y Aplicaciones

Alert type	Risk	Count
Cabecera Content Security Policy (CSP) no configurada	Medio	3 (33,3 %)
Falta de cabecera Anti-Clickjacking	Medio	1 (11,1 %)
Cookie Sin Flag HttpOnly	Bajo	1 (11,1 %)
Cookie sin el atributo SameSite	Bajo	1 (11,1 %)
Divulgación de Información - Mensajes de Error de Depuración	Bajo	1 (11,1 %)
El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP	Bajo	4 (44,4 %)
Falta encabezado X-Content-Type-Options	Bajo	2 (22,2 %)
Divulgación de información - Comentarios sospechosos	Informativo	2 (22,2 %)
Respuesta de Gestión de Sesión Identificada	Informativo	3 (33,3 %)
Total		9

Fuente: OWASP ZAP

En la Figura 17 se destacan las áreas críticas que requieren atención para proteger la confidencialidad y disponibilidad de la información financiera y personal de los empleados.

Tabla 5

Resumen Cuantitativo de los Riesgos de Cada Servidor

SERVIDOR	ALTO	MEDIO	BAJO	INFORMATIVO	RIESGO TOTAL
Servidor RP	0	2	1	0	3
Servidor de Nómina	1	3	2	0	6
Servidor de Base de Datos y Aplicaciones (Backup)	2	4	2	0	8

SERVIDOR	ALTO	MEDIO	BAJO	INFORMATIVO	RIESGO TOTAL
Servidor Virtualizado	2	3	3	0	8
Servidor de Archivos	1	2	1	1	5
Servidor DNS	0	2	2	1	5
Active Directory (2 IPS)	0	2	2	1	5
	3	6	3	2	14
Servidor Replicado (Esxi)	0	4	3	0	7
Servidor de Cámaras	0	1	2	4	7
Servidor Linux – Ubuntu 22 de IA	1	1	3	0	5
Servidor de Aplicaciones Principal	0	2	5	2	9
SEVERIDAD TOTAL	17	32	29	11	83

Fuente: Tabla elaborada bajo los resultados dados de cada análisis por Diego Fernando Guerra.

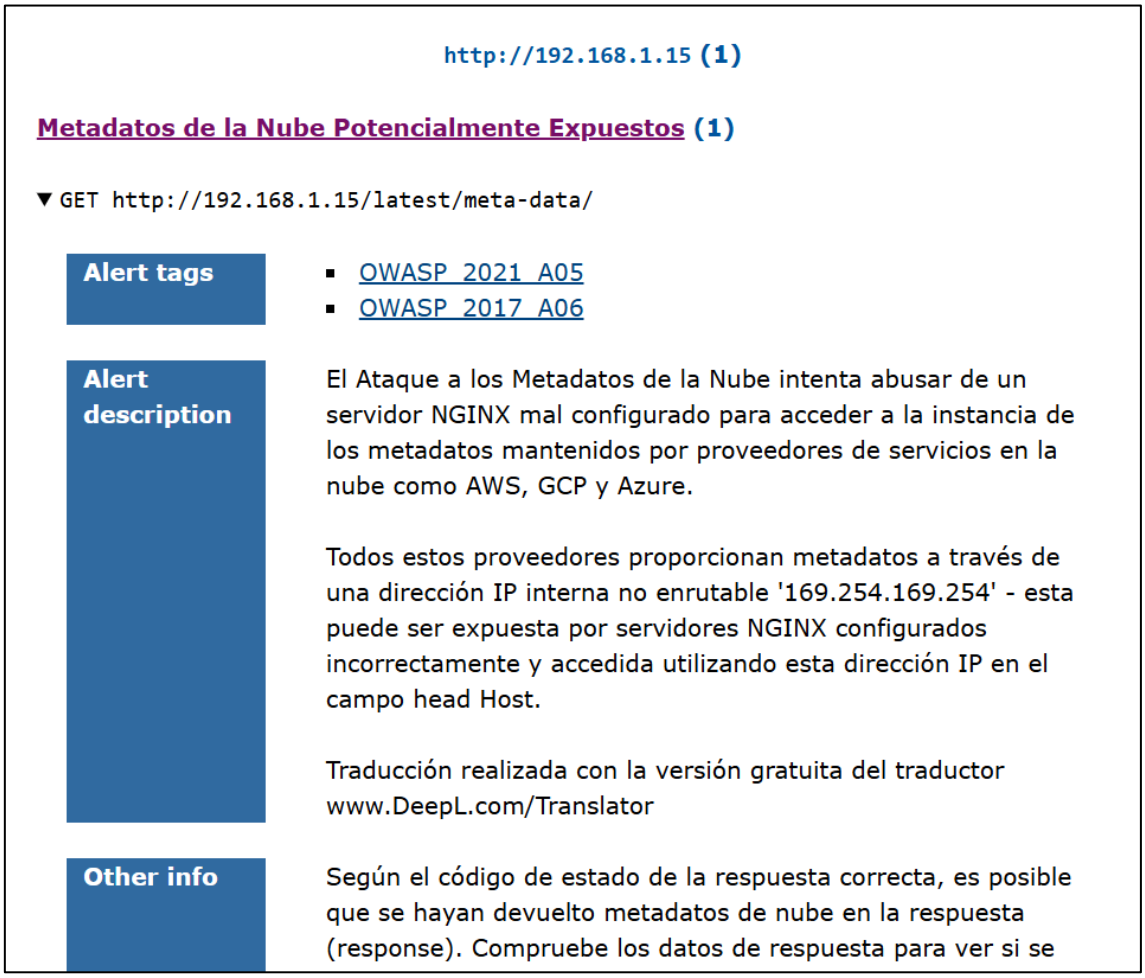
3.1 Vulnerabilidades de riesgo ALTO

3.1.1 Vulnerabilidad de Metadatos Expuestos

Explicación: Esta alerta indica que la aplicación podría estar exponiendo metadatos de la nube debido a una configuración incorrecta del servidor, permitiendo el acceso a información sensible del entorno de la nube.

Impacto: Un atacante podría acceder a metadatos de la instancia, lo que puede incluir credenciales, configuraciones y otra información sensible, comprometiendo la seguridad de la aplicación y la infraestructura subyacente.

Figura 18
Vulnerabilidad de Tipo "Metadatos de la Nube Potencialmente Expuestos"



Fuente: OWASP ZAP

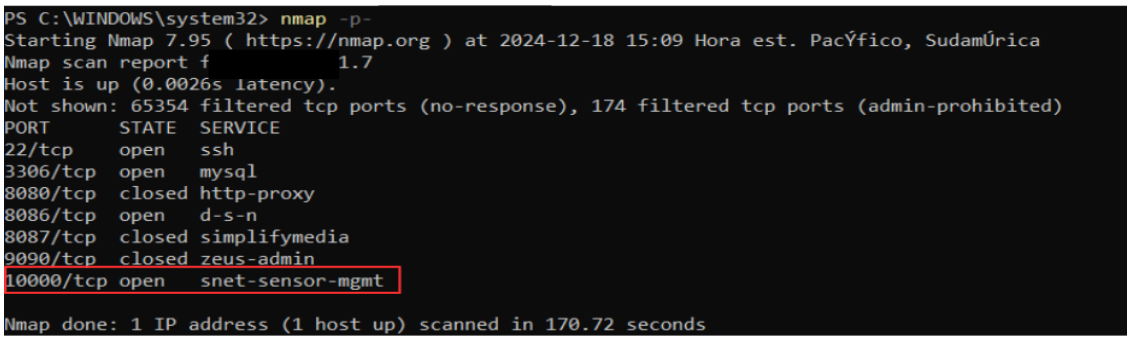
3.1.2 Vulnerabilidad en el Servidor de Nomina en el Puerto 1000/tcp

Explicación: Este puerto generalmente está asociado con servicios de administración, como Webmin, que permite la gestión remota de sistemas.

Impacto: Existe la posibilidad de que un atacante tome control total del servidor de nómina, también hay riesgo de exposición de información confidencial como salarios e identificaciones del personal.

Figura 19

Vulnerabilidad en el Puerto 10000/tcp: snet-sensor-mgmt del Servidor de Nomina



Fuente: Nmap

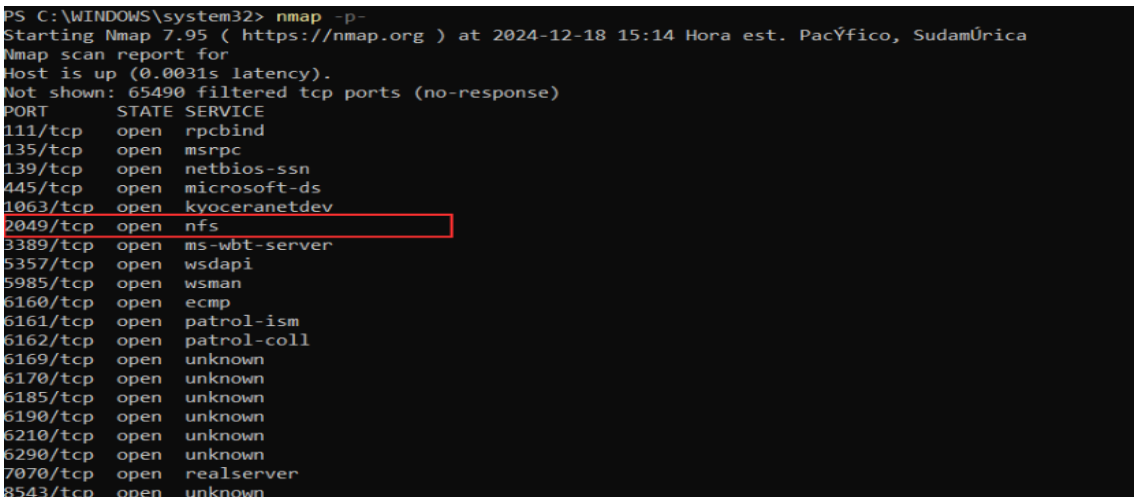
3.1.3 Vulnerabilidad en el Servidor de Base de Datos y Aplicaciones (Backup) en el Puerto 2049/tcp

Explicación: Este puerto está asociado al servicio **NFS**, utilizado para compartir archivos en red. Si no está configurado adecuadamente, puede permitir que usuarios no autorizados accedan o modifiquen archivos críticos en el servidor.

Impacto: Existe la posibilidad de que se alteren archivos importantes, comprometiendo la integridad del sistema. Un atacante podría usar este punto de entrada para intentar acceder a otros sistemas conectados en la red.

Figura 20

Vulnerabilidad en el Puerto 2049/tcp (NFS - Network File System) del servidor de Base de Datos y Aplicaciones (Backup)



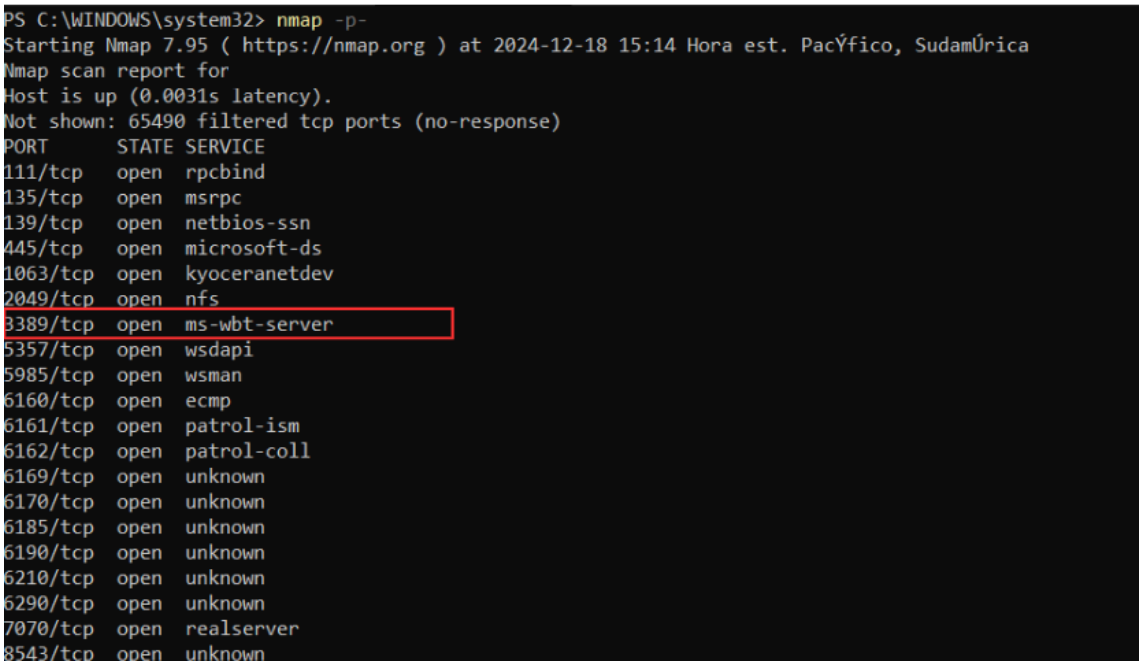
Fuente: Nmap

3.1.4 Vulnerabilidad en el Puerto 3389/tcp

Explicación: El puerto 3389 está relacionado con el servicio de Escritorio Remoto (RDP) de Microsoft. RDP es un objetivo común de los atacantes, especialmente para ataques de fuerza bruta y explotación de vulnerabilidades conocidas.

Impacto: Existe el riesgo de un compromiso total del sistema, donde un atacante podría obtener privilegios administrativos para ejecutar comandos o instalar software malicioso.

Figura 21
Vulnerabilidad en el Puerto 3389/tcp (MS-RDP - Microsoft Remote Desktop Protocol) del Servidor de Base de Datos y Aplicaciones (Backup)



Fuente: Nmap

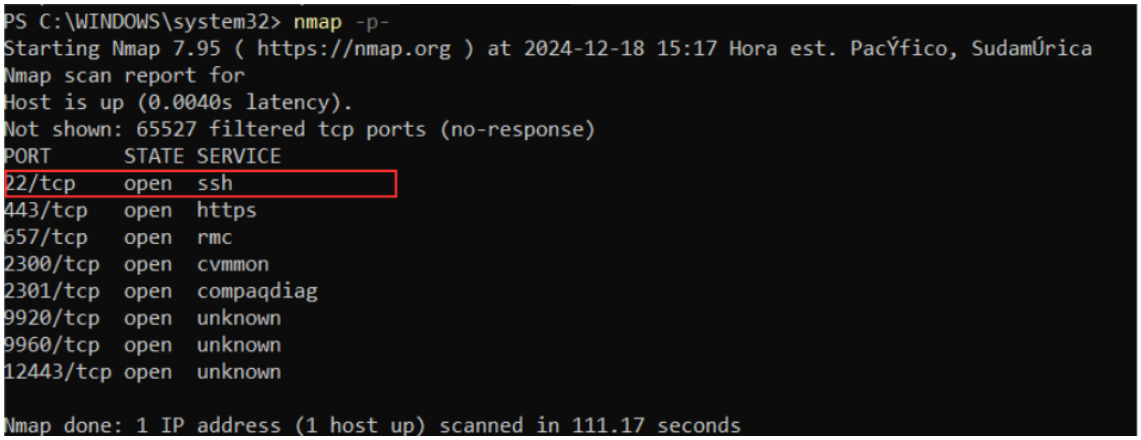
3.1.5 Vulnerabilidad en el Servidor Virtualizado en el Puerto 22/tcp

Explicación: Aunque SSH es un protocolo seguro utilizado para la administración remota, si no se configura adecuadamente, puede ser objetivo de ataques de fuerza bruta, intentos de acceso no autorizado y explotación de vulnerabilidades en implementaciones antiguas o mal actualizadas.

Impacto: Existe la amenaza de que un atacante obtenga control total del servidor virtualizado al comprometer las credenciales SSH, con este acceso SSH, el atacante podría desactivar las medidas de seguridad existentes o instalar malware que persista en el sistema.

Figura 22

Vulnerabilidad en el Puerto 22/tcp (SSH - Secure Shell) del Servidor Virtualizado



Fuente: Nmap

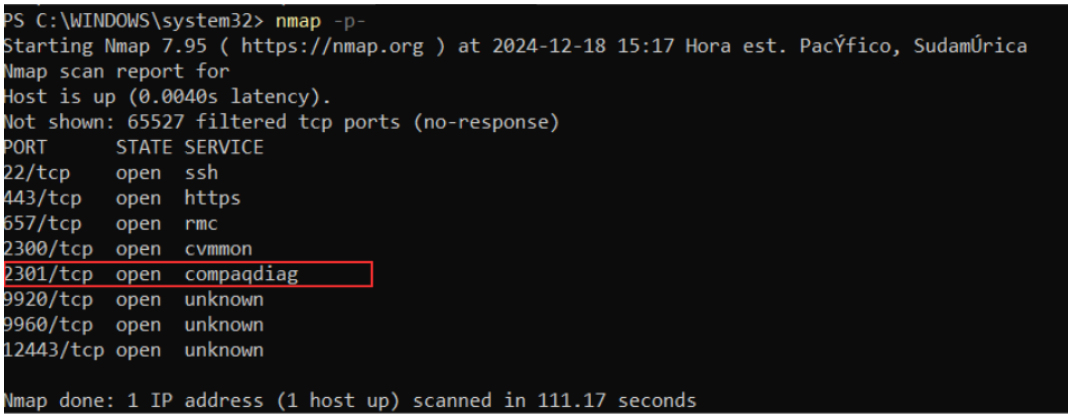
3.1.6 Vulnerabilidad en el Servidor Virtualizado en el Puerto 2301/tcp

Explicación: El puerto 2301 corresponde a la interfaz del Compaq Insight Manager, una herramienta para la administración de hardware en servidores.

Impacto: Este servicio puede ser vulnerable a ataques si no está configurado con autenticación robusta, también si está expuesto a redes no confiables o utiliza una versión obsoleta con vulnerabilidades conocidas.

Figura 23

Vulnerabilidad en el Puerto 2301/tcp (Compaq Insight Manager - compaqdiag) del Servidor Virtualizado



Fuente: Nmap

3.1.7 Vulnerabilidades en el Active Directory

Puerto 389/tcp (LDAP sin cifrar): Este protocolo permite consultas y autenticaciones al AD, pero al no usar cifrado, expone credenciales y datos sensibles a interceptación por ataques de tipo *Man-in-the-Middle*.

Puerto 445/tcp (SMB - Microsoft-DS): SMB es vulnerable a ataques como *EternalBlue* o *Pass-the-Hash*, lo que podría permitir a un atacante comprometer el servidor o realizar movimientos laterales dentro de la red.

Puerto 3268/tcp (Global Catalog LDAP sin cifrar): El catálogo global expone información de usuarios y objetos del dominio. Si no se cifra, es vulnerable a intercepción o abuso por actores malintencionados.

Impacto: Estas vulnerabilidades pueden llevar al compromiso de cuentas privilegiadas, fuga de información sensible del AD y acceso no autorizado al dominio, lo que pone en riesgo la seguridad de toda la infraestructura organizacional.

Figura 24

Vulnerabilidades en Active Directory

```
PS C:\WINDOWS\system32> nmap -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-18 15:20 Hora est. PacŶfico, SudamÚrica
Nmap scan report for
Host is up (0.0010s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
53/tcp    open     domain
88/tcp    open     kerberos-sec
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
389/tcp   open     ldap
445/tcp   open     microsoft-ds
464/tcp   open     kpasswd5
623/tcp   filtered oob-ws-http
636/tcp   open     ldapssl
664/tcp   filtered secure-aux-bus
3268/tcp  open     globalcatLDAP
3269/tcp  open     globalcatLDAPssl
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds
```

Fuente: Nmap

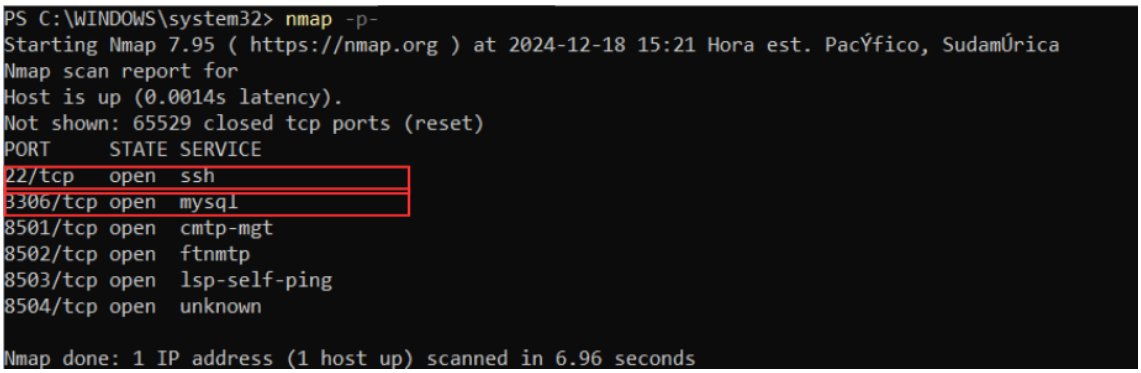
3.1.8 Vulnerabilidad en el servidor Ubuntu IA

Puerto 22/tcp (SSH): Si el servicio SSH está configurado sin medidas de seguridad adecuadas, como autenticación mediante claves, desactivación de acceso root remoto o implementación de políticas de tiempo límite y bloqueo, es vulnerable a ataques de fuerza bruta o acceso no autorizado, comprometiendo el servidor y los datos sensibles asociados.

Puerto 3306/tcp (MySQL): Este puerto expone el servicio de base de datos MySQL. Si no está protegido adecuadamente mediante políticas de acceso restrictivas, contraseñas robustas y cifrado, un atacante podría acceder o manipular los datos almacenados en las bases de datos, comprometiendo su confidencialidad e integridad.

Impacto: Estas vulnerabilidades pueden ser explotadas para obtener acceso no autorizado al servidor, comprometer modelos de inteligencia artificial en desarrollo, extraer información confidencial de las bases de datos o interrumpir las operaciones críticas.

Figura 25
Vulnerabilidad en el servidor Ubunto IA



Fuente: Nmap

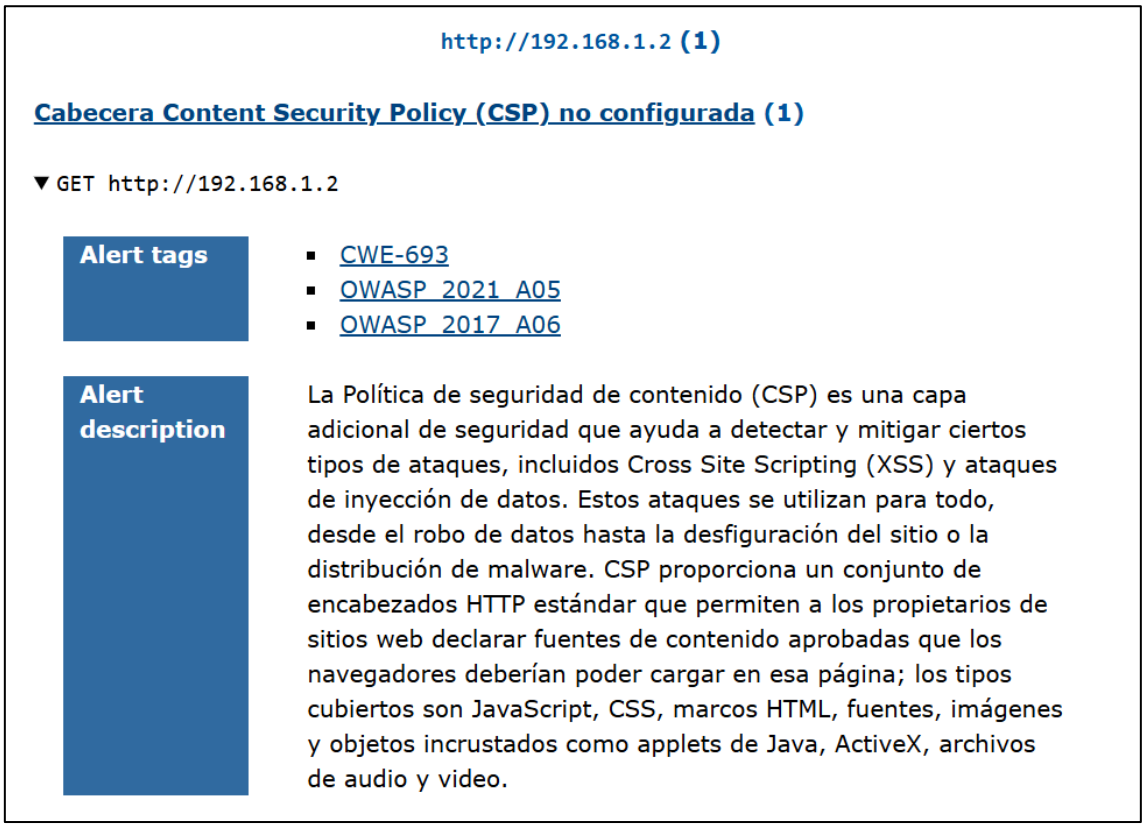
3.2 Vulnerabilidades de riesgo MEDIO

3.2.1 Vulnerabilidad de Cabecera no Configurada

Descripción: La Política de Seguridad de Contenidos (CSP) es una medida de seguridad que ayuda a prevenir ataques como Cross-Site Scripting (XSS) al controlar los recursos que el navegador puede cargar.

Impacto: Sin una CSP adecuada, un atacante podría inyectar scripts maliciosos en la aplicación, comprometiendo la integridad y confidencialidad de los datos de los usuarios.

Figura 26
Vulnerabilidad de Tipo "CSP"



Fuente: OWASP ZAP

3.2.2 Vulnerabilidad de Cabecera Anti-Clickjacking

Explicación: La cabecera X-Frame-Options se utiliza para proteger contra ataques de clickjacking, evitando que la página sea cargada dentro de un marco (iframe) en otro sitio. La ausencia de esta cabecera permite que la página sea incrustada en otros sitios, lo que podría ser explotado para engañar a los usuarios y realizar acciones no deseadas.

Impacto: Un atacante podría incrustar la página en un sitio malicioso y superponer elementos visuales para engañar al usuario, logrando que realice acciones involuntarias, como clics en botones o enlaces, comprometiendo la seguridad de la información y las operaciones del usuario.

Figura 27
Vulnerabilidad de Tipo "Cabecera Anti-Clickjacking"

Fuente: OWASP ZAP

3.2.3 Vulnerabilidades en el Servidor RP

Puerto 23(Telnet): Telnet es un protocolo antiguo para comunicación remota que no utiliza cifrado, lo que lo hace vulnerable a ataques como acceso no autorizado.

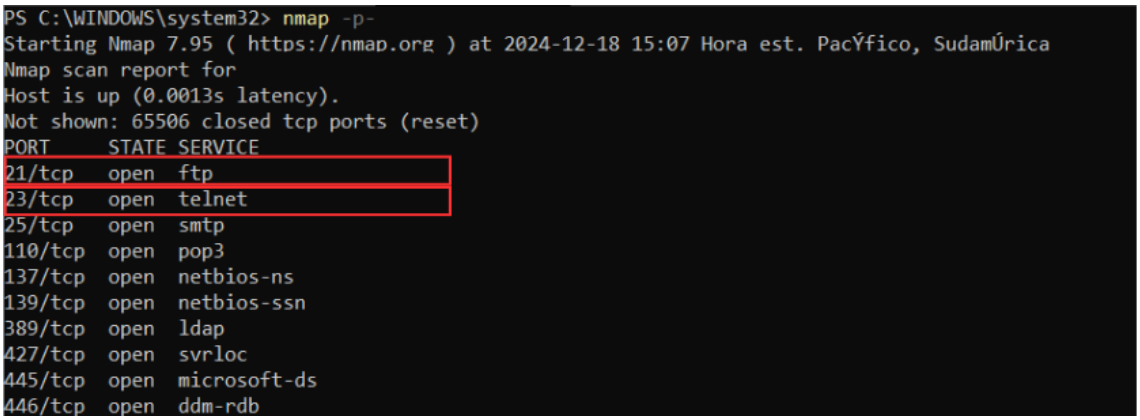
Impacto: Aunque no se clasifica como alta porque no tiene una vulnerabilidad específica reportada, su naturaleza insegura eleva el riesgo.

Puerto 21(FTP): El servicio FTP (File Transfer Protocol) puede ser un riesgo si:

- Está configurado sin cifrado (modo activo o pasivo sin TLS/SSL).
- Permite accesos anónimos o utiliza credenciales débiles.

Impacto: FTP transmite datos en texto plano, lo que lo hace susceptible a ataques de intermediario (MITM) o robo de credenciales.

Figura 28
Vulnerabilidades del Servidor RP



Fuente:Nmap

3.2.4 Vulnerabilidades en el Servidor de Nomina

Puerto 22/tcp(SSH): Aunque no representa un riesgo alto, una configuración inadecuada del servicio SSH, como la ausencia de medidas de autenticación robusta (por ejemplo, claves SSH) o políticas de bloqueo de intentos fallidos.

Puerto 3306/tcp (MySQL): La exposición del servicio de base de datos MySQL puede ser explotada por atacantes que aprovechen credenciales débiles o configuraciones inadecuadas.

Puerto 8086/tcp (InfluxDB): Este puerto sugiere la presencia de InfluxDB, una base de datos para series temporales.

Impacto: Estas vulnerabilidades medias, aunque no críticas por sí mismas, pueden ser explotadas en conjunto para obtener información valiosa o acceso inicial al servidor.

Figura 29
Vulnerabilidades en el Servidor de Nomina

```
PS C:\WINDOWS\system32> nmap -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-18 15:09 Hora est. PacÝfico, SudamÚrica
Nmap scan report for
Host is up (0.0026s latency).
Not shown: 65354 filtered tcp ports (no-response), 174 filtered tcp ports (admin-prohibited)
PORT      STATE  SERVICE
22/tcp    open   ssh
3306/tcp  open   mysql
8080/tcp  closed http-proxy
8086/tcp  open   d-s-n
8087/tcp  closed simplifymedia
9090/tcp  closed zeus-admin
10000/tcp open   snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 170.72 seconds
```

Fuente: Nmap

3.2.5 Vulnerabilidades en el servidor de Base de Datos y Aplicaciones

Puerto 111/tcp (rpcbind): Este servicio permite mapear solicitudes RPC (Remote Procedure Call) a servicios en el sistema. Si no está configurado correctamente, puede ser utilizado por atacantes para obtener información sobre los servicios RPC disponibles o para llevar a cabo ataques de enumeración.

Impacto: Los atacantes podrían identificar puntos débiles en servicios que dependen de RPC, como NFS.

Puerto 139/tcp (NetBIOS-SSN) y 445/tcp (Microsoft-DS): Estos puertos son utilizados para compartir archivos e impresoras en sistemas Windows mediante SMB (Server Message Block). Las configuraciones predeterminadas o credenciales débiles pueden exponer datos sensibles o permitir la ejecución remota de código.

Impacto: Un atacante podría acceder a archivos compartidos o aprovechar vulnerabilidades conocidas de SMB como "EternalBlue" para comprometer el sistema.

Puerto 5357/tcp (WSDAPI): El protocolo Web Services for Devices (WSD) se utiliza para descubrir e interactuar con dispositivos conectados a la red. Si está habilitado en entornos no controlados, puede ser aprovechado para realizar ataques de red, como spoofing o denegación de servicio.

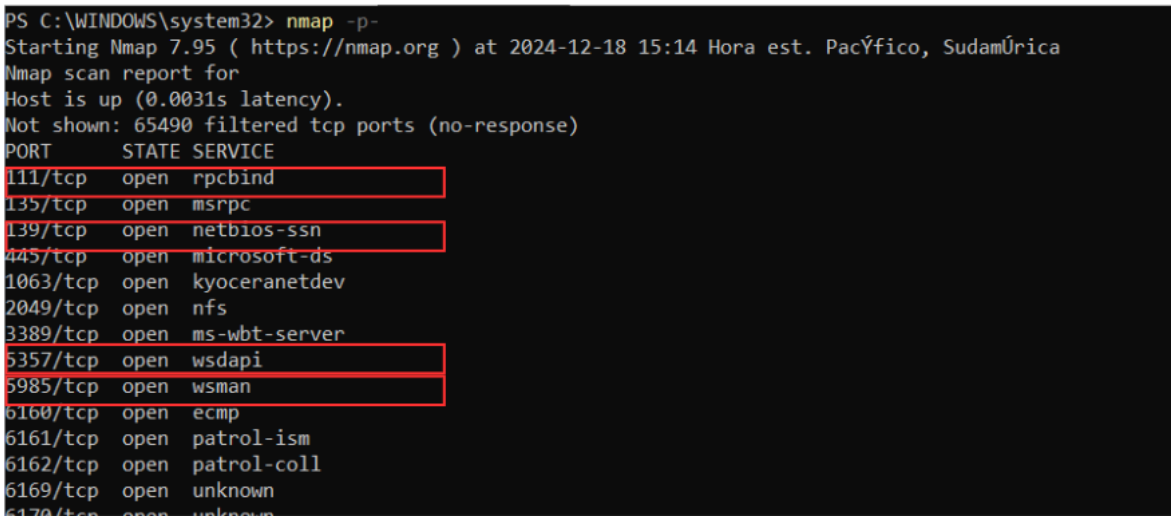
Impacto: Posibilidad de exposición innecesaria de la red interna a través de dispositivos no seguros.

Puerto 5985/tcp (WS-Management): Este puerto se asocia con WinRM (Windows Remote Management), un servicio de administración remota. Sin autenticación adecuada o restricciones de IP, puede permitir a un atacante realizar acciones administrativas en el sistema.

Impacto: Riesgo de comprometer el servidor a través de comandos remotos.

Figura 30

Vulnerabilidades del Servidor de Base de Datos y Aplicaciones



Fuente: Nmap

3.2.6 Vulnerabilidades en el Servidor Virtualizado

Puerto 443/tcp (HTTPS): HTTPS se utiliza para comunicaciones seguras. Sin embargo, si el servidor no cuenta con un certificado SSL/TLS actualizado o usa configuraciones débiles (como soporte a protocolos antiguos o cifrados inseguros), puede ser vulnerable a ataques como exposición de datos sensibles.

Impacto: Permite a un atacante interceptar o manipular las comunicaciones si el cifrado no es seguro.

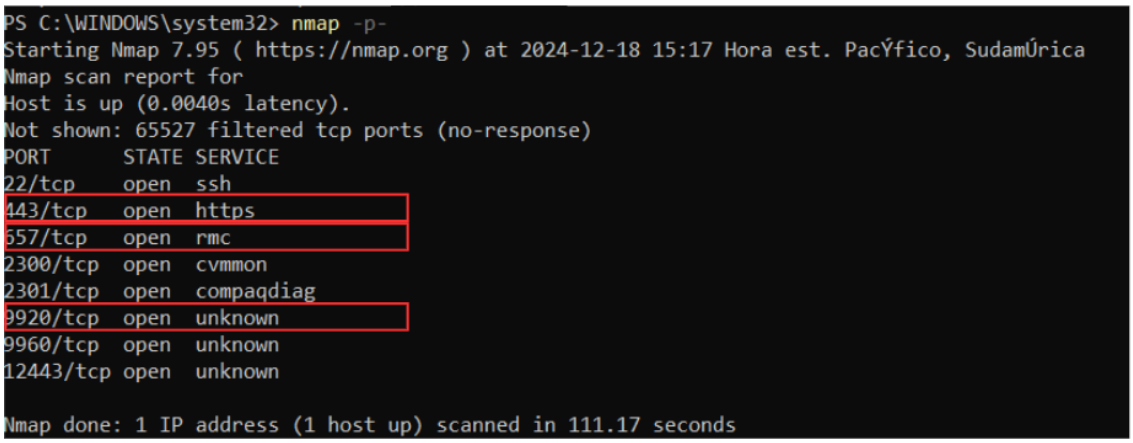
Puerto 657/tcp (RMC - Remote Management Control): Este puerto se asocia con herramientas de administración remota. Si no cuenta con controles de acceso adecuados o se expone públicamente, podría ser explotado para obtener acceso remoto no autorizado.

Impacto: Un atacante podría comprometer el control remoto del servidor y ejecutar comandos maliciosos.

Puerto 9920/tcp (Servicio desconocido): Aunque no se identifica un servicio estándar en este puerto, los servicios desconocidos pueden representar un riesgo si no están documentados o gestionados. Pueden ser aplicaciones personalizadas con vulnerabilidades no parcheadas.

Impacto: Si el servicio no está asegurado, un atacante podría utilizarlo para realizar ataques de enumeración, explotación o acceso no autorizado.

Figura 31
Vulnerabilidades del Servidor Virtualizado



Fuente: Nmap

3.2.7 Vulnerabilidades en el Active Directory

Puerto 53/tcp (Domain - DNS): Utilizado para la resolución de nombres en redes. Si la configuración no está protegida, puede ser vulnerable a ataques de envenenamiento de caché (cache poisoning).

Impacto: Un atacante puede redirigir tráfico o amplificar ataques DDoS.

Puerto 88/tcp (Kerberos-sec): Protocolo de autenticación utilizado por Active Directory. Si está mal configurado o si las claves de cifrado son débiles, puede ser susceptible a ataques de fuerza bruta contra las claves.

Impacto: Compromiso del sistema de autenticación.

Puerto 135/tcp (MSRPC): Utilizado para llamadas a procedimientos remotos en sistemas Windows. Puede ser explotado si se permite acceso no autorizado o si hay vulnerabilidades en los servicios expuestos.

Impacto: Posible ejecución remota de código o recolección de información.

Puerto 464/tcp (Kerberos password change): Permite cambiar contraseñas en el protocolo Kerberos. Si no se protege adecuadamente, un atacante puede ejecutar ataques de repetición (replay attacks).

Impacto: Posibilidad de comprometer cuentas de usuarios.

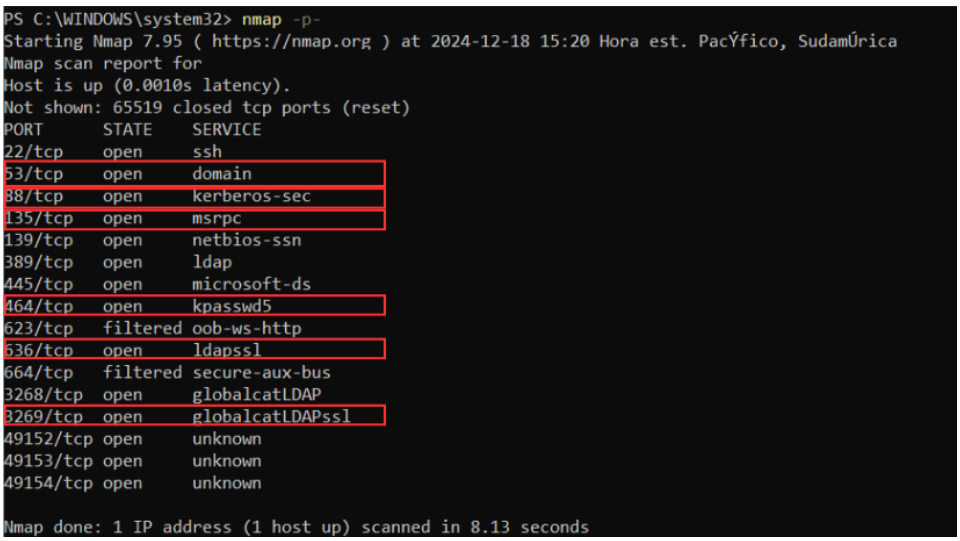
Puerto 636/tcp (LDAP SSL): Proporciona LDAP sobre SSL para cifrar la comunicación. Sin embargo, si el certificado SSL es débil o está mal configurado, podría ser vulnerable a ataques MitM (Man-in-the-Middle).

Impacto: Exposición de datos sensibles o manipulación del tráfico LDAP.

Puerto 3269/tcp (Global Catalog LDAP SSL): Similar al puerto 636, pero relacionado con el catálogo global. La seguridad depende del cifrado SSL, y cualquier mala configuración puede exponerlo a riesgos similares.

Impacto: Compromiso del servicio de catálogo global.

Figura 32
Vulnerabilidades del Active Directory



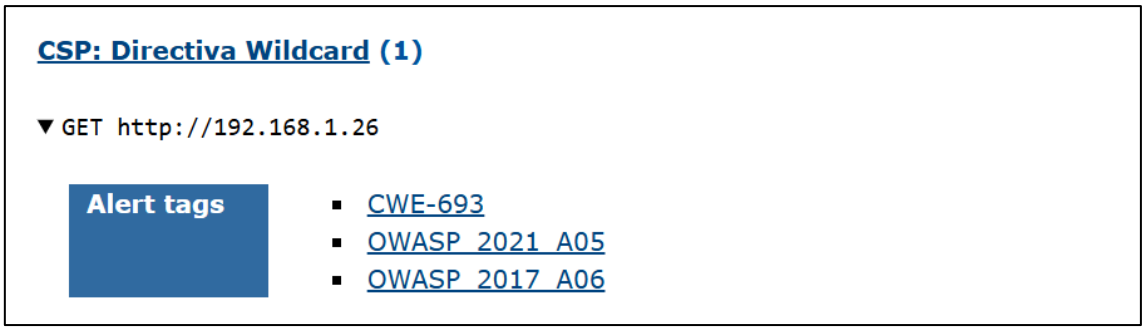
Fuente: Nmap

3.2.8 Vulnerabilidad de tipo Wildcard

CSP: Directiva Wildcard: Se refiere a la configuración de una política de seguridad que permite cargas de recursos desde cualquier fuente (denotada por el símbolo "*"). Esto puede incluir scripts, imágenes, estilos, etc.

Impacto: Al permitir recursos desde cualquier fuente, se abre la puerta a posibles ataques de inyección de contenido malicioso, como Cross-Site Scripting (XSS), ya que los atacantes pueden inyectar código desde cualquier dominio. Esto reduce la capacidad de la CSP para proteger de fuentes no confiables.

Figura 33
Vulnerabilidad CSP: Directiva Wildcard



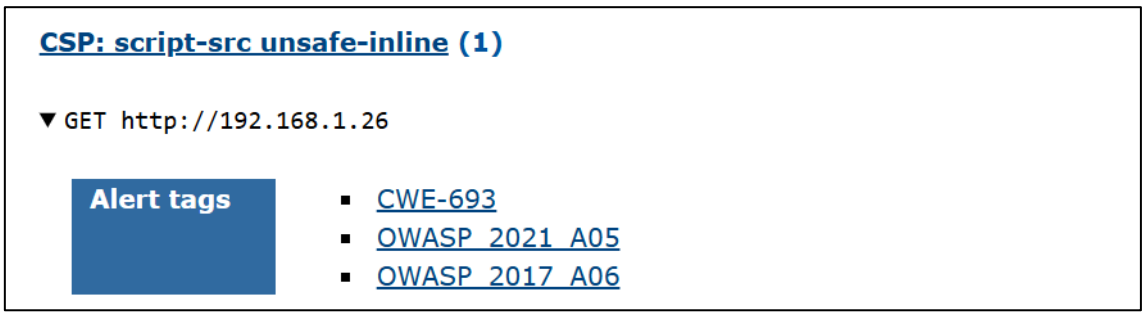
Fuente: OWASP

3.2.9 Vulnerabilidad de tipo Script-src unsafe-inline

CSP: script-src unsafe-inline: Permite la ejecución de scripts inline (aquellos que están directamente dentro de la página HTML, como en un `<script>`), lo que puede ser un riesgo si se inyecta código malicioso.

Impacto: Esta configuración permite que se ejecuten scripts inline, lo que facilita que los atacantes inyecten y ejecuten código malicioso a través de vulnerabilidades como XSS. Al permitir scripts inline, se pierde una capa importante de seguridad que la política de CSP debería proporcionar.

Figura 34
Vulnerabilidad de tipo Script-src unsafe-inline



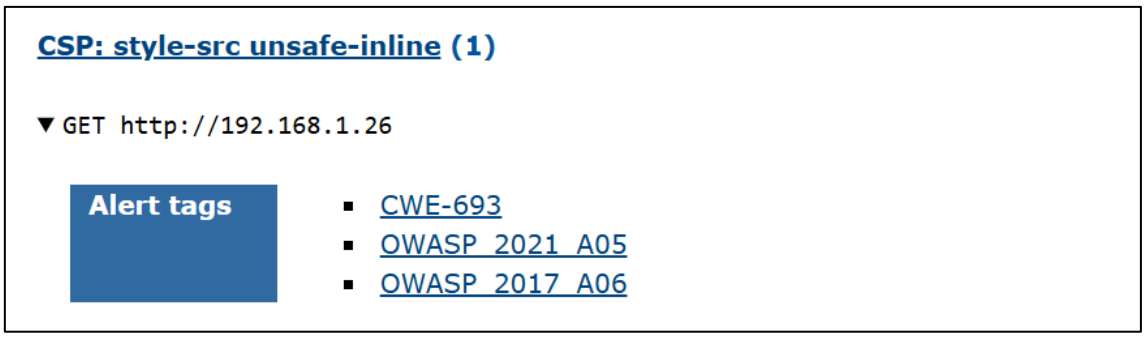
Fuente: OWASP ZAP

3.2.10 Vulnerabilidad de tipo Style-src

CSP: style-src unsafe-inline: Permite la aplicación de estilos CSS inline dentro de la página, lo que incluye estilos en línea o definidos dentro de etiquetas `<style>`.

Impacto: Al permitir estilos inline, se expone la aplicación a riesgos, especialmente si un atacante es capaz de inyectar código CSS malicioso que puede modificar la apariencia de la página y ocultar contenido o redirigir a los usuarios a sitios peligrosos.

Figura 35
Vulnerabilidad de tipo Style-src unsafe-inline



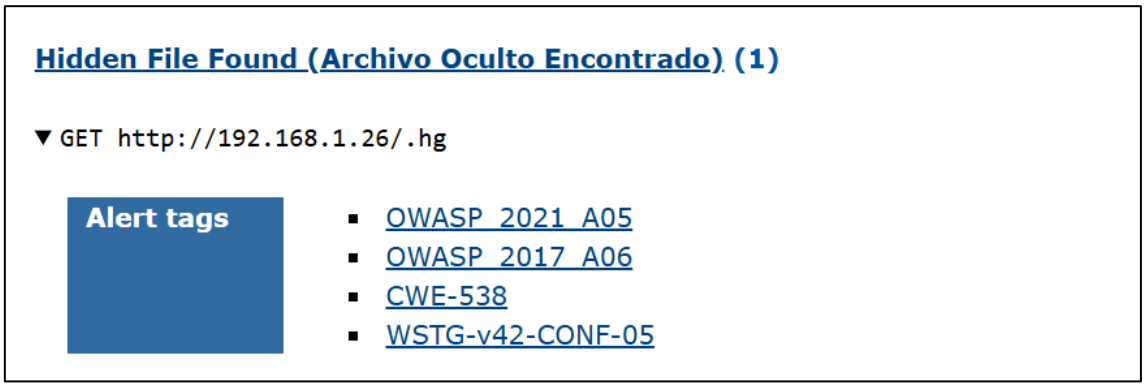
Fuente: OWASP ZAP

3.2.11 Vulnerabilidad de tipo HIdden File Found

Hidden File Found (Archivo Oculto Encontrado): Un archivo oculto en un sistema o aplicación web es un archivo que no es fácilmente accesible o visible, pero que puede contener información sensible o ser utilizado por un atacante para almacenar datos maliciosos.

Impacto: Los archivos ocultos pueden ser utilizados para almacenar scripts maliciosos, credenciales o información confidencial que podría ser explotada por un atacante. Además, pueden pasar desapercibidos en un análisis de seguridad, lo que dificulta su detección y corrección.

Figura 36
Vulnerabilidad de tipo Hidden File Found



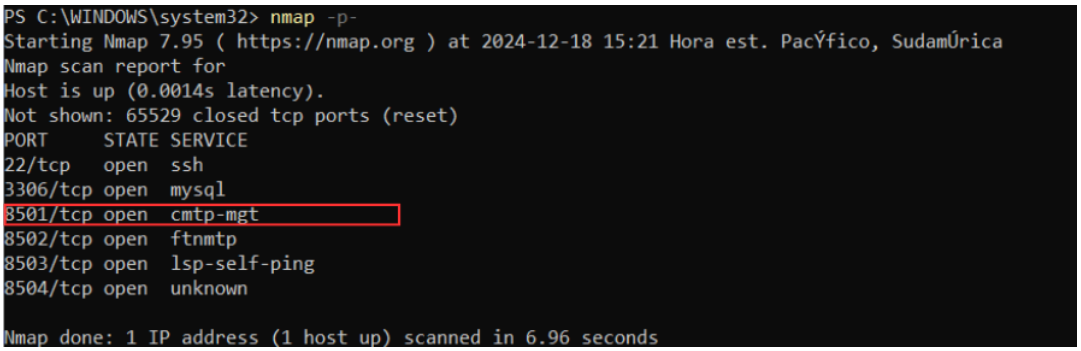
Fuente: OWASP ZAP

3.2.12 Vulnerabilidades del Servidor Ubuntu 22 Linux

Puerto 8501/tcp (CMTP Management): Este puerto está asociado con servicios personalizados o configuraciones específicas, como administración remota o monitoreo. Si el servicio no está adecuadamente asegurado, podría permitir ataques basados en autenticación débil o exposiciones no documentadas.

Impacto: Aunque no se detectan vulnerabilidades críticas, este puerto presenta riesgos potenciales si el servicio en cuestión no está actualizado o tiene configuraciones predeterminadas.

Figura 37
Vulnerabilidades del Servidor Ubuntu 22 Linux para IA



Fuente: Nmap

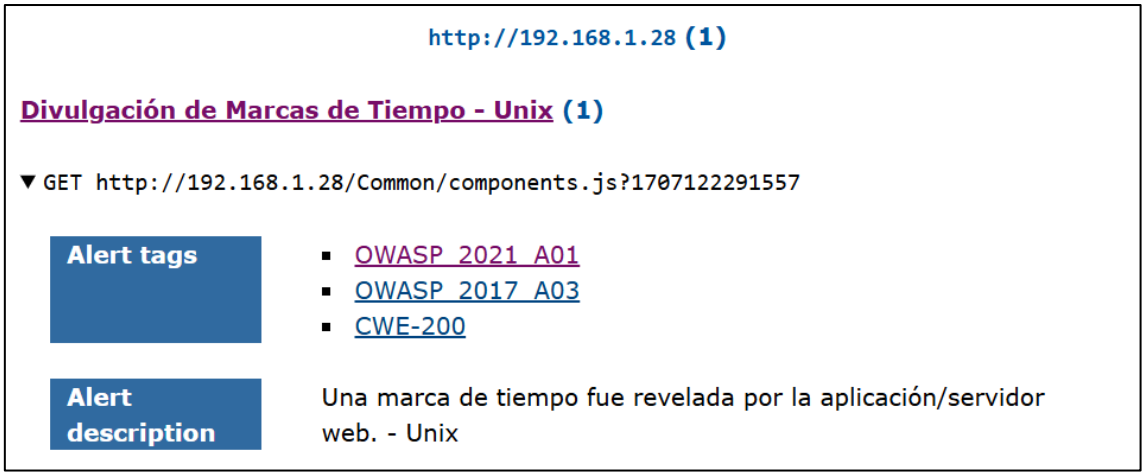
3.3 Vulnerabilidades de riesgo BAJO

3.3.1 Vulnerabilidad de tipo Divulgacion de Tiempo

Explicación: Se detectaron marcas de tiempo Unix en las respuestas, lo que podría revelar información sobre la estructura interna de la aplicación.

Impacto: Los atacantes podrían utilizar esta información para inferir detalles sobre la aplicación y planificar ataques más dirigidos.

Figura 38
Vulnerabilidad de tipo "Divulgación de Marcas de Tiempo"



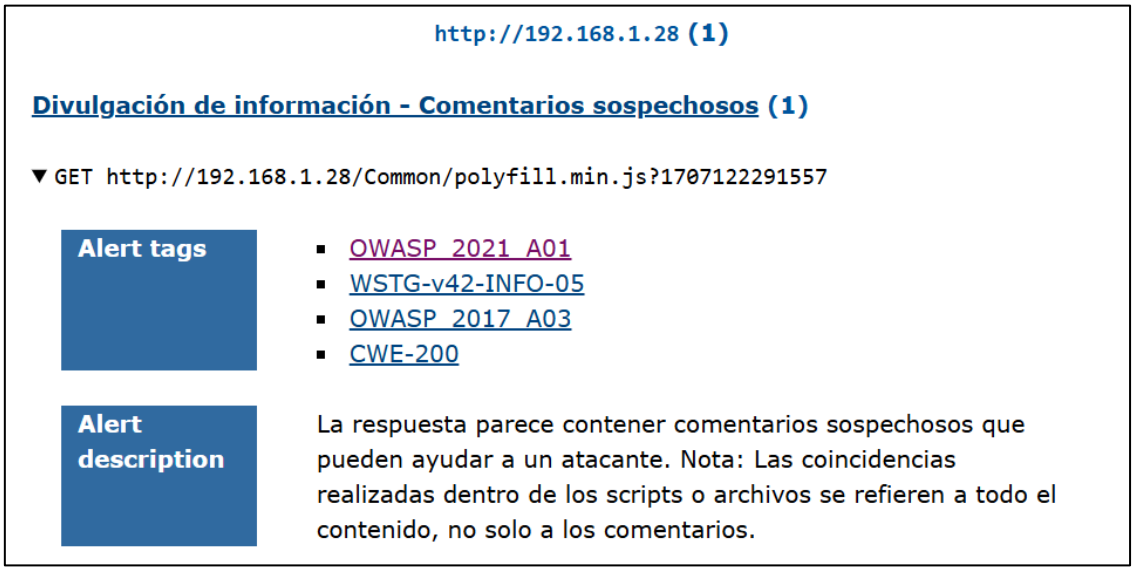
Fuente: OWASP ZAP

3.3.2 Vulnerabilidad de tipo Divulgación de Información

Explicación: Se encontraron comentarios en el código fuente que podrían contener información sensible o pistas sobre la lógica de la aplicación.

Impacto: Los atacantes pueden utilizar esta información para identificar vulnerabilidades o entender mejor la estructura de la aplicación.

Figura 39
Vulnerabilidad de Tipo "Divulgación de Información"



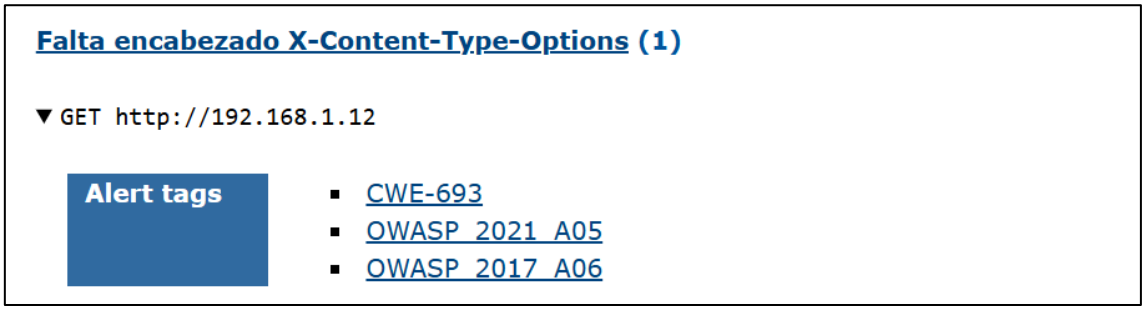
Fuente: OWASP ZAP

3.3.3 Vulnerabilidad de tipo Content-Type-Options

Falta encabezado X-Content-Type-Options: Es una medida de seguridad que indica a los navegadores que no deben interpretar el contenido de una respuesta HTTP de manera diferente al tipo MIME especificado.

Impacto: permite que un atacante engañe al navegador para que ejecute archivos maliciosos, como scripts o archivos de datos maliciosos, incluso si el tipo MIME de la respuesta es seguro.

Figura 40
Vulnerabilidad de tipo X-content-Type-Options



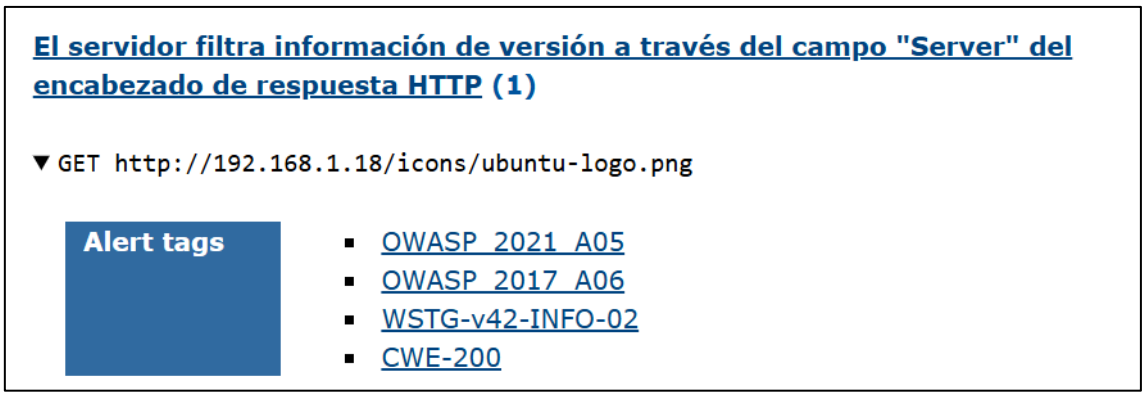
Fuente: OWASP ZAP

3.3.4 Vulnerabilidad de tipo Encabezado de respuesta HTTP

El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP: Revela detalles sobre el servidor web y su versión. Cuando un servidor filtra esta información, está exponiendo detalles que pueden ser aprovechados por un atacante para identificar vulnerabilidades específicas asociadas con esa versión del servidor o software.

Impacto: Exponer la versión del servidor aumenta el riesgo de que un atacante pueda buscar y explotar vulnerabilidades conocidas en esa versión específica.

Figura 41
Filtrado de Información de Version a Traves del Campo Server



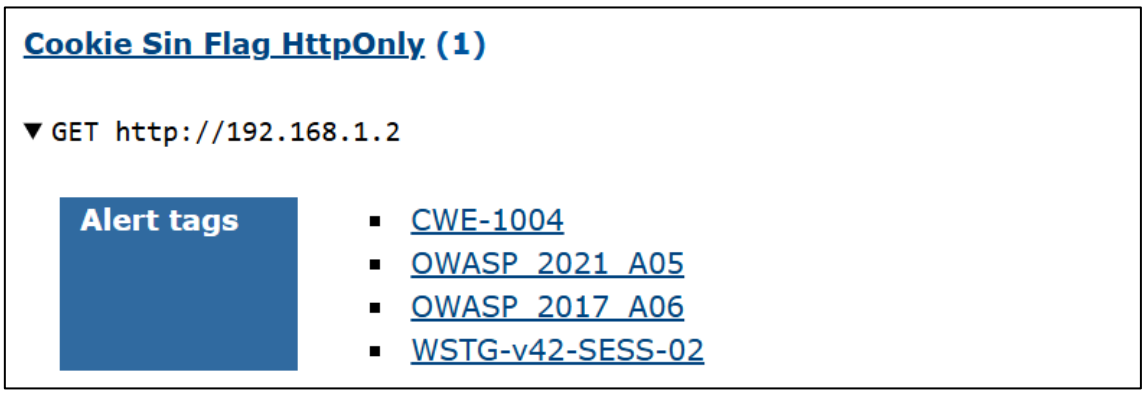
Fuente: OWASP ZAP

3.3.5 Vulnerabilidad de tipo Cookie Sin Flag

Cookie Sin Flag HttpOnly: Una cookie sin el flag `HttpOnly` puede ser accedida mediante scripts del lado del cliente (como JavaScript). Esto es problemático porque las cookies suelen contener información sensible, como tokens de sesión o credenciales.

Impacto: Sin el flag `HttpOnly`, un atacante puede utilizar técnicas como Cross-Site Scripting (XSS) para acceder y robar cookies, comprometiendo sesiones de usuario, información personal y la seguridad general del sistema.

Figura 42
Vulnerabilidad de tipo Cookie Sin Flag HttpOnly



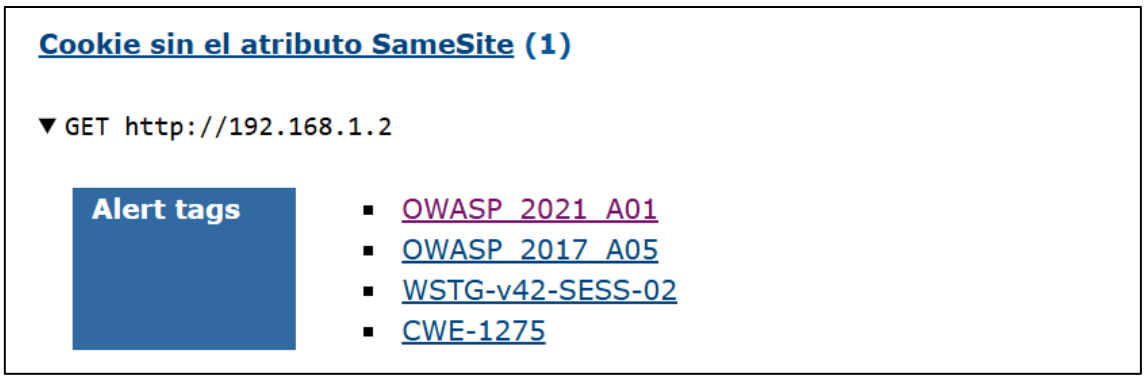
Fuente: OWASP ZAP

3.3.6 Vulnerabilidad de tipo SameSite

Cookie Sin el Atributo SameSite: El atributo `SameSite` en una cookie controla si la cookie puede ser enviada con solicitudes de otros sitios web. Si este atributo no está conigurado, las cookies pueden ser enviadas con solicitudes cross-site.

Impacto: La falta del atributo `SameSite` puede facilitar ataques de Cross-Site Request Forgery (CSRF), en los que un atacante puede realizar acciones no autorizadas en nombre de un usuario autenticado en el sistema. Esto pone en riesgo la integridad y seguridad de la aplicación.

Figura 43
Vulnerabilidad de tipo Cookie Sin el Atributo SameSite



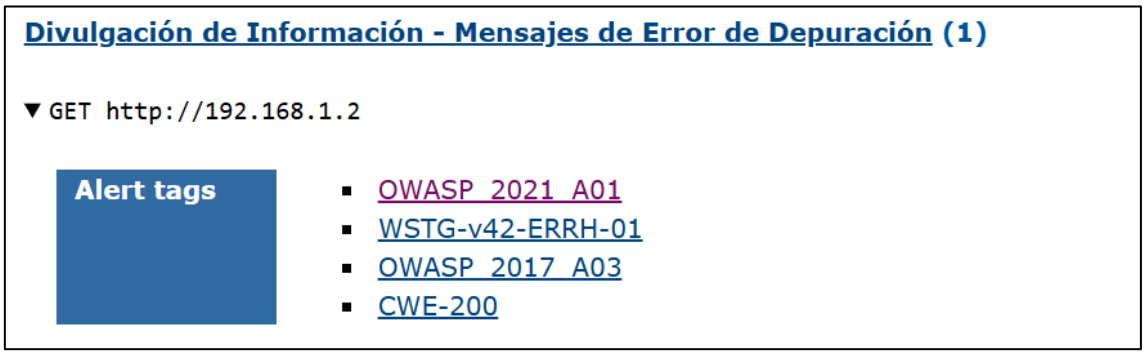
Fuente: OWASP ZAP

3.3.7 Vulnerabilidad de tipo Mensaje de Error de Depuración

Divulgación de Información - Mensajes de Error de Depuración: Los mensajes de error de depuración suelen incluir detalles técnicos sensibles, como nombres de variables, estructuras de base de datos, rutas de archivos o configuraciones del servidor.

Impacto: Los atacantes pueden utilizar esta información para entender la arquitectura de la aplicación y encontrar vulnerabilidades específicas para explotarlas. Esto puede conducir a ataques como inyección SQL, XSS o escalada de privilegios, comprometiendo la seguridad de la aplicación y los datos del sistema.

Figura 44
Vulnerabilidad de tipo Divulgación de Información



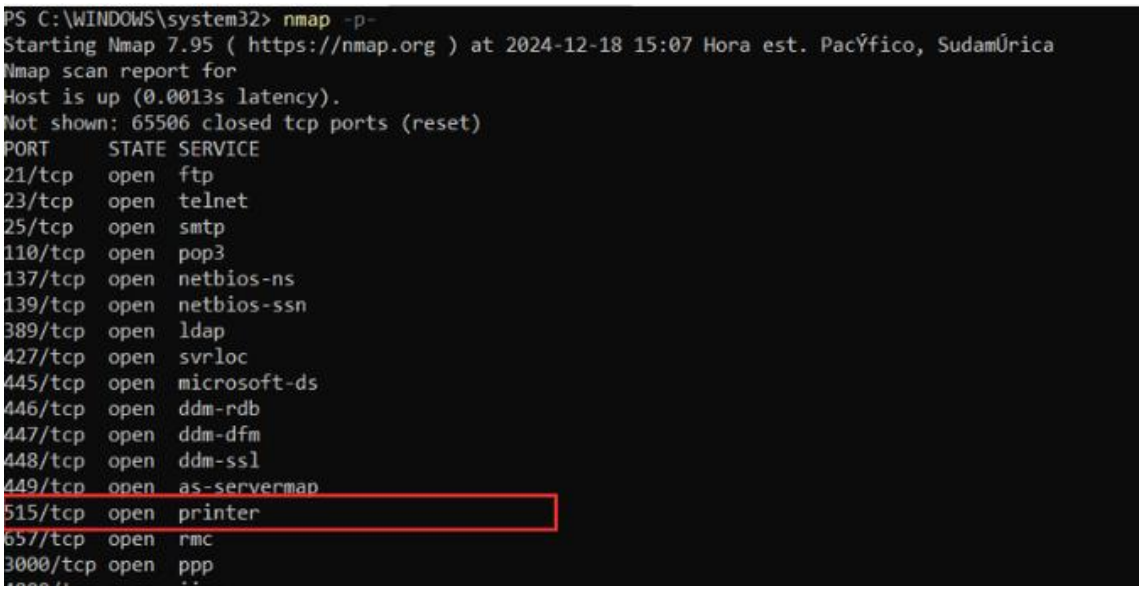
Fuente: OWASP ZAP

3.3.8 Vulnerabilidades en el Servidor RP

Puerto 515 (Printer): El puerto 515 está asociado al servicio de impresión Line Printer DaemoImn (LPD). Este es un protocolo antiguo que no incluye autenticación robusta ni cifrado.

Impacto: Este tipo de servicio generalmente no representa un riesgo significativo porque la explotación directa requiere acceso interno a la red o una configuración muy específica del servicio.

Figura 45
Vulnerabilidades del Servidor RP



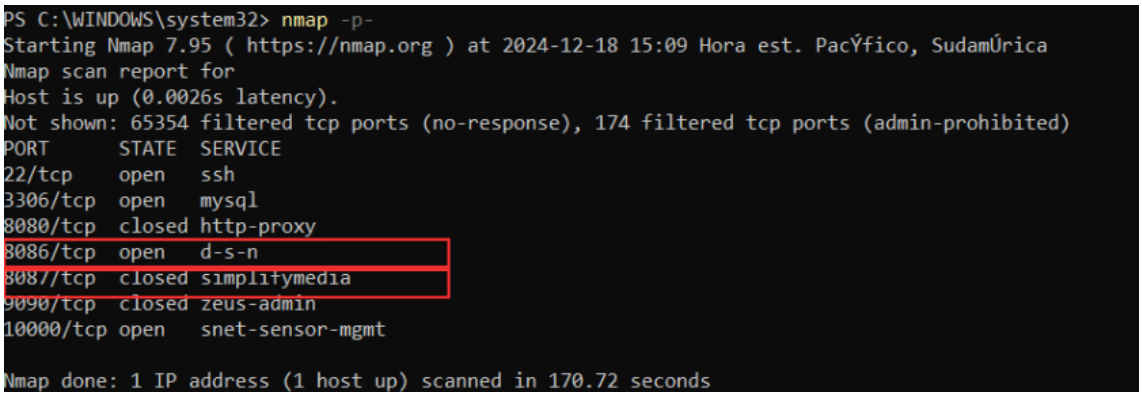
Fuente: Nmap

3.3.9 Vulnerabilidades en el Servidor de Nomina

Puerto 8086 (D-N-S): El puerto 8086 podría estar relacionado con servicios personalizados o aplicaciones de monitoreo/diagnóstico. Este puerto no es ampliamente documentado y puede ser utilizado por software propietario.
Impacto: Posible exposición de información sobre configuraciones o versiones de software.

Puerto 8087 (SimplifyMedia, cerrado): Aunque el puerto está reportado como cerrado, su presencia en el escaneo podría indicar una configuración que lo hace visible a herramientas como Nmap.
Impacto: Un atacante podría aprovechar configuraciones incorrectas del firewall o debilidades en la administración de servicios.

Figura 46
Vulnerabilidades del Servidor de Nomina



Fuente: Nmap

3.3.10 Vulnerabilidades en el Servidor de Base de Datos y Aplicaciones (Backup)

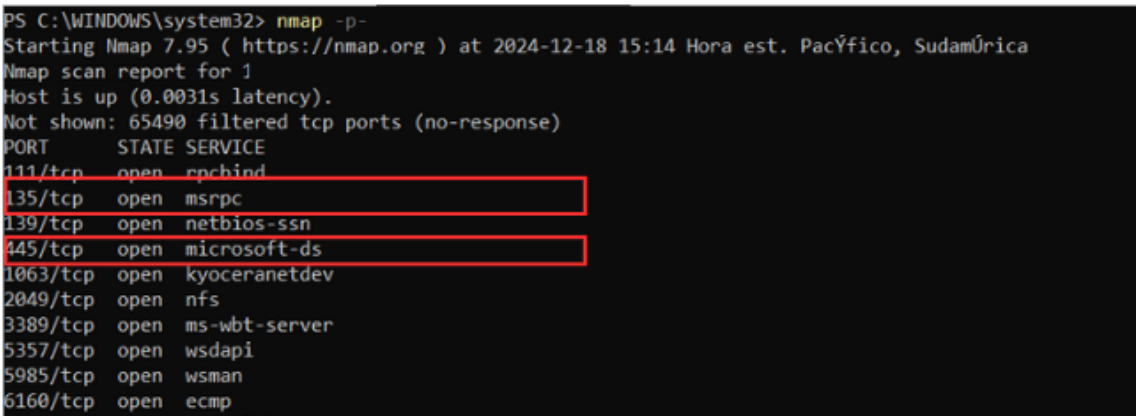
Puerto 135 (MSRPC): Este puerto corresponde al servicio de Microsoft RPC (Remote Procedure Call). Aunque es ampliamente utilizado en sistemas Windows para la comunicación entre procesos, puede ser un vector de enumeración para atacantes.

Impacto: Enumeración de usuarios y servicios en sistemas Windows.

Puerto 445 (Microsoft-DS): Este puerto se utiliza para compartir archivos e impresoras en redes Windows a través de SMB (Server Message Block). Aunque es esencial para muchas funciones de red, puede ser aprovechado para ataques como el ransomware o la propagación de malware.

Impacto: Enumeración de recursos compartidos y credenciales débiles.

Figura 47
Vulnerabilidades en el servidor de Base de Datos y Aplicaciones (Backup)



Fuente: Nmap

3.3.11 Vulnerabilidades del Servidor Virtualizado

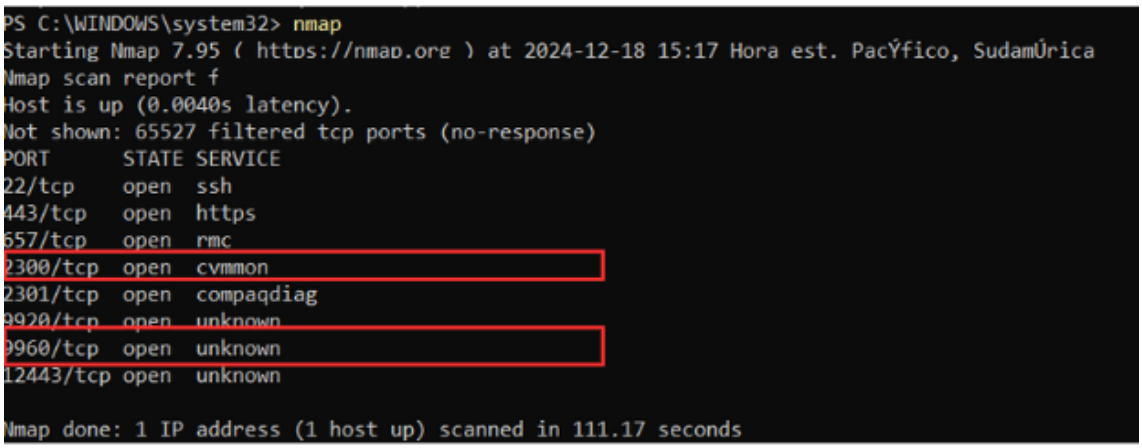
Puerto 2300 (CVMON): Este puerto está asociado con aplicaciones de monitoreo de sistemas, como servicios de administración en servidores Compaq antiguos.

Impacto: Enumeración de servicios o configuraciones del sistema.

Puerto 9960 (Unknown): Este puerto no está asociado a un servicio ampliamente documentado, lo que podría indicar una aplicación personalizada o un servicio no estándar.

Impacto: Posible punto de ataque si el servicio no está configurado correctamente o no tiene parches de seguridad aplicados.

Figura 48
Vulnerabilidades del Servidor Virtualizado



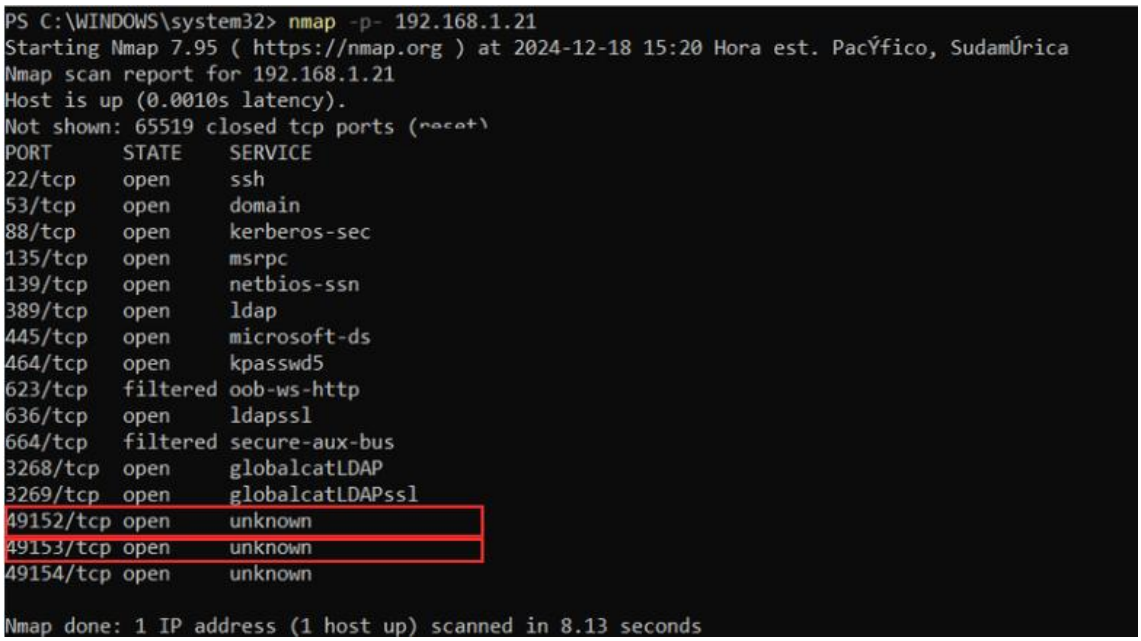
Fuente: Nmap

3.3.12 Vulnerabilidades en el Active Directory

Puerto 49152, 49153 (Unknown): Estos puertos dinámicos son típicamente utilizados por el sistema operativo Windows para comunicación entre servicios.

Impacto: Aunque generalmente son seguros, pueden ser aprovechados si servicios asociados tienen vulnerabilidades no parcheadas.

Figura 49
Vulnerabilidades del Active Directory



Fuente: Nmap

3.3.13 Vulnerabilidades en el Servidor Ubuntu Linux 22

Puerto 8502 (FTNMTP): Este puerto puede estar relacionado con servicios específicos de aplicaciones o configuraciones personalizadas.

Impacto: Si el puerto no está protegido o el servicio tiene configuraciones débiles, podría permitir enumeración o acceso no autorizado.

Puerto 8503 (LSP-Self-Ping): Comúnmente asociado con herramientas internas de aplicaciones para diagnóstico o monitoreo.

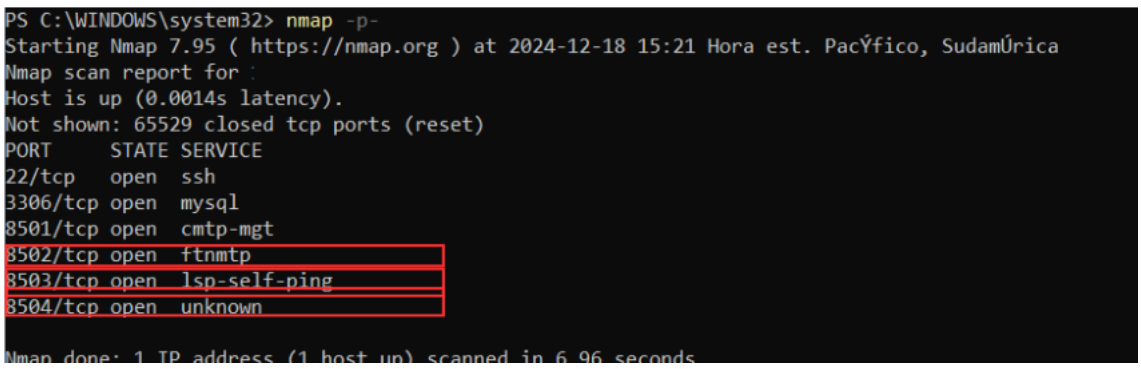
Impacto: Servicios mal configurados podrían ser utilizados por un atacante para recopilar información del sistema o realizar pruebas de conectividad no autorizadas.

Puerto 8504 (Unknown): Este puerto no tiene un servicio estándar asociado, lo que indica que podría ser utilizado por una aplicación personalizada o un servicio no identificado.

Impacto: Un servicio en este puerto podría estar expuesto a ataques si no está actualizado o configurado correctamente.

Figura 50

Vulnerabilidades del Servidor Ubuntu 22 Linux Para Inteligencia Artificial



Fuente: Nmap

4. Reporte

4.1 Reporte de Seguridad - Servidor de Nómina

Para mitigar las vulnerabilidades relacionadas con los servicios y puertos detectados, se recomienda restringir el acceso a los servicios abiertos únicamente a direcciones IP autorizadas mediante reglas de firewall. También es fundamental implementar autenticación robusta, como el uso de claves SSH para el puerto 22 (SSH), y reforzar las configuraciones de bases de datos como MySQL para evitar accesos no autorizados.

Además, es importante deshabilitar servicios innecesarios o cerrarlos si no se utilizan, como los puertos relacionados con aplicaciones que no están activas. Las configuraciones de seguridad deben actualizarse regularmente para asegurar que el software esté protegido contra vulnerabilidades conocidas.

Estas acciones garantizarán un entorno más seguro para los datos sensibles manejados en el servidor de nómina y minimizarán los riesgos de accesos no autorizados o ataques cibernéticos.

4.2 Reporte de Seguridad - Servidor RP

Para mitigar las vulnerabilidades identificadas en el servidor, se recomienda implementar controles generales que fortalezcan la seguridad del sistema. Es esencial configurar encabezados de seguridad, como la política de seguridad de contenido (CSP) para controlar los recursos permitidos en el sitio, proteger contra ataques de clickjacking mediante el encabezado X-Frame-Options y prevenir la interpretación incorrecta de archivos con el encabezado X-Content-Type-Options: nosniff.

Además, se sugiere revisar las configuraciones del servidor web para garantizar que cumplan con las mejores prácticas de seguridad. Esto incluye actualizar constantemente el software, limitar la exposición pública de los servicios a través de firewalls, y aplicar configuraciones que minimicen los riesgos asociados con la divulgación de información innecesaria.

Estas medidas no solo mejorarán la resiliencia del servidor frente a ataques, sino que también garantizarán un entorno más seguro para los usuarios y los datos que se manejan.

4.2.1 Reporte de Seguridad por Nmap - Servidor RP

Para mitigar las posibles vulnerabilidades identificadas en este servidor, es fundamental deshabilitar o restringir los servicios innecesarios, tales como FTP, Telnet, NetBIOS, y otros servicios no utilizados o configurados incorrectamente. Estos servicios suelen ser vectores comunes de ataques si no están adecuadamente protegidos.

Adicionalmente, para los servicios que deben permanecer habilitados, como LDAP, SMTP, o Microsoft-DS, se recomienda implementar controles de acceso estrictos mediante listas de control de acceso (ACLs) y configuraciones específicas de firewall que permitan conexiones solo desde IP autorizadas. Es imprescindible usar protocolos seguros como SFTP en lugar de FTP y deshabilitar Telnet, que no cifra la información transmitida.

Se debe reforzar la seguridad de los servicios que manejan autenticación o datos críticos configurando políticas de contraseñas robustas y habilitando cifrado siempre que sea posible. Finalmente, monitorear constantemente las actividades de red en estos puertos abiertos ayudará a detectar accesos sospechosos y responder a tiempo a posibles incidentes.

4.3 Reporte de Seguridad - Servidor de Base de Datos y Aplicaciones (Backup)

Para mitigar las vulnerabilidades del servidor de base de datos y aplicaciones (Backup), se recomienda deshabilitar todos los servicios y puertos que no sean esenciales para el funcionamiento del sistema, restringiendo el acceso a puertos como rpcbind, msrpc, y netbios-ssn. Implementar reglas de firewall que permitan únicamente conexiones desde IP autorizadas a los servicios críticos, como ms-wbt-server (RDP) y wsman. Asegurar la configuración de autenticación fuerte y cifrado en los servicios habilitados para prevenir accesos no autorizados. Finalmente, se deben realizar auditorías periódicas de seguridad para identificar y cerrar posibles brechas.

4.4 Reporte de Seguridad – Servidor Virtualizado

Para mitigar las vulnerabilidades del servidor virtualizado, se debe cerrar o restringir el acceso a puertos no esenciales como cvmmon, compaqdiag, y otros puertos desconocidos. Es fundamental asegurar que el puerto SSH (22/tcp) esté protegido con autenticación fuerte y que el acceso HTTPS (443/tcp) esté configurado con un certificado válido y protocolos de seguridad robustos. Además, se deben aplicar políticas de firewall para restringir el acceso a estos puertos solo a IPs y redes autorizadas, asegurando que se mantenga un monitoreo constante y una revisión periódica de las configuraciones de seguridad.

4.5 Reporte de Seguridad – Servidor de Archivos

Para mitigar las vulnerabilidades identificadas en el servidor de archivos, es crucial tomar varias acciones. La exposición de metadatos en la nube debe ser corregida, restringiendo el acceso no autorizado a información sensible a través de los servicios web. La configuración de una cabecera Content Security Policy (CSP) debe ser implementada adecuadamente para prevenir ataques de inyección de código y otros riesgos relacionados con el contenido no seguro. Además, la falta de cabecera Anti-Clickjacking debe resolverse configurando correctamente la cabecera X-Frame-Options para evitar la posibilidad de que los usuarios sean engañados al hacer clic en contenido malicioso. Es esencial también añadir el encabezado X-Content-Type-Options para evitar problemas de detección incorrecta del tipo de contenido que puede exponer a la aplicación a vulnerabilidades. Finalmente, aunque la alerta sobre una "Aplicación Web Moderna" es informativa, es importante evaluar las mejores prácticas actuales para garantizar que la aplicación esté alineada con las tecnologías y métodos más seguros.

4.6 Reporte de Seguridad – Servidor DNS

Para mitigar las vulnerabilidades detectadas en el servidor DNS, se debe implementar de inmediato una política de Content Security Policy (CSP) para controlar qué recursos pueden cargarse en la aplicación, protegiendo contra ataques de inyección de código como XSS. También es crucial configurar la cabecera X-Frame-Options para evitar ataques de clickjacking, lo que impide que el contenido sea incrustado en otros marcos de páginas maliciosas. Además, se debe ajustar la configuración del servidor para ocultar la información de versión en las respuestas HTTP, lo que evitará que atacantes exploten

vulnerabilidades conocidas asociadas a versiones específicas de software. Estas acciones son esenciales para fortalecer la seguridad del servidor DNS.

4.7 Reporte de Seguridad – Active Directory

Para mitigar las vulnerabilidades detectadas en el servidor Active Directory, se deben tomar acciones inmediatas. Primero, se debe implementar una política de Content Security Policy (CSP) para restringir qué recursos pueden ser cargados, previniendo ataques de inyección de código. También es esencial configurar el encabezado X-Frame-Options para prevenir ataques de clickjacking, protegiendo la aplicación contra el uso indebido de marcos en páginas maliciosas. Asimismo, es necesario ajustar la configuración del servidor para ocultar la información de versión en las respuestas HTTP, lo que evita que atacantes aprovechen posibles vulnerabilidades en versiones específicas del software. Finalmente, se debe asegurar que el encabezado X-Content-Type-Options esté configurado correctamente para evitar ataques de tipo sniffing de contenido. Estas acciones son fundamentales para proteger la seguridad del servidor Active Directory.

4.7.1 Reporte de Seguridad con Nmap – Active Directory

El escaneo realizado con Nmap ha identificado varios puertos abiertos en el servidor Active Directory que requieren atención para mitigar posibles riesgos de seguridad. Se deben tomar las siguientes acciones: primero, asegurar el puerto 22 (SSH) configurando autenticación con claves SSH y restringir el acceso solo a direcciones IP confiables. Para el puerto 53 (DNS), se debe garantizar que las consultas recursivas estén limitadas a fuentes autorizadas. En el caso del puerto 88 (Kerberos), es fundamental verificar la correcta configuración del sistema de autenticación Kerberos y establecer políticas de seguridad para evitar falsificación de TGT. Los puertos 135 (MSRPC), 139 y 445 (NetBIOS y SMB) deben ser restringidos a la red interna, con especial atención al deshabilitar SMBv1 y aplicar parches de seguridad. Para los puertos 389 y 636 (LDAP y LDAPS), se debe asegurar el tráfico utilizando TLS/SSL y restringir el acceso solo a servidores necesarios. Además, el puerto 464 (Kpasswd5) debe estar protegido mediante autenticación robusta. Los puertos 623, 664, 3268, y 3269 deben ser revisados para minimizar su exposición y, si no son esenciales, bloquear su acceso. Finalmente, los puertos 49152-49154, utilizados por servicios temporales, deben ser analizados y

restringidos si no son necesarios. En resumen, se recomienda aplicar medidas de seguridad como firewalls, políticas de acceso restringido, cifrado y monitoreo constante, además de mantener los sistemas actualizados con los últimos parches para prevenir vulnerabilidades.

4.8 Reporte de Seguridad – Servidor Replicado (EXSI)

El análisis de seguridad con ZAP reveló varias vulnerabilidades críticas en el servidor replicado. Se identificaron problemas con las configuraciones de CSP, permitiendo scripts y estilos no verificados, lo que puede generar ataques XSS. Además, se encontró un archivo oculto (.hg) que podría exponer información sensible, y se detectó un intento de explotación a través de la manipulación del agente de usuario. También se observó la divulgación de información en comentarios sospechosos y configuraciones incorrectas de control de caché. Se recomienda corregir estas configuraciones, eliminar archivos innecesarios y reforzar las políticas de seguridad para mitigar los riesgos.

4.9 Reporte de Seguridad – Servidor de Cámaras

El análisis de seguridad con ZAP en el servidor de cámaras identificó varias vulnerabilidades. Se detectó la ausencia de la cabecera Content Security Policy (CSP), lo que podría permitir ataques de inyección de contenido. Además, se observó la falta de la cabecera X-Content-Type-Options, lo que expone a riesgos de ejecución no deseada de contenido. La divulgación de marcas de tiempo Unix también fue señalada, lo que podría ayudar a un atacante a obtener información adicional del sistema. Además, se encontró una librería JavaScript vulnerable y un problema de fuzzing del agente de usuario que podría facilitar ataques de fuerza bruta. Se recomienda aplicar una política CSP, incluir la cabecera X-Content-Type-Options, eliminar información sensible y actualizar las librerías vulnerables.

4.10 Reporte de Seguridad – Servidor Linux

El escaneo con Nmap en el servidor Ubuntu Linux (192.168.1.30) reveló que varios puertos están abiertos. El puerto 22 (SSH) está disponible, lo que permite acceso remoto, mientras que el puerto 3306 (MySQL) podría exponer la base de datos a accesos no autorizados si no está adecuadamente protegido. También se encuentran abiertos los puertos 8501 (cmtp-mgt), 8502 (ftnmpt), 8503 (lsp-self-ping) y 8504 (desconocido), lo

que podría ser indicativo de servicios que requieren revisión de seguridad. Se recomienda asegurar el acceso a estos puertos, especialmente SSH y MySQL, mediante autenticación adecuada, firewalls y auditorías de los servicios expuestos en los puertos no reconocidos.

4.11 Reporte de Seguridad – Servidor de Aplicaciones Principal

El escaneo realizado con ZAP en el servidor de aplicaciones ha identificado varias vulnerabilidades que deben ser corregidas para mejorar la seguridad del sistema. En primer lugar, la falta de la cabecera Content Security Policy (CSP) representa un riesgo medio, ya que no se protege adecuadamente contra ataques como Cross-Site Scripting (XSS), por lo que es esencial configurarla. Además, la ausencia de la cabecera Anti-Clickjacking, también con riesgo medio, expone al sistema a ataques de clickjacking, lo que requiere su implementación inmediata. Se encontraron cookies sin los atributos HttpOnly y SameSite, lo cual es un riesgo bajo, pero debe corregirse para proteger las cookies contra ataques de JavaScript. Además, la divulgación de mensajes de error de depuración y la exposición de información de versión del servidor en los encabezados HTTP son vulnerabilidades de bajo riesgo, pero se deben resolver deshabilitando la depuración y ocultando la versión del servidor. Finalmente, la falta del encabezado X-Content-Type-Options y la presencia de comentarios sospechosos en el código son detalles menores, pero deben ser abordados para evitar posibles filtraciones de información y mejorar la seguridad general del servidor.

CONCLUSIONES

1. El análisis de vulnerabilidades en los sistemas web de IANCEM permitió identificar debilidades clave en la configuración de seguridad, como la falta de cabeceras de protección y la exposición de metadatos sensibles. Estas vulnerabilidades, aunque no críticas, podrían ser aprovechadas por atacantes si no se abordan adecuadamente, lo que resalta la importancia de realizar auditorías de seguridad periódicas.

2. Durante el proceso de escaneo, herramientas como Nmap y OWASP ZAP fueron esenciales para identificar puertos abiertos y servicios activos vulnerables, así como configuraciones incorrectas en las aplicaciones. Estos escaneos ayudaron a establecer un mapa claro de las posibles vías de ataque que requerían intervención.

3. La ausencia de cabeceras de seguridad clave como Content Security Policy (CSP) y X-Frame-Options expuso a las aplicaciones web a riesgos de inyección de código y ataques de Clickjacking. La implementación de estas cabeceras de seguridad es una medida técnica fundamental para mitigar estos riesgos y proteger la integridad de las aplicaciones contra manipulaciones maliciosas.

4. La correcta configuración de cabeceras de seguridad y la validación de entradas son aspectos fundamentales en el desarrollo seguro. Se concluye que integrar estas prácticas en todas las fases del ciclo de vida del software es clave para reducir los riesgos de vulnerabilidades, evitando que ataques como XSS e inyecciones puedan comprometer los sistemas.

5. A través de la implementación de las soluciones recomendadas y la postura de seguridad de la organización mejoró sustancialmente. La remediación de vulnerabilidades, como la filtración de metadatos y la configuración de cabeceras de

seguridad, fortalecerá la defensa ante posibles ataques, protegiendo tanto la integridad de los datos como la confianza en los servicios proporcionados.

En resumen, Aunque los sistemas del Ingenio están resguardados por una intranet, las vulnerabilidades identificadas evidencian la necesidad de implementar medidas de seguridad adicionales. Abordar tanto las vulnerabilidades de alto, medio o bajo riesgo es crucial para mantener la integridad y seguridad de los sistemas internos.

RECOMENDACIONES

1. Configurar encabezados HTTP adicionales para reforzar la seguridad**,** además de la cabecera CSP, implementar encabezados como `X-Content-Type-Options` con el valor `nosniff` y `Strict-Transport-Security (HSTS)` para garantizar que todas las comunicaciones se realicen de manera segura y evitar la manipulación de tipos de contenido en las respuestas del servidor.

2. Establecer una política de control de acceso basada en roles (RBAC) en el cual se pueda implementar un esquema de acceso granular en las aplicaciones y sistemas internos, garantizando que los usuarios solo puedan acceder a los datos y funcionalidades que correspondan a su nivel de autorización, reduciendo riesgos derivados de accesos no autorizados.

3. Implementar herramientas de análisis estático y dinámico de código (SAST y DAST), además integrar estas herramientas en el proceso de desarrollo para identificar vulnerabilidades de seguridad en el código fuente antes de la implementación y detectar comportamientos anómalos en las aplicaciones durante su ejecución.

4. Proteger contra la exposición de metadatos sensibles para evitar la exposición de información no necesaria en las respuestas HTTP, como detalles sobre la versión del servidor o directorios accesibles.

5. Desplegar sistemas de monitoreo en tiempo real que incluyan la detección de tráfico anómalo, el análisis de logs y la identificación de patrones de ataque. Esto permitirá responder de manera inmediata a incidentes y mejorar la detección temprana de posibles amenazas.

En resumen, La implementación de estas recomendaciones contribuirá significativamente a mejorar la seguridad de la intranet de IANCEM, protegiendo los activos de información y garantizando la continuidad operativa de la organización teniendo el menor riesgo de que si se produce un ataque se pueda acceder a la manipulación de los datos que se manejan dentro de la empresa.

BIBLIOGRAFIA

Ingenio Azucarero del Norte Compania de Economia Mixta Iance Perfil de Compañía - Ecuador | Finanzas y ejecutivos clave | EMIS. (s. f.). https://www.emis.com/php/company-profile/EC/Ingenio_Azucarero_del_Norte_Compania_de_Economia_Mixta_Iancem_es_3565640.html#:~:text=El%20Ingenio%20Azucarero%20del%20Norte,LILLE%20CAIL%20y%20Granda%20Centeno.

Arsys. (2024, 16 octubre). OWASP: ¿Qué es y cómo usar esta metodología? https://www.arsys.es/blog/owasp

Yacelga, J. (s. f.). ANÁLISIS DE VULNERABILIDADES EN SERVIDORES DE APLICACIONES EMPRESARIALES MEDIANTE TÉCNICAS DE PENTESTING UTILIZANDO LA METODOLOGÍA OWASP Y PTES: ESTUDIO DE CASO EMPRESA CUBOSOFT. https://repositorio.utn.edu.ec/bitstream/123456789/16080/2/PG%201844%20TRABAJO%20GRADO.pdf

Muñoz, A., Pérez, S., & Amador, S. (s. f.). Pentesting sobre aplicaciones web basado en la metodología OWASP utilizando un cluster conformado por dispositivos SBC de bajo costo. https://www.proquest.com/docview/2194005434/fulltextPDF/F24B3BEE0E564E3BPQ/1?accountid=13357

Creative Commons. (2017). OWASP Top 10 - 2017 Los diez riesgos más críticos en Aplicaciones Web. https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

INCIBE. (2024, 8 agosto). La ciberseguridad en el sector agroalimentario. https://www.incibe.es/incibe-cert/blog/la-ciberseguridad-en-el-sector-agroalimentario

TOTVS LATAM. (2024, 29 mayo). ¿Qué es la agroindustria? TOTVS. https://es.totvs.com/blog/cat-agroindustria/que-es-la-agroindustria-aprende-todo-sobre-este-sector/

Santos, J. (2024, 21 octubre). principales amenazas de ciberseguridad para empresas y cómo prevenirlas. Deltaprotect. https://www.deltaprotect.com/blog/amenazas-de-ciberseguridad

OWASP. (2024, septiembre). Los diez mejores de OWASP. https://owasp.org/www-project-top-ten/

Bortnik, S. (2024). Pruebas de penetración para principiantes: 5 herramientas para empezar. .Seguridad. https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Jackson, P. (2024, 13 octubre). How To Create A Vulnerability Assessment Report. WebSecInsights. https://www.websecinsights.com/vulnerability-assessment/create-vulnerability-assessment-report/

Machaca, A. (2024). ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP [Diapositivas]. https://wiki.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

Comunnity Latam. (2023, 17 noviembre). OWASP ZAP: Herramienta de seguridad de aplicaciones web. Listopro. https://community.listopro.com/owasp-zap-herramienta-de-seguridad-de-aplicaciones-web/

Beschokov, M. (2024, 10 junio). OWASP ZAP – Proxy de ataque Zed. Wallarm. https://lab.wallarm.com/what/owasp-zap-proxy-de-ataque-zed/?lang=es#:~:text=OWASP%20ZAP%20es%20una%20soluci%C3%B3n,de%20sus%20plataformas%20en%20l%C3%ADnea.

Hernández, M. (2024, 12 noviembre). Escaneo de vulnerabilidades automático con OWASP ZAP. https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-autom%C3%A1tico-OWASP-ZAP

Araujo, A. (2024, 5 diciembre). CVSS: Guía para interpretar los puntajes de vulnerabilidad y su impacto. Hackmetrix. https://blog.hackmetrix.com/puntajes-de-vulnerabilidad-cvss/

Shivanandhan, M. (2023, 23 abril). Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos. freeCodeCamp. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

Eliseo, M. (2024, 31 octubre). *¿Qué es la seguridad informática y cómo implementarla?* Cibernos Grupo. https://www.grupocibernos.com/blog/que-es-la-seguridad-informatica-y-como-implementarla

Aguilar, M. A. (2024, 16 octubre). *Seguridad informática: qué es, tipos, posibles amenazas y consejos*. Delta Protect. https://www.deltaprotect.com/blog/seguridad-informatica-que-es

Lindemulder, G., & Kosinski, M. (2024, 12 agosto). *¿Qué es la ciberseguridad?* IBM. https://www.ibm.com/es-es/topics/cybersecurity

ANEXO

Ingenio
Azucarero
del Norte

CARTA DE ACEPTACION

Por medio de la presente, la empresa *Ingenio Azucarero del Norte Compañía de Economía Mixta* **IANCEM**, con número de RUC **1090075744001**, tiene el agrado de informar que el señor **Diego Fernando Guerra Olmedo**, portador de la cédula de ciudadanía **Nº 1004172746**, ha realizado la entrega del informe técnico titulado:

"Implementación de la Metodología OWASP para la Detección de Vulnerabilidades en los Sistemas Informáticos de IANCEM".

Este proyecto fue desarrollado con el objetivo de fortalecer la seguridad de los sistemas informáticos de la empresa, contribuyendo significativamente a la protección de la información y la infraestructura tecnológica de IANCEM.

Nos complace informar que el proyecto ha sido concluido con un alto grado de satisfacción, cumpliendo con todos los requisitos establecidos y demostrando el compromiso, capacidad y profesionalismo del señor **Diego Fernando Guerra Olmedo** en su ejecución.

Agradecemos su valiosa contribución y le extendemos nuestro reconocimiento por su excelente desempeño.

CARLOS ARMANDO PERALTA SEGARRA

Firmado digitalmente por CARLOS ARMANDO PERALTA SEGARRA
Fecha: 2025.01.28 11:37:14 -05'00'

Atentamente,

Ing. Carlos Peralta | Jefe de Sistemas

Ingenio Azucarero del Norte
Panamericana Norte km 25 vía Tulcán, Ibarra, Imbabura, Ecuador
(+593) 6 299 8100 Ext. 110
jefesistemas@tababuela.com | www.tababuela.com

Ingenio
Azucarero
del Norte

www.tababuela.com
Panamericana Norte Km. 25 Vía Tulcán
Conmutador: (06) 2998 100
administracion@tababuela.com
Ibarra - Ecuador

PUCE
IBARRA

INFORME TECNICO

2025

"Implementación de la Metodología OWASP para la Detección de Vulnerabilidades en los Sistemas Informáticos de IANCEM"

Autor: Diego Fernando Guerra Olmedo

Fecha: 20/01/2025

INDICE DE CONTENIDOS

Resumen Ejecutivo

El presente informe detalla el análisis de vulnerabilidades realizado en los sistemas informáticos de "IANCEM", enfocado en garantizar la seguridad y protección de la información sensible manejada por la organización. Este análisis se llevó a cabo aplicando la metodología OWASP, ampliamente reconocida en el ámbito de la ciberseguridad, y utilizando herramientas especializadas como OWASP ZAP y Nmap para la identificación de riesgos y configuraciones incorrectas.

Durante el proceso, se evaluaron las configuraciones de seguridad de las aplicaciones web y la infraestructura de red, identificando vulnerabilidades de alta, media y baja severidad. Entre los hallazgos destacados se incluyen la ausencia de cabeceras de seguridad críticas como Content Security Policy (CSP) y Anti-Clickjacking, además de configuraciones que podrían facilitar ataques como la inyección de código o la ejecución de scripts maliciosos. También se detectaron filtraciones de metadatos en la nube, clasificadas como de alto riesgo, que exponen a la organización a posibles compromisos de información.

Las vulnerabilidades encontradas, si bien en su mayoría no representan un peligro crítico inmediato, incrementan la superficie de ataque de la organización y podrían ser explotadas por actores malintencionados para comprometer la confidencialidad, integridad y disponibilidad de la información.

Como parte del análisis, se elaboraron recomendaciones específicas para mitigar los riesgos identificados. Estas incluyen la implementación de cabeceras de seguridad, el refuerzo de políticas de acceso, la capacitación en ciberseguridad del personal y la realización de auditorías de seguridad periódicas.

Este informe proporciona una visión integral de la postura de seguridad actual de los sistemas web de IANCEM y establece un conjunto de medidas prácticas para fortalecer la protección de la información y los activos digitales de la organización.

Introducción

La seguridad de los sistemas web es fundamental para garantizar la protección de la información y los procesos operativos de las organizaciones. En este contexto, el presente informe técnico tiene como objetivo identificar y mitigar los riesgos de seguridad en los sistemas web de IANCEM, con el fin de fortalecer su postura frente a posibles ciberataques y garantizar la integridad, confidencialidad y disponibilidad de su información.

Alcance del Trabajo

El análisis se centró en los sistemas web de IANCEM, evaluando tanto la infraestructura de red como las configuraciones específicas de seguridad de las aplicaciones web críticas. El período de evaluación abarcó desde el 30 de octubre de 2024 hasta el 18 de diciembre de 2024.

Para llevar a cabo este análisis, se utilizaron herramientas especializadas como:

- **OWASP ZAP**, para detectar vulnerabilidades específicas en las aplicaciones web, como configuraciones incorrectas y la ausencia de cabeceras de seguridad.
- **Nmap**, para mapear los puertos y servicios activos en la red, lo que permitió identificar posibles vectores de ataque en la infraestructura interna.

Metodología Aplicada

La metodología utilizada para este análisis fue el estándar OWASP, un marco ampliamente reconocido en el ámbito de la seguridad web. Este marco abarca una serie de pruebas diseñadas para evaluar las aplicaciones web en busca de vulnerabilidades comunes, clasificadas según su severidad y el impacto potencial en la organización.

Entre las pruebas realizadas se incluyeron:

- Evaluación de configuraciones de cabeceras de seguridad, como Content Security Policy (CSP) y Anti-Clickjacking.
- Validación de la exposición de servicios en la red interna.

Vulnerabilidad	Severidad	Impacto	Solución
		capturar credenciales o datos sensibles en la red.	conexiones seguras.
389/tcp	Alto	La falta de cifrado puede exponer credenciales e información sensible del directorio.	Usar LDAPS (LDAP sobre SSL/TLS) para proteger las conexiones. Configurar ACLs para limitar accesos y privilegios.
445/tcp	Alto	Frecuentemente explotado en ataques como EternalBlue para comprometer sistemas mediante SMB.	Aplicar actualizaciones de seguridad, deshabilitar SMBv1 y habilitar SMBv2/3 con cifrado.
25/tcp	Medio	Puede ser utilizado para enviar correos no autorizados (SPAM) o facilitar ataques de phishing.	Configurar autenticación en SMTP, habilitar TLS y monitorear el tráfico de correo para detectar abuso.
110/tcp	Medio	Las credenciales y correos electrónicos pueden ser interceptados si no se usa cifrado.	Implementar POP3 con TLS (POP3S) o migrar a protocolos más seguros como IMAP con cifrado.
137/tcp	Medio	Puede filtrar información sobre la red, como nombres de equipo y servicios disponibles.	Deshabilitar NetBIOS si no es necesario o restringir accesos mediante firewall.
139/tcp	Medio	Puede ser explotado para ataques de enumeración o	Deshabilitar NetBIOS sobre TCP/IP en configuraciones modernas. Usar

Vulnerabilidad	Severidad	Impacto	Solución
		propagación de malware.	cortafuegos para limitar accesos.
515/tcp	Medio	Puede ser utilizado para explotar servicios de impresión y obtener acceso al sistema.	Restringir accesos al servicio de impresión mediante firewall y deshabilitar en caso de no ser necesario.
3000/tcp	Medio	Podría estar asociado a servicios de desarrollo o pruebas, exponiendo información sensible.	Deshabilitar servicios de desarrollo en entornos de producción y proteger con autenticación y cifrado si es necesario.
8470-8479/tcp	Medio	Podría estar relacionado con servicios de red, y si no están configurados correctamente, pueden ser explotados por atacantes.	Identificar el uso de estos puertos, verificar configuraciones y deshabilitar aquellos que no sean necesarios.
427/tcp	Bajo	Puede divulgar información sobre servicios en la red, facilitando la enumeración para posibles ataques.	Monitorear y limitar el acceso a este puerto mediante reglas de firewall.
446/tcp	Bajo	Puede ser un servicio poco usado o redundante, lo que aumenta la superficie de ataque sin beneficio.	Identificar el uso del servicio y, si no es necesario, cerrarlo mediante configuraciones del servidor o firewall.
447/tcp	Bajo	Podría ser aprovechado por atacantes si no se	Restringir accesos innecesarios y monitorear las