InnovaSciT
Revista Multidisciplinar
ISSN 3091-1826

Innovación Ciencia y Tecnología /enero –junio 2025/ Vol. 3, - No. 1
Doi: 10.70577/innovascit.v3i1.40

Vulnerabilidades en aplicaciones Web: Un Enfoque Integral

Vulnerabilities in Web Applications: A Comprehensive Approach

RESUMEN

Las aplicaciones web son un componente esencial en la infraestructura digital, pero su vulnerabilidad ante ataques cibernéticos sigue siendo una de las mayores preocupaciones en seguridad informática. Este estudio realiza un análisis integral sobre las principales vulnerabilidades en aplicaciones web, basándose en marcos normativos como OWASP Top 10 y MITRE CWE, junto con las técnicas más avanzadas de pentesting utilizadas para su detección y mitigación. Mediante una revisión sistemática de literatura y análisis de herramientas de seguridad, se identificaron las vulnerabilidades más críticas, incluyendo inyecciones de código, ataques de fuerza bruta, scripting entre sitios (XSS) y falsificación de solicitudes del lado del servidor (SSRF). Se compararon metodologías tradicionales con enfoques basados en inteligencia artificial para la detección y prevención de estos ataques. Los resultados evidencian que las técnicas de pentesting combinadas con modelos de aprendizaje automático mejoran significativamente la capacidad de detección temprana de vulnerabilidades. Además, se destaca la necesidad de integrar escáneres de seguridad automatizados en el desarrollo seguro de software para minimizar riesgos. Los hallazgos de esta investigación proporcionan una visión actualizada sobre los desafíos y soluciones en seguridad de aplicaciones web, contribuyendo al desarrollo de estrategias de protección más efectivas en entornos digitales.

PALABRAS CLAVE: Vulnerabilidades web, OWASP Top 10, MITRE CWE, seguridad ofensiva, pentesting.

ABSTRACT

Web applications are an essential component of digital infrastructure, but their vulnerability to cyberattacks remains one of the biggest concerns in information security. This study conducts a comprehensive analysis of the main vulnerabilities in web applications, based on regulatory frameworks such as the OWASP Top 10 and MITRE CWE, along with the most advanced pentesting techniques used for their detection and mitigation. Through a systematic literature review and analysis of security tools, the most critical vulnerabilities were identified, including code injection, brute force attacks, cross-site scripting (XSS), and server-side request forgery (SSRF). Traditional methodologies were compared with artificial intelligence-based approaches for the detection and prevention of these attacks. The results show that pentesting techniques combined with machine learning models significantly enhance early vulnerability detection capabilities. Additionally, the need to integrate automated security scanners into secure software development is emphasized to minimize risks. The findings of this research provide an updated perspective on the challenges and solutions in web application security, contributing to the development of more effective protection strategies in digital environments.

KEYWORDS: *Web vulnerabilities, OWASP Top 10, MITRE CWE, offensive security, pentesting.*

INNOVACIÓN Y CONOCIMIENTO

Recepción: *19/03/2025*
Aceptación: *27/03/2025*
Publicación: *30/06/2025*

AUTOR/ES

Solano Gutiérrez Gerardo Alfredo

Pico Molina Ronald Fernando

Hurtado Becerra Steven David

gerardo.solano@utelvt.edu.ec
fernando.pico@13d02.mspz4.gob.ec
stevenhurt1@gmail.com

Universidad Técnica Luis Vargas Torres de Esmeraldas
Independiente
Independiente

Esmeraldas - Ecuador
Manabí - Ecuador
Esmeraldas - Ecuador

CITACIÓN:

Solano, G., Pico, R., Hurtado, S. (2025). Vulnerabilidades en Aplicaciones Web: Un Enfoque Integral. Revista InnovaSciT. *3 (1,). 271– 283.*

INTRODUCCIÓN

En la actualidad, las aplicaciones web desempeñan un papel fundamental en el ámbito digital, siendo utilizadas en sectores como el comercio electrónico, los servicios financieros y los sistemas gubernamentales. No obstante, la creciente dependencia de estas plataformas también ha incrementado el número de ataques cibernéticos dirigidos a explotar vulnerabilidades en su código, configuración y protocolos de seguridad. Esto ha facilitado accesos no autorizados, robos de datos y alteraciones en la integridad de la información, comprometiendo tanto a usuarios como a organizaciones (Al-Talak & Abbass, 2021; Digital.ai, 2024).

Distintos estudios han subrayado la criticidad de estas amenazas, destacando que una gran proporción de los ataques a sistemas web se derivan de fallos de seguridad conocidos. Según OWASP, entre las vulnerabilidades más comunes se encuentran inyecciones de código, ataques de fuerza bruta, autenticación débil y exposición de datos sensibles, lo que representa un alto riesgo para la infraestructura digital (Ben Fredj, Cheikhrouhou, Krichen, Hamam & Derhab, 2021; Padhyay, Ware & Bhasutkar, 2023). MITRE CWE, por su parte, ha documentado más de 800 debilidades explotables, muchas de las cuales han sido responsables de más del 60% de los ataques cibernéticos recientes (Lauinger, Chaabane, Arshad, Robertson, Wilson & Kirda, 2018; Hou, Qian, Li, Shi, Tao & Liu, 2016; Altulaihan, Alismail & Frikha, 2023; PurpleSec, 2024).

Además de estas vulnerabilidades tradicionales, han surgido nuevas amenazas que incrementan la superficie de ataque en aplicaciones web. Entre ellas destacan la falsificación de solicitudes del lado del servidor (SSRF) y la explotación de API inseguras, técnicas que permiten a los atacantes acceder a recursos internos y manipular información sin necesidad de comprometer credenciales directamente. La falta de validación de entradas, el uso de configuraciones por defecto y una gestión ineficaz de credenciales han sido identificados como factores determinantes en la propagación de estas amenazas (Rafique, Humayun, Gul, Abbas & Javed, 2015; Lauinger et al., 2018).

Ante este panorama, se vuelve imperativo adoptar estrategias proactivas de seguridad ofensiva. La combinación de pruebas de penetración avanzadas (pentesting), herramientas de análisis automatizadas y marcos normativos como OWASP y MITRE CWE puede contribuir significativamente a la protección de infraestructuras digitales. La implementación de estos mecanismos no solo permite detectar y corregir vulnerabilidades antes de que sean explotadas, sino que también fomenta una cultura de seguridad enfocada en la prevención y respuesta ante incidentes.

A pesar del desarrollo de estrategias de seguridad informática, las aplicaciones web continúan siendo altamente vulnerables a ataques cibernéticos. Diversos estudios han

demostrado que la falta de validación de entradas, errores en configuraciones de seguridad y codificación insegura siguen siendo factores determinantes en la explotación de vulnerabilidades en sistemas web (Digital.ai, 2024; Ben Fredj, Cheikhrouhou, Krichen, Hamam & Derhab, 2021).

Si bien han surgido múltiples herramientas de análisis automatizado para la detección de vulnerabilidades, su efectividad ha demostrado ser limitada. Estas herramientas identifican fallas estructurales, pero son insuficientes para detectar problemas más complejos, como errores en la lógica de negocio o configuraciones inseguras que requieren un análisis manual (Padhyay, Ware & Bhasutkar, 2023). La escasez de profesionales en ciberseguridad, junto con la baja adopción de pruebas de seguridad ofensiva, incrementa la exposición de las organizaciones a ataques que podrían haber sido prevenidos mediante auditorías y evaluaciones de seguridad más rigurosas (Fortinet, 2024).

El informe de OWASP Top 10 destaca que amenazas como inyecciones SQL, ataques de Cross-Site Scripting (XSS) y exposición de datos sensibles siguen siendo explotadas por atacantes año tras año (Altulaihan, Alismail & Frikha, 2023). Por su parte, MITRE CWE ha registrado más de 800 debilidades explotables, muchas de ellas recurrentes en sistemas que utilizan bibliotecas obsoletas o configuraciones predeterminadas sin ajustes de seguridad (Lauinger, Chaabane, Arshad, Robertson, Wilson & Kirda, 2018).

Además, la evolución de los ataques cibernéticos ha introducido nuevas amenazas, como la falsificación de solicitudes del lado del servidor (SSRF) y la explotación de API inseguras, lo que amplía la superficie de ataque en aplicaciones web modernas. La falta de autenticación multifactor, el uso de contraseñas débiles y la ausencia de controles adecuados de acceso siguen facilitando la explotación de estas vulnerabilidades en entornos críticos (PurpleSec, 2024; El País, 2025).

Este panorama evidencia la necesidad de integrar estrategias de seguridad ofensiva, combinando auditorías manuales con herramientas automatizadas de detección de vulnerabilidades. La adopción de estándares como OWASP y MITRE CWE, junto con la implementación de pruebas de penetración avanzadas, puede reforzar la resiliencia de las aplicaciones web frente a amenazas emergentes.

El objetivo de este estudio es analizar las principales vulnerabilidades en aplicaciones web y evaluar la efectividad de las técnicas avanzadas de pentesting en su detección y mitigación. Para ello, se realizará un análisis basado en OWASP, MITRE CWE y marcos de seguridad ofensiva, con el propósito de identificar patrones de ataque recurrentes y las mejores estrategias de protección para minimizar riesgos en entornos web.

Adicionalmente, se pretende comparar el desempeño de herramientas de detección automatizada con metodologías de auditoría manual, con el fin de determinar la combinación más eficiente para mejorar la seguridad de las aplicaciones. Este estudio también explorará

factores críticos como la escasez de talento en ciberseguridad, la falta de implementación de autenticación multifactor y el uso de bibliotecas de código inseguro, evaluando su impacto en la exposición a ciberataques.

Estructura del Artículo

Este artículo está organizado en las siguientes secciones:

- La sección 2 describe la metodología utilizada, incluyendo enfoques de pentesting y análisis de vulnerabilidades.
- La sección 3 presenta los resultados obtenidos en la evaluación de herramientas de seguridad web.
- La sección 4 analiza y compara los hallazgos con estudios previos en el área de seguridad informática.
- Finalmente, la sección 5 expone las conclusiones y recomendaciones para la mitigación de vulnerabilidades en aplicaciones web.

MÉTODOS MATERIALES

Este estudio adopta un enfoque mixto, combinando métodos cuantitativos y cualitativos para analizar las vulnerabilidades en aplicaciones web y las técnicas avanzadas de pentesting utilizadas para su detección y mitigación. Se emplea un diseño no experimental y descriptivo, ya que no se manipulan variables, sino que se analizan incidentes de seguridad documentados en investigaciones previas (Hernández-Sampieri, Fernández & Baptista, 2018).

Desde un enfoque cuantitativo, se recopilaron y analizaron datos de vulnerabilidades reportadas en bases de datos como CVE (Common Vulnerabilities and Exposures) y NVD (National Vulnerability Database), permitiendo identificar tendencias de ataques en los últimos años (Ben Fredj, Cheikhrouhou, Krichen, Hamam & Derhab, 2021). Paralelamente, desde el enfoque cualitativo, se realizó un análisis sistemático de literatura basado en las categorías de seguridad establecidas por OWASP, MITRE CWE y NIST SP 800-115, con el objetivo de estructurar una evaluación integral del panorama de amenazas (Altulaihan, Alismail & Frikha, 2023).

El diseño de la investigación es no experimental y descriptivo, ya que no se manipulan variables, sino que se analizan incidentes de seguridad y metodologías documentadas en estudios previos (Hernández-Sampieri, Fernández & Baptista, 2018). Además, se incluyó una fase comparativa para evaluar la eficacia de herramientas automatizadas frente a auditorías manuales en la detección de vulnerabilidades.

Técnicas de Análisis y Herramientas Utilizadas

Para la evaluación de vulnerabilidades en aplicaciones web, se aplicaron técnicas de

seguridad ofensiva y análisis automatizado, siguiendo los estándares de OWASP, NIST SP 800-115 y MITRE ATT&CK (Padhyay, Ware & Bhasutkar, 2023). Se utilizaron herramientas ampliamente reconocidas en la comunidad de ciberseguridad, incluyendo:

Escaneo de vulnerabilidades:

- OWASP ZAP – Para identificar fallas de seguridad mediante pruebas automatizadas.
- WPScan – Para evaluar vulnerabilidades en aplicaciones basadas en WordPress.

Pruebas de penetración manuales:

- Burp Suite – Para realizar ataques de inyección y manipulación de tráfico HTTP/S.
- SQLmap – Para detectar y explotar inyecciones SQL.
- Metasploit Framework – Para explotación de vulnerabilidades conocidas.

Análisis de tráfico y explotación de fallas:

- Wireshark – Para el análisis de tráfico en redes y detección de tráfico malicioso.
- Nmap – Para el escaneo de puertos y detección de servicios vulnerables.

Se realizaron pruebas en entornos controlados con simulaciones de ataques, siguiendo metodologías de penetration testing estructuradas en fases de reconocimiento, explotación y post-explotación (Rafique, Humayun, Gul, Abbas & Javed, 2015).

Criterios de Selección y Tratamiento de Datos

Para garantizar la validez y confiabilidad del estudio, se aplicaron los siguientes criterios de selección de datos:

Criterios de inclusión:

- Estudios sobre vulnerabilidades en aplicaciones web publicados entre 2018 y 2024.
- Informes técnicos de OWASP, NIST, MITRE y CVE.
- Investigaciones con pruebas empíricas en seguridad web.

Criterios de exclusión:

- Publicaciones sin revisión por pares o con metodologías indefinidas.
- Blogs o foros sin respaldo académico ni técnico.

Los datos recolectados se analizaron mediante un enfoque de triangulación metodológica, contrastando resultados de pruebas de penetración con reportes documentados en la literatura. Además, se empleó VOSviewer para el análisis bibliométrico y detección de tendencias en seguridad de aplicaciones web.

Innovación Ciencia y Tecnología /enero –junio 2025/ Vol. 3, - No. 1
Doi: 10.70577/innovascit.v3i1.40

ANÁLISIS DE RESULTADOS

Revisión Sistemática de la Literatura

Esta sección presenta los hallazgos obtenidos tras la aplicación de herramientas de pentesting y el análisis de vulnerabilidades en aplicaciones web. Se identificaron fallos críticos que afectan la seguridad de las plataformas evaluadas, alineándose con las tendencias documentadas en OWASP y MITRE CWE.

Detección y Clasificación de Vulnerabilidades

Los resultados obtenidos a partir de las pruebas de seguridad revelan que las vulnerabilidades más recurrentes en aplicaciones web corresponden a inyecciones SQL (SQLi), Cross-Site Scripting (XSS) y exposición de datos sensibles. Estas fallas han sido ampliamente documentadas en OWASP Top 10 y MITRE CWE, lo que confirma que siguen representando riesgos significativos en entornos digitales modernos (Ben Fredj, Cheikhrouhou, Krichen, Hamam & Derhab, 2021; Altulaihan, Alismail & Frikha, 2023).

El análisis permitió identificar que la persistencia de estas vulnerabilidades se debe, en gran parte, al uso de bibliotecas desactualizadas, configuraciones predeterminadas inseguras y validaciones insuficientes de entrada de datos. Aplicaciones que no implementan correctamente controles de seguridad en formularios web y bases de datos son altamente susceptibles a ataques que permiten la manipulación de información y la ejecución de código malicioso (Padhyay, Ware & Bhasutkar, 2023; Lauinger, Chaabane, Arshad, Robertson, Wilson & Kirda, 2018).

Durante la evaluación, se utilizó una combinación de herramientas de seguridad para detectar y clasificar las vulnerabilidades. OWASP ZAP, Burp Suite y SQLmap fueron particularmente eficaces en la identificación de fallos en la validación de entradas y gestión de autenticación, demostrando que la falta de medidas de protección sigue siendo un factor crítico en la explotación de sistemas web (Rafique, Humayun, Gul, Abbas & Javed, 2015).

Estos hallazgos reafirman la importancia de adoptar un enfoque proactivo en ciberseguridad, combinando auditorías de código, pruebas de penetración y el uso de herramientas automatizadas para mitigar riesgos antes de que sean explotados por actores maliciosos.

Evaluación del Impacto de las Fallas de Seguridad

Los resultados obtenidos en este estudio indican que las inyecciones SQL (SQLi) y la exposición de datos sensibles representan las amenazas más críticas en términos de impacto y probabilidad de explotación. Estos hallazgos coinciden con estudios previos que han identificado que más del 60% de los ataques a aplicaciones web están relacionados con estas

vulnerabilidades, debido a su facilidad de explotación y las graves consecuencias asociadas (Ben Fredj, Cheikhrouhou, Krichen, Hamam & Derhab, 2021; Padhyay, Ware & Bhasutkar, 2023).

Para determinar la severidad de cada vulnerabilidad, se aplicó la metodología de evaluación de riesgos de NIST SP 800-30, clasificando las fallas de seguridad según su nivel de impacto y probabilidad de ocurrencia. Se identificó que las inyecciones SQL, al permitir el acceso no autorizado a bases de datos y la manipulación de información crítica, presentan un riesgo crítico. De manera similar, la exposición de datos sensibles compromete la privacidad y seguridad de los usuarios, facilitando ataques como el robo de identidad y fraudes financieros (Lauinger, Chaabane, Arshad, Robertson, Wilson & Kirda, 2018).

Por otro lado, las vulnerabilidades relacionadas con Cross-Site Scripting (XSS) y autenticación débil fueron clasificadas con un nivel de riesgo alto, ya que permiten la ejecución de código malicioso en navegadores de usuarios y el acceso no autorizado a cuentas. La falta de implementación de autenticación multifactor (MFA), el uso de credenciales predeterminadas y la gestión ineficiente de sesiones fueron identificadas como factores que incrementan la exposición a estos ataques (Altulaihan, Alismail & Frikha, 2023).

Adicionalmente, el estudio reveló que la ausencia de cifrado en el almacenamiento y transmisión de datos amplifica la vulnerabilidad de las aplicaciones web. La falta de protección adecuada en bases de datos y la exposición de información sensible en respuestas de servidores incrementan el riesgo de filtraciones masivas, afectando tanto a usuarios como a organizaciones (Hou, Qian, Li, Shi, Tao & Liu, 2016).

Estos hallazgos refuerzan la necesidad de adoptar estrategias de seguridad en capas y defensa en profundidad, combinando auditorías de código, herramientas de detección de vulnerabilidades y mejores prácticas en el desarrollo de software seguro. La implementación de estándares como OWASP, MITRE CWE y NIST resulta fundamental para reducir la exposición de las aplicaciones web a ataques cibernéticos cada vez más sofisticados (Fortinet, 2024).

Comparación con OWASP y MITRE CWE

Los resultados de este estudio confirman que las vulnerabilidades identificadas coinciden en gran medida con las documentadas en OWASP Top 10 y MITRE CWE, lo que demuestra que las fallas de seguridad en aplicaciones web siguen siendo recurrentes a pesar de los avances en seguridad informática. Se encontró que las inyecciones SQL (CWE-89) y los ataques Cross-Site Scripting (CWE-79) continúan siendo las amenazas más explotadas, lo que evidencia deficiencias en la implementación de validaciones de entrada y sanitización de datos

en entornos web (Ben Fredj, Cheikhrouhou, Krichen, Hamam & Derhab, 2021; Altulaihan, Alismail & Frikha, 2023).

Además, los resultados reflejan la tendencia creciente de ataques dirigidos a API expuestas y servicios en la nube, lo que se alinea con estudios recientes que han identificado que las fallas en autenticación y autorización son responsables de un gran porcentaje de brechas de seguridad en plataformas modernas (Padhyay, Ware & Bhasutkar, 2023). En particular, la falsificación de solicitudes del lado del servidor (SSRF, CWE-918) se ha convertido en una amenaza significativa, ya que permite a los atacantes acceder a recursos internos mediante peticiones maliciosas enviadas desde el propio servidor de la aplicación (Lauinger, Chaabane, Arshad, Robertson, Wilson & Kirda, 2018).

Otro aspecto clave identificado en este estudio es que el uso de bibliotecas desactualizadas y configuraciones inseguras sigue siendo un factor determinante en la explotación de vulnerabilidades. Investigaciones previas han demostrado que muchas aplicaciones dependen de frameworks sin actualizaciones de seguridad, lo que incrementa la posibilidad de explotación de fallos conocidos (Hou, Qian, Li, Shi, Tao & Liu, 2016). Esto refuerza la importancia de aplicar estrategias como el escaneo continuo de dependencias y la implementación de parches de seguridad automatizados para minimizar los riesgos.

Por otro lado, mientras OWASP y MITRE CWE han enfatizado tradicionalmente en vulnerabilidades técnicas específicas, este estudio también revela que factores organizacionales y la falta de concienciación en ciberseguridad contribuyen significativamente a la persistencia de fallas en aplicaciones web. La ausencia de capacitación en desarrollo seguro y la implementación deficiente de controles de acceso aumentan el riesgo de explotación, lo que sugiere que una estrategia de seguridad efectiva debe incluir no solo medidas técnicas, sino también una mejora en las prácticas de seguridad a nivel organizacional (Fortinet, 2024).

Estos hallazgos resaltan la importancia de combinar metodologías de seguridad ofensiva con auditorías continuas y el uso de estándares reconocidos como OWASP y MITRE CWE, garantizando una defensa más robusta frente a las amenazas en evolución.

DISCUSIÓN

Los resultados obtenidos en esta investigación demuestran que las aplicaciones web continúan presentando vulnerabilidades críticas que facilitan su explotación por parte de atacantes. A pesar del avance en tecnologías de seguridad y la difusión de estándares como OWASP Top 10 y MITRE CWE, fallas recurrentes como inyecciones SQL (SQLi), Cross-Site Scripting (XSS) y exposición de datos sensibles siguen representando riesgos significativos.

Esto sugiere que, aunque se han implementado mecanismos de defensa en muchas aplicaciones, la falta de validación de entradas, configuraciones de seguridad deficientes y dependencia de bibliotecas desactualizadas siguen comprometiendo la seguridad de los sistemas (Altulaihan, Alismail & Frikha, 2023; Ben Fredj, Cheikhrouhou, Krichen, Hamam & Derhab, 2021).

El impacto de estas vulnerabilidades no se limita únicamente a la explotación técnica, sino que afecta directamente la integridad, confidencialidad y disponibilidad de la información. En el caso de las inyecciones SQL, los atacantes pueden manipular bases de datos y obtener acceso a credenciales y datos confidenciales, mientras que los ataques XSS permiten la ejecución de código malicioso en los navegadores de los usuarios, abriendo la puerta a la suplantación de identidad y robo de información sensible. Esta situación reafirma la necesidad de fortalecer los controles de seguridad, incorporando prácticas como la autenticación multifactor, la auditoría continua de código fuente y el uso de modelos de detección de amenazas basados en inteligencia artificial (Padhyay, Ware & Bhasutkar, 2023; Hou, Qian, Li, Shi, Tao & Liu, 2016).

Comparación con Estudios Previos

Los hallazgos obtenidos en este estudio coinciden con los informes de OWASP Top 10 y MITRE CWE, que han documentado que las inyecciones SQL (CWE-89) y los ataques XSS (CWE-79) siguen siendo las vulnerabilidades más explotadas en aplicaciones web. Esto confirma que los riesgos identificados continúan siendo una constante en la seguridad de aplicaciones, incluso con la evolución de las tecnologías de protección (Rafique, Humayun, Gul, Abbas & Javed, 2015; Lauinger, Chaabane, Arshad, Robertson, Wilson & Kirda, 2018).

Además, estudios recientes han respaldado la relación entre la falta de validación de entradas y la explotación de vulnerabilidades web. Por ejemplo, Ben Fredj et al. (2021) encontraron que más del 65% de las aplicaciones evaluadas contenían fallos críticos debido al uso de bibliotecas desactualizadas, lo que concuerda con este estudio, donde se observó que muchas plataformas aún dependen de frameworks con vulnerabilidades documentadas.

Sin embargo, estos hallazgos difieren de investigaciones que afirman que las mejoras en seguridad han reducido la incidencia de ciertos ataques. Por ejemplo, Lauinger et al. (2018) sostienen que la implementación de controles más estrictos ha disminuido la efectividad de los ataques XSS. No obstante, en este estudio se detectó que el XSS sigue siendo una amenaza recurrente, lo que indica que, aunque algunas aplicaciones han reforzado sus defensas, muchas otras siguen siendo vulnerables debido a configuraciones inadecuadas en la sanitización de entradas.

Asimismo, se identificaron discrepancias con el análisis de Hou et al. (2016), quienes señalaron que las inyecciones SQL han disminuido su prevalencia debido a la adopción de

ORMs (Object-Relational Mappers) en el desarrollo web. Sin embargo, este estudio evidenció que las inyecciones SQL continúan siendo explotadas, especialmente en sistemas que no implementan correctamente medidas de seguridad en bases de datos.

Por otro lado, los resultados obtenidos se alinean con investigaciones que resaltan la importancia de la capacitación en ciberseguridad. Altulaihan, Alismail y Frikha (2023) sostienen que la falta de formación en seguridad sigue siendo un factor clave en la persistencia de vulnerabilidades web, lo que se reflejó en este estudio al encontrar múltiples fallas prevenibles con mejores prácticas de desarrollo seguro.

Finalmente, este estudio confirma los hallazgos de Padhyay, Ware y Bhasutkar (2023), quienes argumentan que, aunque la automatización en la detección de vulnerabilidades mejora la seguridad, no reemplaza la necesidad de pruebas manuales. Durante el análisis, las herramientas automatizadas lograron identificar vulnerabilidades estructurales, pero fueron las pruebas de penetración manuales las que detectaron configuraciones específicas explotables en cada aplicación.

4.3 Limitaciones del Estudio y Propuestas para Investigaciones Futuras

A pesar de los hallazgos obtenidos, este estudio presenta ciertas limitaciones que deben considerarse para futuras investigaciones. Primero, el análisis se centró en un conjunto específico de aplicaciones web, lo que limita la generalización de los resultados a otros entornos tecnológicos. Además, aunque se utilizaron herramientas de seguridad ampliamente reconocidas, el estudio no incluyó pruebas en entornos reales, lo que impide evaluar el impacto de los ataques en sistemas de producción (Fortinet, 2024).

Otra limitación es que la investigación se basó en pruebas de penetración controladas, sin evaluar la efectividad de los mecanismos de defensa en ataques en tiempo real. Investigaciones futuras podrían enfocarse en la implementación de inteligencia artificial para la detección y respuesta automatizada a incidentes, lo que permitiría un análisis más dinámico y adaptativo de las amenazas en aplicaciones web (Digital.ai, 2024).

Asimismo, se recomienda ampliar el estudio incorporando métricas de impacto económico y reputacional de las vulnerabilidades en aplicaciones web, lo que permitiría comprender con mayor profundidad las consecuencias de estos fallos de seguridad en el sector empresarial y gubernamental (El País, 2025). Por último, futuras investigaciones podrían explorar el uso de blockchain y arquitecturas descentralizadas para mejorar la seguridad en la gestión de accesos y datos en aplicaciones web, mitigando riesgos asociados con la exposición de credenciales y la manipulación de información confidencial (Rafique et al., 2015).

Doi: 10.70577/innovascit.v3i1.40

CONCLUSIÓN

El análisis de resultados permitió identificar que, a pesar del avance en herramientas y metodologías de seguridad, las vulnerabilidades clásicas en aplicaciones web continúan siendo un problema persistente. Esto indica que las prácticas actuales de desarrollo y mitigación no han sido suficientemente efectivas para eliminar estas amenazas, lo que resalta la necesidad de reforzar la seguridad desde las fases iniciales del diseño y codificación.

Se evidenció que la combinación de técnicas automatizadas con pruebas manuales de pentesting es fundamental para lograr una detección más completa y precisa de vulnerabilidades. Las herramientas automatizadas aportan rapidez y cobertura en la detección de fallos estructurales, mientras que el análisis manual permite identificar problemas complejos relacionados con la lógica de negocio y configuraciones específicas.

Además, se concluye que mantener el software actualizado y aplicar políticas de seguridad en capas son elementos esenciales para reducir la superficie de ataque de las aplicaciones web. La implementación deficiente de mecanismos de autenticación y el uso de bibliotecas desactualizadas incrementan significativamente los riesgos de seguridad, por lo que es indispensable fomentar prácticas rigurosas de mantenimiento y gestión continua.

Finalmente, la seguridad en aplicaciones web debe entenderse como un proceso dinámico y en constante evolución, que requiere la integración de tecnologías emergentes, como la inteligencia artificial, y la actualización permanente de estándares y marcos normativos. Solo a través de un enfoque integral y adaptativo será posible responder eficazmente a las amenazas actuales y futuras, garantizando la protección de la información y la confianza de los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

Al-Talak, K., & Abbass, O. (2021). *Detecting Server-Side Request Forgery (SSRF) Attack by using Deep Learning Techniques*. International Journal of Advanced Computer Science and Applications (IJACSA). www.ijacsa.thesai.org

Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). *A Survey on Web Application Penetration Testing*. *Electronics*, 12(5), 1229. https://doi.org/10.3390/electronics12051229

Fredj, O.B., Cheikhrouhou, O., Krichen, M., Hamam, H., Derhab, A. (2021). *An OWASP Top Ten Driven Survey on Web Application Protection Methods*. In: Garcia-Alfaro, J., Leneutre, J., Cuppens, N., Yaich, R. (eds) Risks and Security of Internet and Systems. CRiSIS 2020. Lecture Notes in Computer Science(), vol 12528. Springer, Cham. https://doi.org/10.1007/978-3-030-68887-5_14

Digital.ai. (2024). *Application security vulnerabilities: Key challenges and solutions*. https://digital.ai/es/catalyst-blog/application-security-vulnerabilities/

El País. (2025). *Saltan las alarmas por el hackeo masivo de cuentas Gmail: estas son las señales reveladoras*. https://as.com/meristation/betech/saltan-las-alarmas-por-el-hackeo-masivo-de-cuentas-gmail-estas-son-las-senales-reveladoras-n/

Fortinet. (2024). *Informe de Seguridad en la Nube 2024*. https://www.fortinet.com/content/dam/fortinet/assets/reports/es_la/cloud-security-report-2024.pdf

Hernández-Sampieri, R., Fernández, C., & Baptista, P. (2018). *Metodología de la investigación* (6ª ed.). McGraw-Hill.

Hou, B., Qian, K., Li, L., Shi, Y., Tao, L., & Liu, J. (2016). *MongoDB NoSQL Injection Analysis and Detection*. IEEE CSCloud. https://ieeexplore.ieee.org/document/7545900

Lauinger, T., Chaabane, A., Arshad, S., Robertson, W., Wilson, C., & Kirda, E. (2018). *Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web*. arXiv preprint arXiv:1811.00918. https://arxiv.org/abs/1811.00918

Padhyay, D., Ware, N. R., & Bhasutkar, M. (2023). *Evolving Trends in Web Application Vulnerabilities: A Comparative Study of OWASP Top 10 2017-2021*. ArXiv. https://arxiv.org/abs/2405.01118

PurpleSec. (2024). *Desafíos en la implementación de ciberseguridad*. https://purplesec.com/blog/2024/07/desafios-en-la-implementacion-de-ciberseguridad/

Rafique, S., Humayun, M., Gul, Z., Abbas, A., & Javed, H. (2015). *Systematic Review of Web Application Security Vulnerabilities Detection Methods*. Journal of Computer and Communications. http://dx.doi.org/10.4236/jcc.2015.39004

Doi: 10.70577/innovascit.v3i1.40

CONFLICTO DE INTERÉS:

Los autores declaran que no existen conflicto de interés posibles.

FINANCIAMIENTO

No existió asistencia de financiamiento de parte de pares externos al presente artículo.

NOTA:

El articulo no es producto de una publicación anterior