REPÚBLICA DE PANAMÁ

MINISTERIO DE EDUCACIÓN

INSTITUTO SUPERIOR TECNOLÓGICO DEL CLAUSTRO GÓMEZ

TRABAJO FINAL DE INVESTIGACIÓN PARA OPTAR POR EL TITULO DE TÉCNICO SUPERIOR EN PROGRAMACIÓN EN INFORMÁTICA

ANÁLISIS DE VULNERABILIDADES EN APLICACIONES WEB Y CÓMO PREVENIRLAS

ELABORADO POR: LARISSA JUDITH PÉREZ ARENAS - 6-705-1215

Julio 2024

ÍNDICE

I. RESUMEN 3
II. INTRODUCCION 4
III. JUSTIFICACIÓN 5
IV. OBJETIVOS 6
V. MARCO TEORICO 7
VI. METODOLOGIA 8
VII. DESARROLLO O CUERPO DEL TRABAJO 10
VIII. CONCLUSIÓN 12
IX. RECOMENDACIONES 13
X. BIBLIOGRAFIA 15

I. RESUMEN

El tema de esta tesina se centra en el análisis de vulnerabilidades en aplicaciones web y las metodologías para prevenirlas, con el objetivo de identificar las amenazas más comunes que afectan a las aplicaciones en línea y proponer prácticas y herramientas para mitigar los riesgos. En la actualidad, las aplicaciones web se han convertido en una parte integral de la vida cotidiana, desde las plataformas de comercio electrónico hasta los sistemas bancarios en línea. Sin embargo, debido a su exposición a internet, estas aplicaciones están constantemente en riesgo de sufrir ataques cibernéticos que comprometan la seguridad de los usuarios y de la información almacenada. En este contexto, es fundamental comprender las vulnerabilidades más comunes, como la inyección SQL, los ataques de Cross-Site Scripting (XSS), la falsificación de solicitudes entre sitios (CSRF) y otros vectores de ataque, para implementar medidas de protección efectivas.

El objetivo general de esta investigación es proporcionar un análisis detallado de las vulnerabilidades más críticas en las aplicaciones web y desarrollar estrategias prácticas para prevenirlas. Los objetivos específicos incluyen la identificación de las vulnerabilidades más prevalentes en las aplicaciones web actuales, la explicación de las técnicas de ataque utilizadas por los ciberdelincuentes y la propuesta de mejores prácticas de seguridad para proteger las aplicaciones durante su ciclo de vida. Asimismo, se busca sensibilizar a los desarrolladores y administradores de sistemas sobre la importancia de integrar medidas de seguridad desde las etapas iniciales de desarrollo, aplicando principios de "seguridad por diseño".

La metodología empleada en esta investigación es de tipo cualitativa y descriptiva, en la que se realiza una revisión exhaustiva de la literatura existente sobre vulnerabilidades web, normativas de seguridad y estudios de caso sobre ataques recientes. Además, se lleva a cabo un análisis comparativo de herramientas y técnicas utilizadas para detectar vulnerabilidades en las aplicaciones web, como los escáneres de seguridad, las pruebas de penetración y las auditorías de código. Para complementar la revisión documental, se incluyen entrevistas con expertos en seguridad informática para obtener perspectivas prácticas sobre las soluciones más efectivas para mitigar los riesgos.

En cuanto a las conclusiones, se destaca que las aplicaciones web continúan siendo un blanco atractivo para los atacantes debido a su exposición constante a internet. A pesar de las numerosas herramientas y técnicas disponibles, muchas aplicaciones siguen siendo vulnerables debido a la falta de una cultura de seguridad adecuada en el desarrollo de software. Es esencial que los desarrolladores implementen prácticas de desarrollo seguro y realicen pruebas de seguridad de manera continua para detectar posibles fallos antes de que sean explotados. También se concluye que la capacitación constante y la actualización de los sistemas de seguridad son claves para garantizar una protección robusta frente a las amenazas emergentes. Finalmente, se recomienda adoptar un enfoque integral en el diseño de aplicaciones web, que incluya tanto medidas preventivas como sistemas de monitoreo para detectar vulnerabilidades de manera proactiva y mitigar los impactos de posibles ataques.

II. INTRODUCCION

El tema central de esta investigación es el análisis de las vulnerabilidades en aplicaciones web y las metodologías para prevenirlas. En un mundo cada vez más digitalizado, las aplicaciones web han tomado un papel central en la prestación de servicios, desde el comercio electrónico hasta el acceso a servicios financieros y la gestión de datos personales. Sin embargo, debido a su constante exposición a internet, estas aplicaciones se han convertido en un blanco fácil para los cibercriminales. Los ataques a estas plataformas pueden comprometer la seguridad de millones de usuarios, exponer datos sensibles e incluso ocasionar grandes pérdidas económicas y reputacionales para las empresas que las gestionan.

Las aplicaciones web son desarrolladas utilizando diversas tecnologías, y aunque estas tecnologías ofrecen una funcionalidad avanzada y escalable, también introducen diversas vulnerabilidades. Entre las amenazas más comunes se incluyen la inyección SQL, el Cross-Site Scripting (XSS), la falsificación de solicitudes entre sitios (CSRF) y los ataques de denegación de servicio (DoS). Estas vulnerabilidades pueden explotarse de diferentes maneras, y la falta de una estrategia de seguridad adecuada puede permitir que un atacante

obtenga acceso no autorizado, modifique datos o incluso cause una interrupción total del servicio. La investigación se enfoca en identificar las vulnerabilidades más comunes y explorar las mejores prácticas y técnicas para prevenirlas, asegurando que las aplicaciones web sean más resistentes frente a amenazas externas.

Además, es importante reconocer que muchas de estas vulnerabilidades surgen debido a un diseño y desarrollo inadecuado de las aplicaciones, así como a una falta de conciencia en cuanto a las mejores prácticas de seguridad. Muchas veces, los desarrolladores se enfocan principalmente en la funcionalidad de la aplicación y no le otorgan la atención necesaria a los aspectos relacionados con la protección de datos y la prevención de accesos no autorizados. La ausencia de medidas básicas de seguridad, como la validación adecuada de entradas, el cifrado de datos y la implementación de controles de acceso, deja a las aplicaciones expuestas a posibles ataques que pueden ser fácilmente evitados con un enfoque proactivo en la seguridad.

Por lo tanto, esta investigación no solo busca identificar y analizar las vulnerabilidades más comunes en las aplicaciones web, sino también promover una cultura de seguridad en el desarrollo de software. Es fundamental que los desarrolladores, empresas y organizaciones entiendan que la seguridad no debe ser una reflexión posterior, sino un componente integral durante todo el proceso de desarrollo. Adoptar estándares y marcos de seguridad, como los lineamientos de OWASP (Open Web Application Security Project), puede resultar esencial para mitigar riesgos, fortalecer las aplicaciones y garantizar que los servicios prestados sean confiables, seguros y sostenibles a largo plazo.

III. JUSTIFICACIÓN

La importancia de este estudio radica en el creciente número de ataques dirigidos a aplicaciones web en todo el mundo. Según estudios recientes, las vulnerabilidades en las aplicaciones web son la principal causa de violaciones de seguridad cibernética, afectando tanto a empresas como a usuarios individuales. A medida que la dependencia de estas plataformas aumenta, también lo hacen los riesgos asociados a su uso. Por ejemplo, un ataque exitoso de inyección SQL puede dar a los atacantes acceso completo a la base de

datos de una aplicación, mientras que un XSS puede permitirles robar cookies de sesión o redirigir a los usuarios a sitios maliciosos.

La protección de las aplicaciones web es esencial no solo para garantizar la confidencialidad y la integridad de los datos, sino también para proteger la reputación y la confianza de los usuarios en los servicios en línea. El impacto de un ataque cibernético puede ser devastador, con consecuencias económicas significativas debido a la pérdida de clientes, costos legales y de remediación, y daños irreparables a la imagen de la empresa. Por lo tanto, garantizar que las aplicaciones web sean seguras no solo es una prioridad técnica, sino también un factor crítico para la supervivencia y el éxito a largo plazo de cualquier negocio que dependa de plataformas digitales.

Además, el hecho de que las amenazas evolucione constantemente hace que el análisis y la prevención de vulnerabilidades sea un campo de estudio dinámico y crucial. Las nuevas técnicas de ataque se desarrollan continuamente, lo que significa que las estrategias de defensa deben mantenerse al día. Este estudio contribuye a la creación de una base sólida de conocimientos sobre las mejores prácticas de seguridad, herramientas y metodologías utilizadas por los profesionales para identificar y mitigar estos riesgos antes de que puedan ser explotados.

IV. OBJETIVOS

- **Objetivo general**

– El objetivo principal de esta investigación es analizar las vulnerabilidades más comunes que afectan a las aplicaciones web y proponer metodologías y mejores prácticas para prevenirlas, con el fin de mejorar la seguridad de estas plataformas y proteger tanto a los usuarios como a las organizaciones que las gestionan.

- **Objetivos específicos**

– Identificar las vulnerabilidades más comunes en las aplicaciones web actuales, con énfasis en las amenazas más prevalentes como la inyección SQL, Cross-Site Scripting (XSS), falsificación de solicitudes entre sitios (CSRF), y otros tipos de ataques cibernéticos.

- Analizar las técnicas de ataque más comunes utilizadas por los ciberdelincuentes para explotar estas vulnerabilidades, y comprender cómo los atacantes pueden acceder a sistemas sensibles a través de estas brechas de seguridad.
- Examinar las herramientas y metodologías de prevención que los desarrolladores y administradores de aplicaciones web pueden utilizar para mitigar las vulnerabilidades identificadas, incluyendo el uso de autenticación y autorización robustas, cifrado de datos, validación de entradas y otras buenas prácticas.

V. MARCO TEORICO

Las vulnerabilidades en aplicaciones web se refieren a fallos o debilidades en la programación, diseño o configuración de una aplicación web que pueden ser explotadas por atacantes para comprometer la seguridad del sistema. Estas vulnerabilidades permiten a los ciberdelincuentes acceder a información confidencial, modificar datos, o incluso tomar control de los sistemas. Las aplicaciones web modernas suelen estar expuestas a amenazas debido a su accesibilidad a través de internet, lo que las convierte en un blanco frecuente para los atacantes. Las vulnerabilidades más comunes incluyen inyección SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) y denegación de servicio (DoS). Estas amenazas pueden ser mitigadas a través de diversas técnicas de seguridad y buenas prácticas de desarrollo.

El modelo de seguridad en capas es una teoría fundamental en la prevención de vulnerabilidades. Según este modelo, la seguridad debe aplicarse en múltiples niveles, desde el servidor hasta la aplicación y los usuarios. La idea es construir una "defensa en profundidad", donde, incluso si una capa de seguridad es vulnerada, otras capas continúan protegiendo los recursos críticos. Este enfoque ayuda a mitigar el impacto de un ataque y reduce la probabilidad de que un atacante pueda explotar múltiples vulnerabilidades en el sistema. Un componente clave de esta estrategia es el uso de autenticación y autorización robustas, cifrado de datos y validación de entradas. La implementación de estas medidas puede prevenir muchos de los ataques más comunes, como la inyección SQL, que explota vulnerabilidades de entrada no validada.

En términos de prevención y mitigación, diversos estudios han analizado el uso de técnicas como la validación rigurosa de entradas, la gestión de sesiones segura, y la implementación de políticas de acceso restringido. Herramientas como el OWASP Top Ten, un listado de las diez vulnerabilidades más críticas en aplicaciones web, han servido como guía para los desarrolladores. Esta lista se actualiza regularmente, incorporando nuevas amenazas emergentes y proporcionando recomendaciones específicas para abordarlas. La implementación de estas directrices ha demostrado ser eficaz en la reducción de las vulnerabilidades más comunes. Además, las prácticas de código seguro, que incluyen el uso de frameworks y bibliotecas bien mantenidas, también juegan un papel crucial en la reducción de las brechas de seguridad.

La teoría de la seguridad proactiva, que se basa en anticiparse a los posibles ataques mediante la identificación y mitigación de vulnerabilidades antes de que sean explotadas, es otro enfoque relevante. Esta teoría hace hincapié en la importancia de realizar auditorías de seguridad regulares, pruebas de penetración y el uso de herramientas de análisis estático de código para detectar vulnerabilidades. Estas acciones permiten a los desarrolladores detectar problemas de seguridad en las primeras etapas del ciclo de desarrollo, evitando que los atacantes puedan explotarlos una vez que la aplicación esté en producción. La incorporación de seguridad en el ciclo de vida del desarrollo de software (SDLC) es clave para desarrollar aplicaciones web más seguras y resistentes frente a ataques.

VI. METODOLOGIA

La presente investigación es de tipo mixto, ya que combina elementos tanto cualitativos como cuantitativos para abordar de manera integral el análisis de las vulnerabilidades en aplicaciones web y las estrategias para prevenirlas. Por un lado, se realizan análisis cualitativos para entender las amenazas y vulnerabilidades más comunes en aplicaciones web, basándose en estudios previos, informes de expertos y casos documentados. Este enfoque permite una comprensión profunda de los mecanismos que propician los ataques y de cómo las aplicaciones web pueden ser comprometidas. Por otro lado, la investigación incorpora un enfoque cuantitativo, en el cual se realizan encuestas y análisis estadísticos

para evaluar el grado de conocimiento y las prácticas de seguridad que implementan los desarrolladores de aplicaciones web en el ámbito real. La combinación de estos enfoques permitirá obtener tanto una visión general como datos concretos sobre las medidas de seguridad más efectivas y su implementación práctica.

Para llevar a cabo esta investigación se emplean diversas fuentes de datos y técnicas de recopilación. Las fuentes primarias incluyen entrevistas con expertos en seguridad informática, tales como desarrolladores de software, auditores de seguridad y profesionales de ciberseguridad. Estas entrevistas permitirán obtener perspectivas cualitativas sobre las mejores prácticas en el desarrollo seguro de aplicaciones web, así como sobre las vulnerabilidades más comunes y cómo prevenirlas. Adicionalmente, se realizarán encuestas a desarrolladores de aplicaciones web para obtener datos cuantitativos sobre sus conocimientos en seguridad, las herramientas que utilizan y los procesos que implementan para proteger sus aplicaciones. Estas encuestas estarán orientadas a medir la prevalencia de vulnerabilidades conocidas y la efectividad de las prácticas de seguridad aplicadas en proyectos reales.

Otra técnica importante de recopilación de datos es el análisis documental, el cual se realizará mediante la revisión de informes y estudios previos sobre vulnerabilidades en aplicaciones web, así como de los lineamientos de seguridad proporcionados por organizaciones como OWASP (Open Web Application Security Project). Estos documentos proporcionan un marco teórico y práctico para la identificación y mitigación de riesgos. Además, se incluirán los resultados de estudios de casos sobre aplicaciones web que hayan sido víctimas de ataques, lo que permitirá un análisis detallado de las brechas de seguridad más comunes y las respuestas implementadas ante tales incidentes.

En cuanto a los métodos de análisis, se empleará una combinación de análisis cualitativo y cuantitativo para interpretar los datos recopilados. El análisis cualitativo se centrará en la codificación y categorización de las entrevistas realizadas, identificando patrones comunes en las respuestas de los expertos. Esto permitirá extraer conclusiones sobre las vulnerabilidades más críticas y las mejores prácticas para prevenirlas. Además, se utilizará

el análisis de contenido para examinar los informes y estudios de caso, enfocándose en las soluciones implementadas en diversas aplicaciones y su efectividad a largo plazo.

Por otro lado, el análisis cuantitativo se llevará a cabo mediante la estadística descriptiva, procesando los resultados de las encuestas para identificar tendencias y correlaciones entre el conocimiento de seguridad de los desarrolladores y las prácticas que implementan. Se utilizarán herramientas como SPSS o Excel para realizar análisis estadísticos que proporcionen una visión clara sobre la prevalencia de ciertos riesgos y las medidas adoptadas para mitigarlos. Además, se implementarán pruebas de hipótesis para determinar si existen diferencias significativas en la implementación de medidas de seguridad entre diferentes tipos de aplicaciones web o entre desarrolladores con distintos niveles de experiencia.

Este enfoque metodológico mixto permitirá obtener una visión integral sobre las vulnerabilidades en las aplicaciones web, combinando la teoría y la práctica, lo que proporcionará recomendaciones bien fundamentadas para mejorar la seguridad en el desarrollo de aplicaciones.

VII. DESARROLLO O CUERPO DEL TRABAJO

El análisis de las vulnerabilidades en las aplicaciones web y cómo prevenirlas es un tema que reviste gran importancia debido al incremento de ciberataques y la dependencia cada vez mayor de las aplicaciones en diversos sectores. En el primer capítulo se abordaron las principales amenazas y vulnerabilidades que enfrentan las aplicaciones web. Se identificaron riesgos comunes como la inyección SQL, cross-site scripting (XSS), cross-site request forgery (CSRF), y las fallas en la autenticación y autorización. Estos problemas son responsables de la mayoría de los incidentes de seguridad en la web, ya que permiten a los atacantes acceder, manipular o robar datos sensibles de los usuarios o del sistema. Las pruebas y revisiones de código son esenciales para identificar estas vulnerabilidades en etapas tempranas del desarrollo, lo que garantiza que los desarrolladores puedan implementar correcciones antes de que la aplicación sea puesta en producción.

En el segundo capítulo, se profundiza en las estrategias y mejores prácticas de seguridad en el desarrollo de aplicaciones web. La implementación de una arquitectura segura desde el diseño es crucial, y principios como la validación de entradas, el uso de contraseñas seguras y el cifrado de datos deben ser parte del proceso desde el inicio. Asimismo, se destaca la importancia de autenticación robusta utilizando métodos como OAuth 2.0 o JWT (JSON Web Tokens), que permiten controlar y restringir el acceso a los recursos solo a usuarios legítimos. Otra técnica clave es el uso de principios de menor privilegio, lo que implica que cada componente de la aplicación solo debe tener acceso a los recursos necesarios para su funcionamiento. Estas prácticas no solo protegen los datos del usuario, sino que también mejoran la integridad y disponibilidad de la aplicación.

El tercer capítulo discute la evaluación de vulnerabilidades y cómo llevar a cabo auditorías de seguridad regulares. Las herramientas de análisis de seguridad automatizado, como OWASP ZAP y Burp Suite, se presentan como soluciones efectivas para detectar vulnerabilidades durante el ciclo de vida de la aplicación. A través de pruebas de penetración y análisis dinámico, es posible identificar posibles brechas de seguridad que podrían haber pasado desapercibidas durante el desarrollo. Además, se subraya la necesidad de realizar pruebas en entornos controlados para simular los ataques reales y analizar el comportamiento de la aplicación bajo condiciones extremas. Las auditorías regulares no solo ayudan a identificar puntos débiles, sino que también permiten evaluar la efectividad de las medidas de seguridad implementadas a lo largo del tiempo.

En el cuarto capítulo, se aborda el papel fundamental de la educación y capacitación de los desarrolladores y el equipo de TI en cuanto a seguridad. La concientización sobre las amenazas y vulnerabilidades comunes es uno de los pilares de una defensa efectiva. En muchos casos, los errores de seguridad no surgen por fallas tecnológicas, sino por falta de formación en prácticas seguras. Por ello, se recomienda incorporar programas de formación continua sobre seguridad en aplicaciones web, que incluyan temas como el desarrollo de código seguro, la identificación de vulnerabilidades y la gestión adecuada de datos sensibles. Además, se discute la importancia de una cultura de seguridad dentro de las

organizaciones, donde la seguridad no se vea como una tarea secundaria, sino como un componente esencial del ciclo de vida del software.

Finalmente, en el quinto capítulo, se presentan las tecnologías emergentes que están influyendo en la evolución de la seguridad en aplicaciones web, como la inteligencia artificial (IA) y el aprendizaje automático (ML). Estas tecnologías están siendo aplicadas para detectar patrones de ataque en tiempo real, analizar grandes volúmenes de datos y mejorar la respuesta ante incidentes de seguridad. Las herramientas basadas en IA pueden aprender de los ataques anteriores para predecir y mitigar amenazas futuras, proporcionando una capa adicional de protección que no está disponible en los métodos tradicionales de seguridad. Asimismo, se examinan los avances en blockchain como una tecnología prometedora para mejorar la integridad y la trazabilidad de los datos, lo que puede ser especialmente útil en aplicaciones que manejan información crítica o de alto valor.

A través de estos capítulos, se logra construir una visión integral sobre las vulnerabilidades en aplicaciones web, sus riesgos asociados, y las estrategias efectivas para prevenir y mitigar estos problemas. Al combinar análisis técnico con mejores prácticas y el uso de nuevas tecnologías, este trabajo de investigación proporciona un marco de acción para desarrollar aplicaciones web seguras y robustas frente a amenazas cada vez más sofisticadas.

VIII. CONCLUSIÓN

En conclusión, este trabajo de investigación ha abordado de manera integral las vulnerabilidades más comunes a las que están expuestas las aplicaciones web y las metodologías necesarias para prevenirlas, con un enfoque particular en las buenas prácticas de seguridad durante el desarrollo. Se han identificado y analizado las principales amenazas cibernéticas, tales como la inyección SQL, XSS, CSRF, y las vulnerabilidades asociadas a la autenticación y autorización. Estos problemas son responsables de una gran parte de los ataques que comprometen la integridad y la privacidad de los datos en la web, lo que

subraya la necesidad de implementar medidas preventivas en las fases iniciales del ciclo de vida del desarrollo de software.

A lo largo de la investigación, se demostró que las mejores prácticas de seguridad deben ser una prioridad para todos los desarrolladores de aplicaciones web. La implementación de validaciones de entradas, el uso de contraseñas robustas y la cifrado de datos, así como el empleo de sistemas de autenticación segura, como OAuth 2.0 y JSON Web Tokens (JWT), son elementos clave para garantizar la protección de los datos de los usuarios y la integridad de la aplicación. Además, se destacó la importancia de realizar auditorías de seguridad periódicas, utilizando herramientas de análisis de vulnerabilidades como OWASP ZAP y Burp Suite, para identificar y corregir posibles brechas de seguridad antes de que sean explotadas por atacantes. También se identificó la necesidad de un enfoque educativo continuo, no solo en la incorporación de mejores prácticas, sino también en la capacitación de los desarrolladores para reconocer las amenazas de seguridad y aplicar soluciones proactivas.

IX. RECOMENDACIONES

A partir de los hallazgos de esta investigación, se pueden ofrecer varias recomendaciones tanto para futuras investigaciones como para la implementación práctica de medidas de seguridad en el desarrollo de aplicaciones web:

Investigación y adopción de tecnologías emergentes en seguridad: La inteligencia artificial y el aprendizaje automático están transformando la forma en que las aplicaciones web pueden protegerse contra las amenazas cibernéticas. Es recomendable que futuras investigaciones exploren más a fondo cómo estas tecnologías pueden integrarse en los sistemas de seguridad para detectar ataques en tiempo real y prever amenazas futuras, mejorando la capacidad de respuesta ante incidentes. Además, el blockchain se presenta como una tecnología prometedora que podría ser utilizada para reforzar la integridad de los datos en aplicaciones críticas.

Desarrollo de un enfoque de seguridad integral desde el inicio del ciclo de vida del software: Es crucial que la seguridad no sea considerada como una fase final del

desarrollo, sino que debe ser integrada de manera proactiva desde las primeras etapas del diseño. Las futuras investigaciones deberían centrarse en la creación de marcos y guías de mejores prácticas que incluyan seguridad en cada fase del desarrollo, desde la concepción de la idea hasta el mantenimiento post-lanzamiento.

Automatización de auditorías de seguridad: Aunque las auditorías manuales siguen siendo esenciales, las organizaciones deben invertir en herramientas automatizadas que faciliten la detección de vulnerabilidades. Estas herramientas pueden ayudar a realizar pruebas de penetración de manera constante y a detectar patrones de comportamiento anómalo que podrían indicar vulnerabilidades en tiempo real. El uso de plataformas como OWASP ZAP debería ser una práctica común en todas las etapas del ciclo de vida del software.

Concientización y capacitación continua: Una de las claves para mantener una infraestructura de seguridad robusta es la capacitación constante de los desarrolladores y personal técnico en cuanto a las últimas amenazas y buenas prácticas de seguridad. Las organizaciones deben integrar programas de formación sobre desarrollo de código seguro, técnicas de prevención de inyección de código, y metodologías como DevSecOps, que integran la seguridad directamente en los procesos de desarrollo y despliegue de aplicaciones.

Colaboración con la comunidad de seguridad: Las empresas y desarrolladores deben formar parte activa de la comunidad de seguridad informática, colaborando con proyectos como OWASP y compartiendo información sobre vulnerabilidades y técnicas de mitigación. De esta forma, se puede mejorar de manera colectiva la seguridad de las aplicaciones web y estar al tanto de las últimas tendencias y amenazas emergentes.

Este trabajo subraya la importancia de un enfoque proactivo y bien fundamentado en la seguridad de las aplicaciones web. Las vulnerabilidades son una amenaza constante que puede tener consecuencias devastadoras si no se tratan adecuadamente. A través de la adopción de las mejores prácticas, el uso de tecnologías avanzadas y la formación continua

de los profesionales de TI, es posible mitigar estos riesgos y garantizar aplicaciones más seguras y confiables.

X. BIBLIOGRAFIA

- Makianich, J., Lomo, Y., Guerra, B., Colazo, O., Mansilla, M., Dolan, G., & Fabbri, L. M. (2024). Las herramientas para la mitigación de riesgos de las aplicaciones web. AJEA (Actas de Jornadas y Eventos Académicos de UTN), (AJEA 38).
- Páez Poblete, E. R. (2024). Aplicación de herramientas para el análisis estático y dinámico de código en aplicaciones web.
- ORTIZ LEÓN, G. L. (2025). ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN ATAQUE CIBERNETICO PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN (Bachelor's thesis, Jipijapa-Unesum).
- CALLI RODRIGUEZ, B. V. (2024). PROPUESTA DE IMPLEMENTACIÓN DE TÉCNICAS PARA MITIGAR LA INYECCIÓN SQL Y CIFRADO O HASHING DE INFORMACIÓN EN EL SITIO WEB DE ODONTOLOGÍA DE LA UMSS (Doctoral dissertation).
- Miranda Quezada, C. E., Vasquez Vasquez, F., & Yauri Machaca, M. R. Método de Referencia para Identificar Vulnerabilidades en Aplicaciones Android en PYMES utilizando Herramientas Automatizadas de Código Abierto.