Dom. Cien., ISSN: 2477-8818
Vol. 9, núm. 3. Julio-Septiembre, 2023, pp. 2219-2229

DOI: https://doi.org/10.23857/dc.v9i3.3552

Ciencias de la Computación
Artículo de Investigación

Seguridad en desarrollo web: mejores prácticas para proteger aplicaciones y datos

Segurança no desenvolvimento da web: melhores práticas para proteger aplicativos e dados

Segurança no desenvolvimento da web: melhores práticas para proteger aplicativos e dados

Gustavo Andrés Ramírez-Patajalo [I]
gustavo.ramirez@iti.edu.ec
https://orcid.org/0000-0002-1453-5378

Correspondencia: gustavo.ramirez@iti.edu.ec

*__Recibido:__ 13 de junio de 2023 *__Aceptado:__ 23 de agosto de 2023 __* Publicado:__ 11 de septiembre de 2023

I. Instituto Superior Tecnológico Internacional, Ecuador.

Resumen

En un contexto digital cada vez más interconectado y propenso a amenazas cibernéticas, la seguridad en el desarrollo web y la implementación de mejores prácticas para proteger aplicaciones y datos han emergido como una necesidad imperante. La revisión exhaustiva de la literatura revela que adoptar enfoques sólidos de seguridad desde las etapas iniciales del desarrollo es esencial para garantizar la integridad y confidencialidad en un entorno virtual. El Open Web Application Security Project (OWASP) se destaca como una guía fundamental, con un consenso unánime en su relevancia en casi el 85% de los trabajos revisados. Los principios establecidos por OWASP, junto con la atención a las diez principales vulnerabilidades identificadas, se perfilan como un enfoque efectivo para mitigar los riesgos más comunes en las aplicaciones web. La autenticación multifactor y el uso de técnicas de cifrado se reconocen como estrategias esenciales para prevenir accesos no autorizados y salvaguardar datos sensibles. Además, las pruebas de penetración y las auditorías de seguridad regulares, que alcanzan aproximadamente un 55% de consenso, emergen como medios cruciales para identificar y remediar posibles debilidades. La educación y concientización del personal de desarrollo, con un enfoque en buenas prácticas, se considera un factor determinante para una implementación efectiva de la seguridad.

Palabras Claves: Seguridad en desarrollo web; Mejores prácticas de seguridad; Protección de aplicaciones web; Ciberseguridad; OWASP; Vulnerabilidades web.

Abstract

In a digital context that is increasingly interconnected and prone to cyber threats, security in web development and the implementation of best practices to protect applications and data have emerged as a pressing need. The exhaustive review of the literature reveals that adopting solid security approaches from the initial stages of development is essential to guarantee integrity and confidentiality in a virtual environment. The Open Web Application Security Project (OWASP) stands out as a fundamental guide, with a unanimous consensus on its relevance in only 85% of the works reviewed. The principles established by OWASP, together with attention to the main identified vulnerabilities, stand out as an effective approach to mitigate the most common risks in web applications. Multifactor authentication and the use of encryption techniques are recognized as essential strategies for preventing unauthorized access and safeguarding sensitive data. Furthermore, penetration tests and regular security audits, which reach approximately 55% consensus, emerge as

crucial measures to identify and remedy possible weaknesses. Personal development education and awareness, with a focus on good practices, is considered a determining factor for effective security implementation.

Keywords: Segurança e desenvolvimento da web; Melhores práticas de segurança; Proteção de aplicativos web; Cibersegurança; OWASP; Vulnerabilidades web.

Resumo

Em um contexto digital cada vez mais interconectado e sujeito a ameaças cibernéticas, a segurança no desenvolvimento da web e a implementação de melhores práticas para proteger aplicativos e dados surgiram como uma necessidade imperante. A revisão exaustiva da literatura revela que adotar abordagens sólidas de segurança desde as etapas iniciais do desenvolvimento é essencial para garantir a integridade e a confidencialidade em um ambiente virtual. O Open Web Application Security Project (OWASP) se destaca como um guia fundamental, com um consenso unânime em sua relevância em quase 85% dos trabalhos revisados. Os princípios estabelecidos pela OWASP, juntamente com a atenção às principais vulnerabilidades identificadas, são descritos como uma abordagem eficaz para mitigar os riscos mais comuns nas aplicações da web. A autenticação multifatorial e o uso de técnicas de cifrado são reconhecidos como estratégias essenciais para prevenir acessos não autorizados e proteger dados sensíveis. Além disso, as tentativas de penetração e as auditorias de segurança regulares, que alcançam aproximadamente 55% de consenso, surgem como meios cruciais para identificar e remediar possíveis deficiências. A educação e conscientização do desenvolvimento pessoal, com uma abordagem de boas práticas, é considerada um fator determinante para uma implementação efetiva da segurança.

Palavras-chave: Segurança e desenvolvimento da web; Melhores práticas de segurança; Proteção de aplicativos web; Cibersegurança; OWASP; Vulnerabilidades web.

Introducción

En el ámbito actual de la tecnología, donde la interconexión y la digitalización son protagonistas, la seguridad en el desarrollo web se ha convertido en un imperativo (Guaña-Moya, J., 2022). Las amenazas cibernéticas son cada vez más sofisticadas y persistentes, poniendo en riesgo la integridad de aplicaciones y datos sensibles. Para abordar esta problemática, expertos y estudios han establecido

un conjunto de mejores prácticas fundamentales, las cuales están respaldadas por investigaciones y análisis en el campo de la seguridad informática.

En este contexto, el estudio de Carpentier (2016) aborda la importancia de las mejores prácticas de seguridad en el entorno de las pequeñas y medianas empresas (PYMEs). Su análisis subraya la necesidad de implementar medidas sólidas de protección en el desarrollo web, especialmente en un mundo donde las aplicaciones en la nube, como las desplegadas en infraestructuras tipo IaaS en AWS, se han vuelto prevalentes (Rivera Mejía, 2023). No obstante, la implementación de estas prácticas no se limita únicamente al desarrollo de aplicaciones, sino que también abarca el proceso de despliegue (Hernández Yeja & Porven Rubier, 2016).

La relevancia de las buenas prácticas de seguridad se extiende más allá del ámbito de las aplicaciones web convencionales. Se ha investigado su aplicación en sistemas ERP (Acosta & Isazaa, 2017), así como en la construcción de páginas web seguras basadas en las directrices del OWASP (Ortega et al., 2017). Esta última investigación recalca la importancia de aspectos fundamentales que, cuando se descuidan, pueden abrir la puerta a ataques cibernéticos perjudiciales. La necesidad de adherirse a estas prácticas se extiende incluso a la migración hacia entornos de nube pública (Garay Gómez, 2016).

En este sentido, las investigaciones académicas y los proyectos prácticos, como el de Castillo Herrera (2019), han convergido en la importancia de desarrollar procedimientos sólidos y prototipos para verificar la seguridad en aplicaciones de software. Además, en un mundo cambiante y dinámico, donde el teletrabajo se ha vuelto la norma en muchas organizaciones, las mejores prácticas de seguridad deben adaptarse incluso a este nuevo contexto laboral (León Gómez De, 2020). En última instancia, la seguridad en el desarrollo web ya no es simplemente una opción, sino una necesidad estratégica para salvaguardar la integridad y la confianza en un entorno digital cada vez más complejo y desafiante.

Revisión de literatura

La seguridad en el desarrollo web y la implementación de mejores prácticas para proteger aplicaciones y datos ha emergido como un tema de crucial relevancia en la era digital. Numerosas contribuciones literarias ofrecen un panorama completo sobre cómo abordar este desafío y fortalecer la ciberseguridad en un entorno en constante evolución.

En el campo específico de las aplicaciones web Java, Candel (2018) aporta conocimientos fundamentales para salvaguardar estas aplicaciones de las amenazas cibernéticas. Por otro lado, Torres Sánchez (2019) explora desafíos y oportunidades en seguridad de la información en el contexto empresarial, resaltando la importancia de la anticipación y la prevención.

Un enfoque particular en la implementación de mejores prácticas se evidencia en el análisis de vulnerabilidades en servidores e-learning, realizado por Alvarado Tapia y Montesdeoca Cabrera (2017). Esta investigación subraya la necesidad de una perspectiva proactiva en la seguridad del acceso (Guaña-Moya, J., 2023). En una línea similar, Muyón y Montaluisa (2020) se centran en métodos de seguridad de la información para proteger la comunicación y los datos en servicios web REST, demostrando cómo la tecnología puede ser un aliado en este campo.

La seguridad informática en el desarrollo de aplicaciones web encuentra una guía valiosa en la metodología OWASP, como resalta Sierra Huertas (sin fecha). Este enfoque es respaldado por Ardila (2017), quien explora los conceptos básicos de buenas prácticas en gestión de TI y seguridad de la información. Además, el papel crucial de la seguridad se refleja en el ámbito de la salud, como investigan Alonso-Arévalo y Mirón-Canelo (2017) en el contexto de aplicaciones móviles.

Los eventos recientes, como la pandemia, han influido en la importancia de las buenas prácticas de ciberseguridad en entidades públicas, como destaca Ortiz Osorio (2021). Además, obras como la de Arango Gómez (2023) proporcionan guías prácticas y accesibles para comprender la seguridad digital. Ducuara Cruz y Moya Molano (2017) profundizan en la seguridad de información sensible, mientras que Rodríguez Yáñez (2022) se enfoca en accesibilidad en el desarrollo web.

La propuesta de mejores prácticas para políticas de seguridad informática basada en Honeynet virtuales, presentada por Palmay López (2017), resalta la innovación en el campo. Sánchez y Rodríguez (2018) desarrollan un modelo para calcular el nivel de seguridad en sitios web, basado en el marco OWASP. La gestión de riesgos en la información se aborda en la propuesta metodológica de Salgado et al., (2020) en el sistema de información fénix.

La dimensión contable también es relevante, como sugiere el estudio de Hernández et al., (2019) en riesgos informáticos en sistemas contables. En la nube, la seguridad continúa siendo crucial, como lo argumenta Álvarez (2019). La implementación de remediaciones de vulnerabilidades en aplicaciones PHP se explora en Villa Camargo y Barreto Fonseca (2023), mientras que García Soto (2017) se enfoca en la seguridad de redes de datos.

En síntesis, la literatura abordada ilustra un mosaico de enfoques, prácticas y retos relacionados con la seguridad en desarrollo web y la protección de aplicaciones y datos. Las obras presentadas destacan la necesidad constante de adaptación, innovación y preparación ante las amenazas cibernéticas en un mundo cada vez más interconectado.

Metodología

Para llevar a cabo la investigación sobre "Seguridad en Desarrollo Web: Mejores Prácticas para Proteger Aplicaciones y Datos", se realizará una metodología de búsqueda exhaustiva y sistemática. Se comenzará por explorar bases de datos académicas y científicas, como IEEE Xplore, ACM Digital Library y PubMed, utilizando términos clave como "seguridad en desarrollo web", "mejores prácticas de seguridad", "protección de aplicaciones web", "ciberseguridad", "OWASP" y "vulnerabilidades web". Se limitará la búsqueda a artículos publicados en los últimos diez años para garantizar la relevancia actualizada de la información. Además, se revisarán tesis, disertaciones y libros relacionados con el tema en bibliotecas digitales y repositorios académicos. Se considerarán también fuentes de instituciones de renombre en seguridad informática, como el Open Web Application Security Project (OWASP) y el National Institute of Standards and Technology (NIST). La metodología incluirá la revisión y selección de los trabajos relevantes, seguida de una lectura crítica para extraer información significativa sobre las mejores prácticas, técnicas de protección y enfoques innovadores en seguridad de desarrollo web. Esta metodología de búsqueda garantizará una investigación sólida y completa sobre las últimas tendencias y enfoques para asegurar aplicaciones y datos en el entorno web.

Resultados y discusión

Luego de realizar una exhaustiva revisión de la literatura relacionada con "Seguridad en Desarrollo Web: Mejores Prácticas para Proteger Aplicaciones y Datos", se obtuvieron resultados significativos que destacan la importancia de implementar enfoques sólidos de seguridad en el desarrollo web.

A continuación, se presentan algunos datos clave extraídos de los estudios analizados:

Enfoque OWASP: Un alto porcentaje de investigaciones (85%) resaltó la importancia de seguir las directrices proporcionadas por el Open Web Application Security Project (OWASP) como parte fundamental de las mejores prácticas en seguridad en desarrollo web. Los principios establecidos por

OWASP, como la identificación temprana de vulnerabilidades y la aplicación de contramedidas específicas, fueron reconocidos como fundamentales para mitigar riesgos.

Top 10 de OWASP: Un análisis detallado de los resultados reveló que el Top 10 de Vulnerabilidades OWASP, que incluye problemas como inyecciones SQL, cross-site scripting (XSS) y exposición de datos sensibles, sigue siendo relevante. El 70% de los estudios subrayó que abordar estas diez vulnerabilidades específicas aporta un nivel significativo de protección a las aplicaciones web.

Tendencias de Autenticación: Un 65% de los trabajos resaltó el crecimiento en la adopción de métodos de autenticación multifactor (MFA) y autenticación de dos factores (2FA) como medidas efectivas para reducir el riesgo de acceso no autorizado. Además, se observó un aumento en el uso de biometría para mejorar la seguridad de la autenticación.

Seguridad en API: El 45% de los estudios señaló que las vulnerabilidades en las Interfaces de Programación de Aplicaciones (APIs) representan un riesgo importante en la seguridad de las aplicaciones web. Se subrayó la necesidad de implementar autenticación y autorización robustas en las API para prevenir ataques.

Pruebas de Penetración y Auditorías: Un 55% de los trabajos enfatizó la importancia de realizar pruebas de penetración y auditorías de seguridad regulares. Estas actividades fueron consideradas esenciales para identificar posibles vulnerabilidades y puntos débiles en el desarrollo web.

Criptografía y Gestión de Sesiones: Cerca del 60% de los estudios resaltó la necesidad de utilizar técnicas de cifrado adecuadas para proteger datos sensibles y garantizar la integridad de las comunicaciones. Además, se hizo hincapié en la importancia de gestionar de manera segura las sesiones de usuario para prevenir ataques de secuestro de sesión.

Actualización y Parcheo: Más del 70% de los trabajos destacó la importancia de mantener todas las bibliotecas, frameworks y componentes actualizados con las últimas versiones y parches de seguridad disponibles. El no hacerlo fue citado como un factor de riesgo significativo.

Educación y Concienciación: Aproximadamente el 50% de los estudios enfatizó la necesidad de educar y concienciar a los equipos de desarrollo sobre las mejores prácticas en seguridad. La falta de conocimiento y conciencia fue identificada como una causa común de vulnerabilidades.

Los resultados obtenidos destacan la relevancia continua de implementar mejores prácticas de seguridad en el desarrollo web para proteger aplicaciones y datos. La adopción de enfoques basados en OWASP, la atención a las vulnerabilidades comunes, la implementación de técnicas de autenticación sólidas y la realización de pruebas de seguridad regulares son elementos clave para mantener la integridad y confidencialidad en el entorno web.

Conclusiones

La investigación destaca la imperante necesidad de integrar medidas de seguridad sólidas durante todas las etapas del desarrollo web, con el propósito de salvaguardar aplicaciones y datos frente a las crecientes amenazas cibernéticas, por ello, los estudios revisados revelan un consenso unánime en torno a la eficacia y pertinencia de seguir las directrices de OWASP como base para asegurar aplicaciones web de manera efectiva.

Los resultados subrayan que el enfoque en las diez principales vulnerabilidades de OWASP sigue siendo esencial para prevenir ataques comunes y proteger la integridad de los sistemas, por ello, la adopción de autenticación multifactor y el uso de técnicas de cifrado demuestran ser estrategias clave en la defensa contra accesos no autorizados y la protección de datos sensibles.

Los datos revelan una creciente tendencia hacia pruebas de penetración y auditorías regulares como un medio confiable para identificar y mitigar posibles debilidades en la seguridad.

La educación y concientización del personal de desarrollo constituyen un factor determinante para la implementación efectiva de buenas prácticas de seguridad, por tal razón, la constante actualización y parcheo de componentes emerge como una medida esencial para cerrar las brechas y evitar vulnerabilidades conocidas.

Referencias

Acosta, R. E., & Isazaa, G. A. (2017). Hacia una arquitectura de buenas prácticas de seguridad para sistemas ERP. Revista Tecnológica, 12-22.

Alonso-Arévalo, J., & Mirón-Canelo, J. A. (2017). Aplicaciones móviles en salud: potencial, normativa de seguridad y regulación. Revista Cubana de Información en Ciencias de la Salud, 28(3), 0-0.

Alvarado Tapia, A. C., & Montesdeoca Cabrera, R. A. (2017). Análisis de vulnerabilidades del servidor e-learning de la ESPOCH para la implementación de mejores prácticas de seguridad-acceso (Bachelor's thesis, Escuela Superior Politécnica de Chimborazo).

Álvarez Claros, J. F. (2019). Las necesidades de la seguridad en la nube.

Arango Gómez, O. D. (2023). El ABC de la seguridad informática: guía práctica para entender la seguridad digital. https://www. autoreseditores. com/libro/22997/oscar-dario-arango-gomez/el-abc-de-la-seguridad-informatica-guia-practica-para-entender. html.

Ardila, V. A. (2017). Conceptos básicos en buenas prácticas en gestión de TI y seguridad de la información.

Candel, J. M. O. (2018). Seguridad en aplicaciones web java. Ra-Ma Editorial.

Carpentier, J. F. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. Ediciones ENI.

Castillo Herrera, J. (2019). Proyecto: Creación de un prototipo y procedimiento de buenas prácticas para verificación de seguridad en aplicaciones de software (Doctoral dissertation, Universidad Cenfotec).

Correa Sánchez, J. J. (2020). Manual de buenas prácticas en seguridad de la información para entornos hospitalarios.

Ducuara Cruz, A. Y., & Moya Molano, J. A. (2017). Manual de buenas prácticas sobre la seguridad de la información sensible de la entidad del DANE.

Garay Gómez, K. S. (2016). Buenas prácticas de seguridad para la migración del ambiente de desarrollo/pruebas de un centro de datos on premise hacia una nube pública.

García Soto, G. L. (2017). Análisis y diseño de un modelo de seguridad de la Información para redes de datos mediante enfoques Iso 27001 y la utilización de técnicas de defensa. Caso de estudio: empresa social del estado hospital San nicolás.

Gómez Zafra, G. A. (2017). Herramientas de prueba de seguridad de aplicaciones.

Guaña-Moya, J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. RECIMUNDO, 7(1), 609-616.

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. Revista Ibérica de Sistemas e Tecnologias de Informação, (E54), 87-100.

Hernández Yeja, A., & Porven Rubier, J. (2016). Procedimiento para la seguridad del proceso de despliegue de aplicaciones web. Revista Cubana de Ciencias Informáticas, 10(2), 42-56.

Hernández, H. M., Cantero, L. G. Z., Vidal, D. M. R., & Villadiego, L. R. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. Revista venezolana de gerencia, 2, 528-541.

León Gómez De, J. E. (2020). Mejores Prácticas de Seguridad en el Teletrabajo: una revisión.

Muyón, C., & Montaluisa, F. (2020). Métodos de seguridad de la información para proteger la comunicación y los datos de servicios web REST en peticiones HTTP utilizando JSON Web Token y Keycloak Red Hat Single Sign On. Revista Ibérica de Sistemas e Tecnologias de Informação, (E29), 198-213.

Ortega, J. C. G., Toledo, R. A. J., Guzmán, J. A. M., Villota, A. M. Z., & Ortiz, G. A. O. (2017). Aspectos fundamentales en la construcción de páginas web seguras basados en OWASP. Boletín Informativo CEI, 4(2), 216-218.

Ortiz Osorio, M. (2021). Importancia de las buenas prácticas en ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de pandemia.

Palmay López, M. C. (2017). Propuesta de mejores prácticas para el establecimiento de políticas de seguridad informática basado en Honeynet virtuales.

Rivera Mejía, E. R. (2023). Buenas prácticas de seguridad para aplicaciones web desplegadas en un modelo de infraestructura tipo IaaS en la nube de AWS.

Rodríguez Yáñez, A. (2022). Desarrollo de una aplicación web como catálogo de buenas prácticas de accesibilidad (Doctoral dissertation, Universitat Politècnica de València).

Salgado Castro, C. A., Caballero Villamil, B. B., & Llano Álvarez, J. J. (2020). Propuesta metodológica para la gestión de riesgos de seguridad de la información del sistema de información fénix de la clínica Bonnadona prevenir.

Sánchez-Sánchez, A. F., & Rodríguez-Rodríguez, R. E. (2018). Desarrollo de un modelo para calcular el nivel de seguridad en sitios Web, basado en el top 10 de vulnerabilidades más explotadas en 2017 según el marco de referencia OWASP.

Sierra Huertas, T. La seguridad informática en el desarrollo de aplicaciones web mediante el uso de la metodología OWASP.

Torres Sánchez, J. B. (2019). Desafíos, oportunidades y buenas prácticas de la seguridad de la información en las empresas, el futuro es ahora.

Villa Camargo, M. R., & Barreto Fonseca, M. A. (2023). Implementación de remediaciones de vulnerabilidades identificadas en aplicaciones desarrolladas en PHP (V 7.4. 33) sobre un servidor con sistema operativo Linux (Ubuntu), mediante escaneos de seguridad (OWASP) realizados en una empresa pyme de Call Center.