Journal Business Science vol. 3 No. 2 (2022) 1 - 8

JBS JOURNAL BUSINESS SCIENCE

Journal Business Science

https://revistas.uleam.edu.ec/index.php/business_science

ISSN electrónico 2737-615X

VULNERABILIDADES EN LOS SISTEMAS INFORMÁTICOS OWASP TOP 10: REVISIÓN BIBLIOGRÁFICA

VULNERABILITIES IN COMPUTER SYSTEMS OWASP TOP 10: BIBLIOGRAPHIC REVIEW

Karen Barbarita Álava Zambrano[1]; Willians Eduardo Basurto Vidal[2], Roberth Ronaldo Tóala Vera[3]

Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix Lopez"[1,2,3] Manabí, Ecuador

karen.alava@espam.edu.ec[1]; Willians.basurto@espam.edu.ec[2]; Roberth.toala@espam.edu.ec[3]

Karen Barbarita Álava Zambrano[1] https://orcid.org/0000-0001-8852-9598
Willians Eduardo Basurto Vidal[2] https://orcid.org/0000-0001-7293-621X
Roberth Ronaldo Tóala Vera[3] https://orcid.org/0000-0001-6499-6255

Recibido: 5/ 08/2022 **Aceptado:** 28/10/2022

Código Clasificación: C88; O33; D83; M15

RESUMEN

La presente investigación tiene por objetivo realizar una revisión bibliográfica de las "Vulnerabilidades de los sistemas informáticos OWASP Top 10". En la actualidad cualquier computadora conectada a internet está expuesta a diversas amenazas y, como consecuencia, también ha aumentado el número de ataques informáticos. Para prevenirlos, es necesario actuar de manera anticipada, detectando las vulnerabilidades potenciales que puedan ser aprovechadas por los atacantes. El trabajo objeto de estudio está enfocado en describir las características y condiciones de los tipos de vulnerabilidades. Para lo cual, se llevó a cabo el método investigativo, orientado en Open Web Security Proyect (OWASP), que se enfoca en identificar riesgos y proporcionar a la vez información sobre la probabilidad y el impacto técnico, utilizando esquema OWASP-Top-10-2021; por otra parte, se especifica en los resultados, el control para las vulnerabilidades, y para concluir, se describirá un listado de recomendaciones de seguridad para los sistemas informáticos.

Palabras clave: Vulnerabilidades, Sistemas informáticos, Top 10 OWASP, Seguridad, Ataque.

ABSTRACT

The purpose of this research is to carry out a bibliographic review of the "OWASP Top 10 Computer System Vulnerabilities". Nowadays, any computer connected to the Internet is exposed to various threats and, as a consequence, the number of computer attacks has also increased. To prevent them, it is necessary to act in advance, detecting potential vulnerabilities that can be exploited by attackers. The work under study is focused on describing the characteristics and conditions of the types of vulnerabilities. For which, the research method was carried out, oriented in Open Web Security Project (OWASP), which focuses on identifying risks and providing information on the probability and technical impact, using OWASP-Top-10-2021 scheme; on the other hand, the control for vulnerabilities is specified in the results, and to conclude, a list of security recommendations for computer systems will be described.

Keywords: Vulnerabilities, Computer systems, Top 10 OWASP, Security, Attack.

INTRODUCCIÓN

Los sistemas informáticos se enfrentan a numerosas amenazas y ciberataques. Identificar y analizar las vulnerabilidades de seguridad en los sistemas informáticos es una tarea importante para proteger estos sistemas. Los atacantes pueden explotar vulnerabilidades para comprometer la seguridad de un sistema informático (Cuevas et al., 2018). Los atacantes pueden usar estas vulnerabilidades para obtener acceso no autorizado a los sistemas, modificar o destruir datos o lanzar ataques de denegación de servicio. Hay muchas herramientas y técnicas disponibles para realizar este análisis.

Los desarrollos tecnológicos que ha traído Internet y sus múltiples aplicaciones han creado una generación que se enfrenta constantemente a retos, creando habilidades y actitudes relacionadas con el uso de las tecnologías digitales y el refuerzo diario de nuevas habilidades para facilitar su entrada en la sociedad del conocimiento (Domínguez Castillo et al, 2019). Sin embargo, junto con estos desarrollos, han surgido amenazas en una variedad de formas que son cada vez más difíciles de identificar, comprometiendo la seguridad de los usuarios que carecen de la capacitación suficiente para identificarlas, aislarlas o evitarlas en una situación tan peligrosa. Estas cosas, en la mayoría de los casos, tienen un impacto en la vida humana y pueden causar daños significativos (Díaz, 2019).

Galarza (2020) define que The Open Web Application Security Proyect (OWASP) es un proyecto de seguridad de aplicaciones web de código abierto que identifica las causas del software no seguro. Ofrece el top 10 sobre los riesgos más importantes en aplicaciones web con el objetivo principal de capacitar a desarrolladores, diseñadores, arquitectos, administradores y organizaciones.

De acuerdo con Loaiza (2017) OWASP Top 10 se enfoca en identificar los riesgos más serios para una amplia gama de organizaciones. Para cada uno de estos riesgos, brindamos información sobre la probabilidad general y el impacto técnico utilizando un esquema de puntuación simple, basado en la Metodología de evaluación de riesgos de OWASP.

Seguridad informática

La seguridad informática es la responsable de la seguridad del entorno informático, según Romero et al. (2018), la informática es la ciencia que se ocupa de los procesos, técnicas y métodos de procesamiento, almacenamiento y transmisión de la información, mientras que la seguridad de la información no se ocupa únicamente de los medios informáticos, le importa todo lo que pueda contener información, en fin, esto quiere decir que le importa casi cualquier cosa, lo que lleva a afirmar que hay algunas diferencias, pero la más relevante es el universo. El sustrato es gestionado por cada concepto en un entorno informático (Briones, 2018).

La seguridad informática se puede definir como el área encargada de proponer y diseñar reglas, procedimientos, métodos y técnicas para garantizar que el sistema de información sea seguro, confiable y sobre todo su disponibilidad. La tecnología de la información ahora está abrumada con toda la información posible, pero la información por sí sola sigue siendo un mundo más grande y, en muchos casos, más complejo de administrar, ya que en muchos casos los procesos no son manejados por las personas involucradas (Molina & Orozco, 2020).

La tarea principal de la seguridad informática es reducir los riesgos, en este caso proviene de varias partes, puede provenir de la entrada de datos, los medios de transmisión de información y los equipos utilizados para transmitir y recibir información, e incluso usuario por el mismo protocolo. Se ha implementado, pero la tarea principal siempre es reducir los riesgos para una mejor y mayor seguridad (Fernández, 2015).

Vulnerabilidad

Como menciona Torres (2021) una vulnerabilidad de seguridad es una falla o debilidad en un sistema de información que compromete su seguridad. Es un "agujero" que puede ser causado por un error de configuración, falta de proceso o falla de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (como los sistemas operativos) para acceder a ellos y realizar actividades ilegales, robar información confidencial o interrumpir sus operaciones.

Las vulnerabilidades de seguridad son una de las principales razones por las que una empresa tiene un ataque informático en su sistema. Es por eso que debe actualizar a las últimas versiones, aplicaciones informáticas, sistemas de seguridad y sistemas operativos, ya que estas actualizaciones contienen muchas correcciones para las vulnerabilidades descubiertas (Romero et al., 2018).

Amenazas informáticas

De acuerdo con Tarazona (2006) una amenaza informática es cualquier acto que aprovecha una vulnerabilidad para atacar o piratear un sistema informático. Las amenazas de TI empresarial provienen en gran medida de ataques externos, aunque también existen amenazas internas (como el robo de información o el abuso del sistema).

¿Qué es OWASP?

De acuerdo con Martinez (2014) el Proyecto de seguridad de aplicaciones web abiertas, u OWASP, es una organización internacional sin fines de lucro dedicada a la seguridad de aplicaciones web. Uno de los principios básicos de OWASP es que todos los documentos de OWASP están disponibles gratuitamente y son de fácil acceso en su sitio web, lo que permite a cualquier persona mejorar la seguridad de sus

aplicaciones web. Los materiales que proporcionan incluyen documentación, herramientas, videos y foros. Probablemente su proyecto más famoso es OWASP Top 10 (Rojas, 2018).

¿Qué es el OWASP Top 10?

OWASP Top 10 es un informe actualizado periódicamente que trata los problemas de seguridad de las aplicaciones web y se centra en los 10 principales riesgos. El informe fue preparado por un equipo de expertos en seguridad de todo el mundo. OWASP llama a los diez principales un "documento de concientización" y recomienda que todas las empresas incluyan informes en sus operaciones para reducir o mitigar los riesgos de seguridad (Kiuwan, 2021).

A continuación, en la tabla 1 se muestran los riesgos de seguridad recogidos en el informe OWASP Top 10 de 2021:

Tabla 1. Vulnerabilidades OWASP Top 10 2021

OWASP Top 10 2021
A01:2021 - Pérdida de Control de Acceso
A02:2021 - Fallas Criptográficas
A03:2021 - Inyección
A04:2021 – Diseño Inseguro
A05:2021 – Configuración de Seguridad Incorrecta
A06:2021 – Componentes Vulnerables y Desactualizados
A07:2021 – Fallas de Identificación y Autenticación
A08:2021 – Fallas en el Software y en la Integridad de los Datos
A09:2021 – Fallas en el Registro y Monitoreo
A10:2021 – Falsificación de Solicitudes del Lado del Servidor (SSRF)

Fuente: OWASP Top 10:2021

METODOLOGÍA

La metodología utilizada en este estudio se basa en los tipos de vulnerabilidades más comunes en los sistemas informáticos. Fueron seleccionados de la revisión bibliográfica de vulnerabilidades bajo el marco OWASP. Para cada vulnerabilidad identificada se realizó un análisis detallado de su impacto en la seguridad del sistema informático. Se identificaron los riesgos asociados a cada vulnerabilidad y se analizaron las precauciones más comunes utilizadas para explotarlas (Delgado, 2020).

El Top 10 de OWASP se utilizó para determinar el riesgo en los sistemas informáticos y establecer el control y prevención de este. El Top 10 de OWASP permitió a este artículo analizar y descubrir las vulnerabilidades de los sistemas informáticos (Salgado, 2014).

Según Arias et al. (2013) para el análisis de vulnerabilidades en los sistemas informáticos OWASP Top 10 debe contemplar los siguientes pasos:

1. Identificar el problema a tratar. En este caso, el problema a analizar será la existencia de vulnerabilidades en los sistemas informáticos y el impacto que estas pueden tener en la seguridad de la información.
2. Investigar sobre el tema. Para ello, se deberán consultar fuentes de información fiables y actuales, como libros especializados, artículos científicos, páginas web de entidades expertas, etc.
3. Analizar la información recopilada. Una vez realizada la investigación, se deberán analizar los datos obtenidos para extraer conclusiones y proponer soluciones al problema planteado.

RESULTADOS

En relación con los tipos de vulnerabilidades en los sistemas informáticos que se llevó a cabo en este artículo, referenciado con el proyecto OWASP, se muestran los resultados de la investigación, las incidencias de estas vulnerabilidades en estos últimos años en varias empresas del mundo:

- En 2019, la empresa de tecnología de la información Wipro sufrió una violación de datos debido a la vulnerabilidad A03: Inyección. Los hackers explotaron una vulnerabilidad en la aplicación web de la empresa para acceder a datos personales de los clientes.
- En 2020, la empresa de comercio electrónico Giant Eagle descubrió una vulnerabilidad A05: Configuración de Seguridad Incorrecta en su infraestructura, que resultó en una violación de datos. Los hackers utilizaron la debilidad para acceder a la información de tarjetas de crédito de los clientes.
- En 2021, la firma de servicios financieros Credit Karma sufrió una falla de seguridad A02: Fallas Criptográficas. Los hackers explotaron una vulnerabilidad en el cifrado de la empresa para acceder a los datos de los clientes, como números de tarjetas de crédito, direcciones de correo electrónico, números de teléfono y contraseñas.
- British Airways: En Sep 2018, British Airways sufrió un ataque cibernético que afectó a 380,000 pasajeros. Los ciberdelincuentes aprovecharon una vulnerabilidad OWASP Top 10 A01: 2021 - Pérdida de Control de Acceso para robar información de los clientes, incluyendo detalles de tarjetas de crédito.
- Equifax: En Sep 2017, Equifax sufrió un ataque cibernético que afectó a 143 millones de personas de todo el mundo. Los ciberdelincuentes aprovecharon una vulnerabilidad OWASP Top 10 A10: 2021 - Falsificación de Solicitudes del Lado del Servidor para robar información personal.
- Marriott: En Nov 2018, Marriott sufrió una violación de seguridad que afectó a 500 millones de personas. Los ciberdelincuentes aprovecharon una vulnerabilidad OWASP Top 10 A08: 2021 – Fallas en el Software y en la Integridad de los Datos para robar información de los clientes, incluyendo detalles de tarjetas de crédito.
- En 2020, la empresa de bienes raíces CBRE se vio afectada por una vulnerabilidad de inyección de SQL relacionada con la A03: 2021. Esto permitió a los atacantes ingresar al sistema y robar información personal y financiera de los usuarios.
- Otro caso fue el de la empresa de tecnología de la información Tata Consultancy Services, que se vio afectada por la A05: 2021. Esta vulnerabilidad permitió a los atacantes obtener acceso a los servidores internos de la empresa, lo que resultó en la filtración de datos confidenciales.

- Además, la empresa de fabricación de automóviles Tesla vio afectado su sistema por la A06: 2021, lo cual permitió a los atacantes infiltrarse en sus sistemas y robar datos de los clientes, como nombres, direcciones y números de tarjetas de crédito.

DISCUSIÓN

Las vulnerabilidades de seguridad son un problema grave en el mundo de la tecnología de la información. Existen muchos tipos de vulnerabilidades, y cada una puede presentar un riesgo distinto para la seguridad de un sistema (Pacheco et al., 2018). La Open Web Application Security Project (OWASP) es una organización que se dedica a la mejora de la seguridad de las aplicaciones web (Gutiérrez, 2022). La OWASP identifica y clasifica los principales tipos de vulnerabilidades de seguridad de las aplicaciones web. Esta clasificación puede ser útil para comprender mejor los riesgos que existen y tomar medidas para proteger los sistemas de estos ataques. Para proteger los sistemas informáticos de estas amenazas y ataques, es importante implementar medidas de seguridad adecuadas (Chuquitarco, 2018).

Como primer punto, se recomienda que los sistemas informáticos, establezcan un fortalecimiento en seguridad para salvaguardar su información y protegerla de atacantes.

Segundo punto; este artículo, brinda sustentación teórica basándose en referencias calificadas para salvaguardar activos, además, de ampliar conocimientos en la participación social digital, que abren posibilidades para tener acceso a la ciencia y especialmente a la tecnología entre las capas poblacionales privadas de la misma.

CONCLUSIONES

Este estudio ha descrito el top 10 OWASP-2021 de vulnerabilidades de seguridad en los sistemas informáticos. Estas vulnerabilidades pueden ser explotadas por los atacantes para obtener acceso no autorizado a los datos o para realizar otras acciones no autorizadas. Para proteger los sistemas informáticos contra estos ataques, es necesario identificar las vulnerabilidades de seguridad y aplicar las medidas de seguridad adecuadas. Se puede concluir que:

- Sin duda, OWASP apuesta por abrazar el cambio y fortalecer la industria implementando la seguridad desde cero. Esto dio como resultado que las nuevas categorías de "diseño inseguro" y "errores de software e información" se incluyeran en el top 10.
- Una vulnerabilidad es una amenaza potencial a la seguridad de un sistema o aplicación. Las vulnerabilidades pueden ser de diferentes tipos, y el nivel de riesgo que representan varía según el tipo de vulnerabilidad.
- Los sistemas informáticos son cada vez más vulnerables a ataques informáticos debido a su mayor conectividad.
- Los ataques informáticos pueden tener consecuencias graves, como el robo de información confidencial o el bloqueo de sistemas críticos.
- Los usuarios de sistemas informáticos deben tener cuidado al navegar por Internet y abrir archivos adjuntos de correo electrónico sospechosos, ya que pueden permitir que los atacantes en línea se infiltren en el sistema informático.

REFERENCIAS

Arias, G., Marizalde, N. y Noriega, N. (2013). *Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio-visual.* (Tesis de pregrado, Universidad Politécnica Salesiana Sede Guayaquil).

Briones, G. (2018). *Auditoría de Seguridad Del Servidor Web de La Empresa PUBLYNEXT S.A. Utilizando Mecanismos Basados en OWASP.* (Tesis de pregrado, Universidad de Guayaquil).

Chuquitarco, M. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador. *INNOVA Research Journal 3*(2.1), 122–33. doi: 10.33890/innova.v3.n2.1.2018.692.

Cuevas, J., Muñoz, R., Di Gionantonio, A., Gastañaga, I., Gibellini, F., Parisi, G., Barrionuevo, D. y Zea, M. (2018). Análisis de vulnerabilidades de sistemas web en desarrollo y en producción. En *XX Workshop de Investigadores en Ciencias de la Computación.*

Delgado, J. (2020). *Análisis de seguridad mediante metodología OWASP a redes inalámbricas en «Universidad laica Eloy Alfaro de Manabí extensión El Carmen.* https://repositorio.uleam.edu.ec. https://repositorio.uleam.edu.ec/bitstream/123456789/2068/1/ULEAM-INFOR0044.pdf

Díaz, J. (2019). Risks and Vulnerabilities of the Denial of Service Distributed on the Internet of Things. *Revista de Bioetica y Derecho (46)*, 85–100. doi: 10.1344/rbd2019.0.27068.

Domínguez Castillo, J., Cisneros Cohernour, E. y Quiñonez Pech, S. (2019). Vulnerabilidad ante el uso del internet de niños y jóvenes de comunidades mayahablantes del sureste de México. *RIDE Revista Iberoamericana para la investigación y el desarrollo educativo 10*(19). doi: 10.23913/ride.v10i19.531.

Fernández, G. (2015). *Representación del conocimiento en sistemas inteligentes.* (Tesis de pregrado, Universidad Politécnica de Madrid).

Galarza, D. (2020). *Estrategia para la evaluación de vulnerabilidades del sistema de notas de instituciones educativas utilizando técnicas de Hacking Ético. Caso de Estudio, Instituto Tecnológico Quito.* (Tesis de pregrado, Escuela Politécnica Nacional).

Gutiérrez-Oquendo, H. y Luz-o, G. (2022). Análisis de riesgos y vulnerabilidades en la educación 4.0 del proceso de enseñanza – aprendizaje. *Risk and Vulnerability Analysis in Education 4 . 0 of the Teaching - Learning Process, 16*(1), 1–10.

Kiuwan. (2021). *OWASP Top 10 for 2010.*

Loaiza, A. (2017). *Implementación de un esquema de seguridad inicial para las aplicaciones web del grupo comercial Iiasa Ecuador, usando como referencia los riesgos de seguridad.* (Tesis de pregrado, Escuela Superior Politécnica del Litoral).

Molina Marín, Y. y Guillermo Orozco, L. (2020). *Vulnerabilidades de los sistemas de información: una revisión.* https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1&isAllowed=y

Pacheco Amigo, B., Lozano Gutiérrez, J. y González Ríos, N. (2018). Diagnóstico de utilización de redes sociales: factor de riesgo para el adolescente. *RIDE Revista Iberoamericana Para La Investigación y El Desarrollo Educativo 8*(16), 53–72. doi: 10.23913/ride.v8i16.334.

Rojas, J. (2018). *Vulnerabilidades de aplicaciones web según Owasp.* http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8654/Vulnerabilidades%20de%20aplicaciones%20web%20segun%20owasp.pdf?sequence=1&isAllowed=y

Romero, M., Figueroa, G., Soraya Vera, D., Álava, J., Parrales, G., Álava, Ch., Murillo, A. y Castillo, M. (2018). *Mecanismos correctivos en seguridad informática.*

Salgado Yánez, A. (2014). *Análisis de las aplicaciones web de la Superintendencia de Bancos y Seguros, utilizando las recomendaciones top ten de OWASP para determinar los riesgos más críticos de seguridad e implementar buenas prácticas de seguridad para el De.* (Tesis de pregrado, Espe).

Tarazona, C. (2006). Amenazas informáticas y seguridad de la información. *Revista Universidad Externado de Colombia.*

Torres, D. (2021). *Informe definitivo evaluación independiente procedimiento gestión de los servicios de TI.* https://www.cgm.gov.co/cgm/Paginaweb/IP/Reportes%20de%20control%20interno%202021/Informe%20Definitivo%20Evaluacion%20Independiente%20procedimiento%20Gestion%20de%20los%20Servicios%20de%20TI%202021.pdf