Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Vulnerabilidades en aplicaciones web, amenazas y ataques
Vulnerabilities in web applications, threats and attacks

MSc. Elizabeth Alexandra Veloz Segura; MSc. Verónica Teresa Veloz Segura,.

CONFLUENCIA DE INNOVACIONES CIENTÍFICAS
Enero - junio, V°5-N°1; 2024

✓ **Recibido:** 16/02/2024
✓ **Aceptado**: 23/02/2024
✓ **Publicado:** 30/06/2024

PAIS

- Guaranda, Ecuador
- Guaranda, Ecuador

INSTITUCIÓN

- Universidad Estatal de Bolívar
- Universidad Estatal de Bolívar

CORREO:

eveloz@ueb.edu.ec
vveloz@ueb.edu.ec

ORCID:

https://orcid.org/0000-0003-4562-7619
https://orcid.org/0000-0002-1440-0115

FORMATO DE CITA APA.

Veloz, E. Veloz V. *(2024). Vulnerabilidades en aplicaciones web, amenazas y ataques. Revista G-ner@ndo, V°5 (N°1,).384 – 393.*

Resumen

En la actualidad las aplicaciones Web se han convertido en una alternativa indispensable en el manejo de la información dentro de las instituciones, es por ello que existe la necesidad de mantenerse actualizado y aprovechar todos los beneficios que ofrecen los sistemas informáticos en un ambiente web, que permiten procesar, almacenar de una manera confiable y segura, la seguridad es uno de los aspectos más importantes al momento del desarrollo de aplicaciones.El presente artículo tiene como finalidad dar a conocer las vulnerabilidades más comunes que se puede encontrar en las aplicaciones web las mismas que están expuestas a un gran número de amenazas – ataques, convirtiéndose en una debilidad y estar expuesto a riesgos que se presentan por errores en cualquiera de los componentes además una aplicación web es un objetivo mucho más atractivo para un atacante utilizan diferentes medios para suspender y penetrar en un sitio web, con resultados que van desde la paralización del rendimiento de páginas hasta filtraciones de información o las infraestructuras expuestas; hay que tener en cuenta el pilar fundamental es la seguridad de la información sea pública o privada. Una política de seguridad bien definida e implantada en una organización gestionada por procesos es la base para implantar un sistema de gestión de seguridad de la información (SGSI) que regule y gobierne los procesos y procedimientos que han de implementarse en toda organización.

Palabras clave: Seguridad, Aplicación Web, Vulnerabilidad

Abstract

Currently, Web applications have become an indispensable alternative in the management of information within institutions, which is why there is a need to stay updated and take advantage of all the benefits offered by computer systems in a web environment, which allow to process, store in a reliable and safe way.

The purpose of this article is to present the most common vulnerabilities that can be found in web applications, which are exposed to a large number of threats - attacks, becoming a weakness and being exposed to risks that are presented by errors in Any of the components besides a web application is a much more attractive target for an attacker using different means to suspend and penetrate a website, with results ranging from the paralysis of page performance to information leaks or exposed infrastructures.

Keywords: Security, Web Application, Vulnerability

Introducción

Una aplicación Web es una interfaz o conjuntos de páginas Web que interactúan con el usuario final, de esta manera permiten el acceso a la información solicitada y se toma los datos propios del modelo de negocio, así cualquier persona puede interactuar con ella desde Internet por medio de un navegador Web (Mora, 2001)

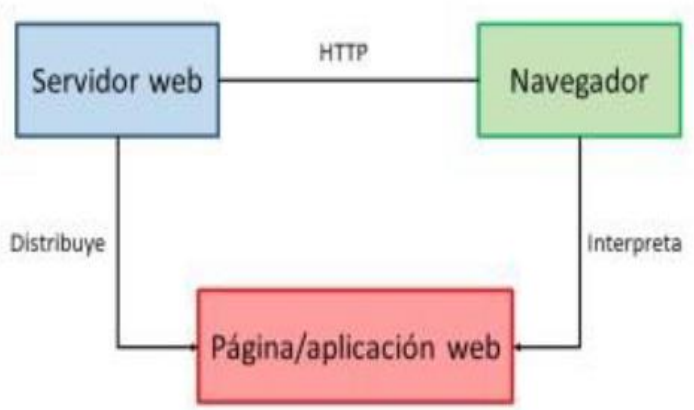

Fig1: Modelo esquemático de una aplicación web (Wiboo media, 2017)

Todas las aplicaciones web deben estar protegidas ante los posibles ataques teniendo en cuenta la seguridad como:

- Disponibilidad
- Autenticidad
- Integridad
- Confidencialidad
- Trazabilidad

Según (Luján Mora, 2002) las aplicaciones Web son aquellas herramientas donde los usuarios pueden acceder a un servidor Web a través de la red mediante un navegador

determinado. Por lo tanto, se define como una aplicación que se accede mediante la Web por una red ya sea intranet o Internet. Por lo general se menciona aplicación Web a aquellos programas informáticos que son ejecutados a través del navegador.

Las aplicaciones web son consideradas como el punto más común para los ataques informáticos debido a su fácil acceso a través de internet, muchas de ellas contienen información sensible de instituciones que mueven todos u negocio mediante una aplicación web. Una institución u organización mientras más va automatizando sus procesos mediante aplicaciones web, se vuelve más importante la necesidad de implementar seguridad en sus procedimientos e información (UNAM-CERT, 2009).

Según (Zalewski, 2012) existe una serie de principios para la seguridad en las aplicaciones web como:

- Mecanismos de autorización: Implementar un mecanismo de autorización potente para restringir el acceso a los recursos y protegerla lógica corporativa.
- Validación de los datos: Utilizar sistemas de validación de datos y validación de entradas en todos los límites de confianza, y así evitar que se exploten errores debidos al procesamiento de datos no válidos. Además de realizar validaciones en el cliente se deben realizar validaciones en el servidor.
- Cifrado de los datos: Cifrar todos los datos importantes que se envíen a través de la red.
- Utilizar servicios web: Implemente la lógica corporativa sensible mediante servicios Web.
- Utilización de tokens: Un token de larga duración se puede incluir en la página del lado de cliente para incluir en las solicitudes de servicios.

En las aplicaciones web existen vulnerabilidades como defectos o descuidos dentro del software que los atacantes realicen algo malicioso, alteren información sensible, que interrumpan

o destruyan un sistema que dan lugar a un comportamiento inesperado y típicamente indeseable, poniendo en peligro los objetivos de seguridad.

El alcance específico de la seguridad debe estar claramente definido por los interesados en términos de los activos a los que se aplica la seguridad y las consecuencias contra las que se evalúa la seguridad (Nist, Mcevilley, & Oren, 2016)

Con el aumento de las aplicaciones web disponibles y las características proporcionadas, se ha producido un aumento exponencial del número de aplicaciones web. Llegando a exponer datos privados y confidenciales, con compañías y usuarios que se dieron cuenta de que eran víctimas de un ataque (De Meo & Viganó, 2017).

El análisis de las vulnerabilidades se convierte en un objetivo primordial para el aumento de la seguridad en las aplicaciones web, el mantener medidas que no son verificados, roles sin ningún tipo de controles, desbordamientos de buffer son algunas situaciones que pueden inducir brechas de seguridad.

Aprovechando de las vulnerabilidades existentes en las aplicaciones web pueden darse ataques de diversos tipos.

- Stealing Passwords.
- Sql injection.
- Cross Site Scripting (XSS)
- Social Engineering.
- Bugs and Back Doors.
- Authentication Failures.
- Protocol Failures.
- Information Leakage.
- Exponential Attacks Viruses and Worms.

- Denial-of-Service Attacks.
- Botnets.
- Active Attacks.

Se puede decir que las vulnerabilidades más frecuentes dentro de las aplicaciones web en los últimos tres años son las vulnerabilidades relativas a inyección de código, de autenticación y gestión de sesiones y XSS (cross site scripting).

Métodos y materiales

La metodología utilizada en el presente trabajo es de carácter documental, mediante una revisión sistemática y un análisis de información, de tipo descriptivo utilizando publicaciones científicas, búsqueda de información.

Se realizó un análisis sistemático acerca de los ataques basados en vulnerabilidades que se puede presentar en la aplicación de asistencia en un ambiente web se utilizó el Test de Intrusión caja de negra (Black-box); es decir podemos diseñar las pruebas a partir de la observación de las entradas y salidas del mismo que suelen estar descriptas en los modelos funcionales (Cavalleri, 2021)

Según Morales, (2023) la investigación documental tiene la particularidad de utilizar como una fuente primaria de insumos, mas no la única y exclusiva, el documento escrito en sus diferentes formas: documentos impresos, electrónicos y audiovisuales.

El diseño de investigación se fundamenta en la revisión sistemática, rigurosa y profunda de material documental de cualquier clase y la investigación de tipo documental se concreta exclusivamente en la recopilación de información en diversas fuentes. Palella y Martins, (2010).

Con el fin de sistematizar de manera organizada la evidencia encontrada acerca de vulnerabilidades en Aplicaciones Web, amenazas y ataques, se lo realiza mediante la utilización rigurosa de una serie de métodos y técnicas de planificación, búsqueda y presentación para promover su replicabilidad. (Kitchenham, 2004)

La búsqueda se realizó en bases de datos: Scielo, Journal, Readaly, Google Scholar, Scopus, Dialnet, tomando en cuenta los descriptores como: Aplicaciones Web, vulnerabilidades, ataques, encontrándose una serie de artículos orientados a dichos descriptores.

Análisis de resultado

Una vulnerabilidad en términos de la seguridad informática es una debilidad que puede existir en un sistema informática, como una aplicación móvil, un programa de escritorio o una aplicación web. Esta debilidad se puede generar por diferentes razones, fallos en la fase de diseño, errores de programación o simplemente por carencia de procedimientos de seguridad. (El Mahjoubi, 2019). La realización de pruebas de penetración permite detectar las vulnerabilidades de los sistemas de información.

La lista de vulnerabilidades que se pueden encontrar en una aplicación web es amplia, desde Cross-Site Scripting CSS y hasta inyección SQL. Estas vulnerabilidades pueden ser explotadas por terceras personas con objetivos malignos, como por ejemplo conseguir acceso a un recurso de forma no autorizada o para hacer un ataque de denegación de servicio. (El Mahjoubi, 2019)

La seguridad de la información describe actividades relativas a la protección de la información

y los activos de la infraestructura de la información contra riesgos de pérdida, uso inadecuado, revelación o daño. (Juan C. Cuevas, 2018). En las aplicaciones web se muestra información de vital importancia, en todos los casos un portal web ofrece una ventana que ciberdelincuentes logran utilizar como un medio para un ataque; por eso resulta importante, realizar un análisis de vulnerabilidades de software que existen en las plataformas. (Gamboa Safla, 2021)

Los riesgos de seguridad de aplicaciones web más comunes según la lista OWASP (Open Web Application Security Project) Top 10 - 2017.

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

Fig2 Los diez riesgos más críticos en Aplicaciones Web (Owasp, 2017)

El objetivo era aumentar la seguridad de la aplicación web de destino que informa sobre los posibles riesgos de seguridad, que se descubrieron durante la prueba, de modo, que se puedan tomar acciones correctivas para mitigarlos.

Según Serna & Andrés (2019) Cualquier organización que expone sus servicios informáticos a redes de acceso tendrán que realizar un esfuerzo significativo para asegurar que la información y recursos estén protegidos. Internet es un factor primordial en la comunicación, sin dejar a un lado, los riesgos potenciales que se tienen en los accesos o en el mal uso de los servicios e información disponibles.

Riesgos en seguridad de aplicaciones

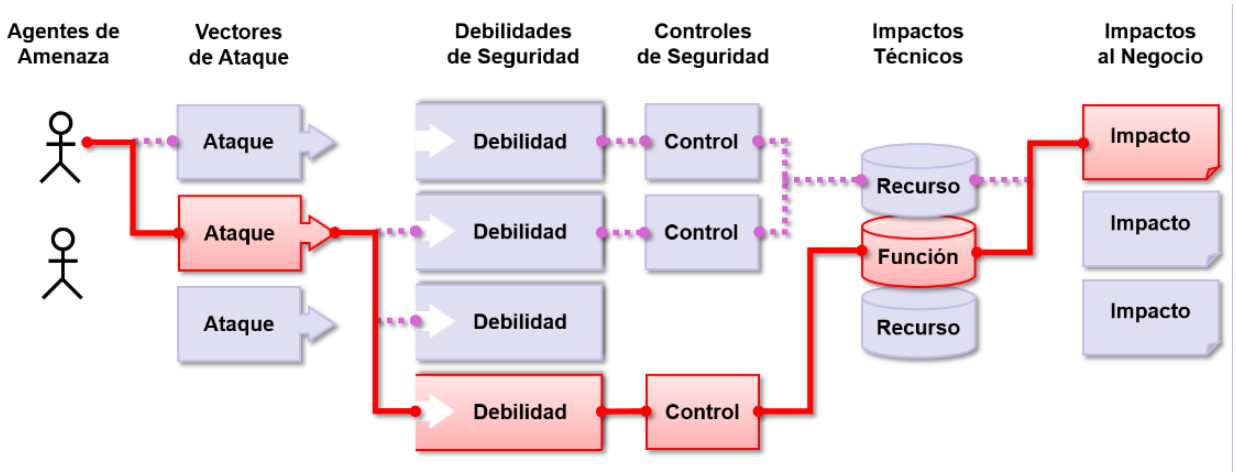

Fig3. Los diez riesgos más críticos en Aplicaciones Web (Owasp, 2017)

Según el Sistema de Gestión de la Seguridad de la Información (SGSI), toda la información almacenada y procesada por una organización está expuesta ante amenazas de ataque(por intereses comerciales, intelectuales y/o chantaje y extorsión), error (intencionado o por negligencia), ambientales (por ej. inundación o incendio), fallo en los sistemas (de almacenamiento de datos, informáticos, redes telemáticas), entre otras y también está sujeta a vulnerabilidades que representan puntos débiles inherentes a su propio uso en el ciclo de vida. (Gamboa Safla, 2021)

Conclusiones

Las vulnerabilidades son fallas en los sistemas, no son puertas abiertas diseñadas deliberadamente, sino errores de diseño, configuración o implementación que generan oportunidades de ataque, es decir que hacen viable una amenaza. Las vulnerabilidades en aplicaciones web son fallos de seguridad que pueden ser explotados por atacantes para comprometer la integridad, confidencialidad o disponibilidad de la aplicación. Estas vulnerabilidades pueden surgir en diversas capas de la aplicación y se deben abordar con medidas de seguridad adecuadas. Es esencial abordar estas vulnerabilidades mediante prácticas sólidas de desarrollo seguro, pruebas de seguridad regulares y la implementación de medidas de seguridad como cortafuegos, cifrado adecuado y controles de acceso. La conciencia y la educación sobre seguridad son también componentes cruciales para prevenir y mitigar las vulnerabilidades en aplicaciones web.

Bibliografía bibliográfica

Cavalleri, N. (2021). Pruebas de caja blanca, caja negra y caja gris. Obtenido de https://nadiacavalleri.com.ar/pruebas-de-caja-blanca-caja-negra-y-caja-gris/

De Meo , F., & Viganó, L. (2017). A Formal Approach to Exploiting Multi-Stage Attacks based on File-System Vulnerabilities of Web Applications. Obtenido de http://arxiv.org/abs/1705.03658

El Mahjoubi, O. (2019). Detección de vulnerabilidades y generación de alertas de seguridad para aplicaciones web. Obtenido de https://openaccess.uoc.edu/bitstream/10609/96087/7/oel_mahjoubiTFM0619memoria.pdf

Gamboa Safla, D. (2021). Vulnerabilidades en Aplicaciones Web utilizando la Metodología de Proyecto Abierto de Seguridad de Aplicaciones Web. Obtenido de https://repositorio.pucesa.edu.ec/bitstream/123456789/3175/1/77336.pdf

Juan C. Cuevas, R. M. (2018). Análisis de Vulnerabilidades de Sistemas Web en desarrollo y en producción. RedUNCI - UNNE .

Luján Mora, S. (2002). Programación de aplicaciones web: historia, principios básicos y clientes web. Alicante. España: Club Universitario.

Mora, S. (2001). Programación de aplicaciones web: historia, principios básicos y clientes web. Editorial Club Universitario.

Nist, R., Mcevilley, M., & Oren, J. (2016). INGENIERÍA DE SEGURIDAD DE SISTEMAS - Consideraciones para un Enfoque Multidisciplinario en la Ingeniería de Sistemas Confiables Confiables.

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

Tenable. (2014). Nessus. Obtenido de http://www.tenable.com/products/nessus

UNAM-CERT. (2009). AspectosBásicosdelaSeguridadenAplicacionesWeb.

Wiboo media. (2017). ¿Qué son las aplicaciones web? Ventajas y tipos de desarrollo web. Obtenido de https://wiboomedia.com/que-son-las-aplicaciones-web-ventajas-y-tiposde-desarrollo-web/

Zalewski, M. (2012). La Web enredada:guía para la seguridad de aplicaciones web modernas. Anaya Multimedia - Anaya Interactiva.