Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2026,
Volumen 10, Número 5.

https://doi.org/10.37811/cl_rcm.v10i5

FRAMEWORK DE SEGURIDAD PARA APLICACIONES WEB BASADO EN OWASP Y OSSTMM

SECURITY FRAMEWORK FOR WEB APPLICATIONS BASED ON OWASP AND OSSTMM

Juan Manuel Bernal Ontiveros
Instituto Tecnológico de Ciudad Juárez, México

Marisela Palacios Reyes
Instituto Tecnológico de Ciudad Juárez, México

Noé Ramón Rosales Morales
Instituto Tecnológico de Ciudad Juárez, México

Montserrat Valdez Escobedo
Instituto Tecnológico de Ciudad Juárez, México

DOI: https://doi.org/10.37811/cl_rcm.v10i5.26225

Framework de Seguridad para Aplicaciones Web basado en OWASP y OSSTMM

Juan Manuel Bernal Ontiveros[1]
Juan.bo@cdjuarez.tecnm.mx
https://orcid.org/0000-0002-3819-5750
Tecnológico Nacional de México
Instituto Tecnológico de Ciudad Juárez
México Campus I
Ciudad Juárez, Chihuahua México

Marisela Palacios Reyes
marisela.pr@cdjuarez.tecnm.mx
https://orcid.org/0000-0003-2830-5829
Tecnológico Nacional de México
Instituto Tecnológico de Ciudad Juárez
México Campus I
Ciudad Juárez, Chihuahua México

Noé Ramón Rosales Morales
noe.rm@cdjuarez.tecnm.mx
https://orcid.org/0000-0003-4526-3448
Tecnológico Nacional de México
Instituto Tecnológico de Ciudad Juárez
México Campus I
Ciudad Juárez, Chihuahua México

Montserrat Valdez Escobedo
L23111475@cdjuarez.tecnm.mx
https://orcid.org/0009-0002-1746-0284
Tecnológico Nacional de México
Instituto Tecnológico de Ciudad Juárez
México Campus I
Ciudad Juárez, Chihuahua México

RESUMEN

Las amenazas a la seguridad son hoy prioritarias, especialmente en aplicaciones web, donde las transacciones del mercado exigen proteger sistemas y garantizar confiabilidad. Por ello, las estructuras computacionales deben integrar software, herramientas y métodos más seguros, que requieran menos actualizaciones y configuraciones complejas. El enfoque en aplicaciones web demanda implementar prácticas y herramientas que mejoren la seguridad de forma medible. Es esencial reducir vulnerabilidades, detectarlas y eliminarlas para lograr rastreabilidad frente a infiltraciones malintencionadas. La complejidad de estas aplicaciones las expone a riesgos que los ciberatacantes aprovechan como objetivos atractivos. Este trabajo busca contribuir a la seguridad web aplicando métodos y herramientas conforme a las guías del Open Web Application Security Project (OWASP, 2021). La digitalización empresarial ha renovado bases de datos en línea y desarrollado aplicaciones que permiten a los usuarios acceder y capturar información confidencial. Las organizaciones están obligadas a garantizar confidencialidad y seguridad ante accesos no autorizados. Además, deben emplear estrategias de seguridad web que utilicen a los delincuentes informáticos como “trampa” para identificar lagunas en las aplicaciones y ofrecer mecanismos de rectificación (Yadav et al., 2018).

***Palabras Clave**:* vulnerabilidades, infiltraciones, intrusiones, ciberatacantes, amenaza

[1] Autor principal
Correspondencia: marisela.pr@cdjuarez.tecnm.mx

Security Framework for Web Applications based on OWASP and OSSTMM

ABSTRACT

Security threats are now a top priority, especially in web applications, where market-driven transactions demand system protection and reliability. Consequently, computational infrastructures must integrate more secure software, tools, and methods that require fewer updates and complex configurations. Focusing on web applications requires implementing practices and tools that measurably improve security. It is essential to reduce, detect, and eliminate vulnerabilities to ensure traceability against malicious intrusions. The inherent complexity of these applications exposes them to risks that cyberattackers exploit as attractive targets. This work aims to contribute to web security by applying methods and tools aligned with the Open Web Application Security Project (OWASP, 2021) guidelines. Corporate digitalization has renewed online databases and developed applications that enable users to access and capture sensitive information. Organizations are obligated to ensure confidentiality and security against unauthorized access. Furthermore, they must employ web security strategies that use cybercriminals as a “trap” to identify gaps in applications and provide remediation mechanisms (Yadav et al., 2018).

***Keywords*:** vulnerabilities; intrusions; breaches; cyberattackers, threat

Artículo recibido 20 julio 2026
Aceptado para publicación: 20 agosto 2026

INTRODUCCIÓN

A través de los años las aplicaciones web se han convertido en elementos importantes en el manejo de la información con base en el comercio electrónico, con los motores de búsqueda, en las redes sociales hasta los sitios web de alojamiento de vídeos, los cuales mejoran la vida de una manera más fácil. Es importante de mencionar que no todo es manera positiva, las aplicaciones web con los beneficios que ofrecen, vienen también acompañados de la parte negativa, entre las que se encuentran los ataques que diariamente son realizados por delincuentes cibernéticos, considerados como elementos antisociales para hacer que las experiencias con las aplicaciones web sean de modo desastroso.

Los ataques son infiltraciones no deseadas a sistemas de infraestructuras de organizaciones, empresas o instituciones y que por lo tanto realizan penetraciones a las lagunas encontradas por los ciber atacantes para acceder a la información confidencial, y así desprestigiando la aplicación web en particular. En este documento se analizará el método para prevenir las infiltraciones no deseadas para disminuir las vulnerabilidades o fallas que sean encontradas en las aplicaciones web. Las aplicaciones web han ido evolucionando recorriendo un extenso camino desde sus inicios como aplicaciones estáticas, con lo que solo se puede navegar entre páginas web hasta ser fuertemente aplicaciones dinámicas llevando a cabo transacciones demasiado complejas.

Para entender mejor las aplicaciones web, se describen en base a la arquitectura cliente-servidor lo que quiere decir que varios usuarios llamados clientes que pueden solicitar la entrada a un servidor y poder usar la base de datos para efectuar servicios solicitados por el cliente. Esta arquitectura amplia el camino provocando infiltraciones debido a las vulnerabilidades tanto en el lado del cliente como en el del servidor (Khari et al 2016).

Los ciber atacantes pueden ser un dolor de cabeza, cuando buscan vulnerabilidades en las aplicaciones web, sino también para los servicios que ofrece la web. Mostrando un ejemplo, los servicios bancarios manejan datos privados y confidenciales que cuando el atacante encuentra la manera de infiltración para acceder a ellos, pueden causar daños quizá irreversibles. Se han sugerido varias acciones para mermar la vulnerabilidad de las aplicaciones web. Se analizarán algunas medidas para idear alguna forma general para prevenir los ataques web, con el objetivo de reducir y si es posible eliminar las posibles amenazas que inducen a encontrar vulnerabilidades (Wassermann y Su, 2007).

Los delitos de alto nivel, han dejado expuesto que el método de clásico de seguridad informática, no ha sido suficientemente capaz con la protección más sólida, ni los mecanismos de defensa debidamente instalados y configurados, como firewalls, sistemas de prevención y detección de infiltraciones, así como tampoco los sólidos estándares de encriptado de extremo a extremo y software antivirus. Los delincuentes informáticos, están bien capacitados en las técnicas, métodos y herramientas para realizar la intrusión en cualquier sistema que exponga vulnerabilidades a través de las lagunas informáticas. En algunos casos, los piratas informáticos de sombrero negro pueden ejecutar ataques de manera tan perfecta que pueden comprometer un sistema, robar todo lo de valor y borrar completamente sus huellas en menos en poco tiempo. Por esto y más problemas de ataques informáticos el Consejo de la CEH (Certified-Ethical-Hacker) se dedica a detener a los ciber atacantes contrarrestando las intrusiones no autorizadas en las infraestructuras de los sistemas de las empresas u organizaciones (CENGAGE, 2017).

La utilización de la información es absolutamente necesaria para aumentar el valor agregado de las empresas y organizaciones proporcionando un excelente servicio a los usuarios que la utilizan para ser competitivos. Por tanto, se tiene que la amenaza de ataques y fugas de datos por las infiltraciones ilegales por parte de atacantes malintencionados es debido a que se ha incrementado el número de delitos informáticos relacionados con las aplicaciones web, entre tanto cada sistema conectado a la web es un blanco potencial a los ataques maliciosos, así como el nivel de ataque también se incrementa (Hariyanto & Siahaan, 2016).

El incremento de las amenazas o ataques contra las aplicaciones web, el atacante no necesita mucha experiencia o conocimiento para llevar a cabo la intrusión en una aplicación web que no tiene una protección muy sólida. Si bien los ataques comunes, como los scripts entre sitios y la inyección SQL tienen mucho tiempo de existir, también se siguen descubriendo constantemente nuevos *exploits* (software que ataca una vulnerabilidad) que hacen que las empresas necesiten una mayor seguridad (Bitdefender, 2023).

DESARROLLO

Descripción del Problema

Existen una gran variedad de problemas que afectan a las aplicaciones web, por lo que también convergen en la existencia de intrusiones que son muy comunes entre la mayoría de ellas, y por tanto

son explotadas por los delincuentes informáticos que son expertos y noveles. Las intrusiones de las aplicaciones web dejan al descubierto las vulnerabilidades para los delincuentes en obtener un control no autorizado de un código fuente, manipular la información confidencial e interrumpir el buen funcionamiento normal de la aplicación y así realizando desastres. Ante lo descrito existen resultados que son muestra de los análisis que son explicados y reconocidos en la fundación OWASP top 10, MITRE Common Weakness Enumeration, SANS top 20 Attack Targets y WASC Web Application Security Statistics Project (OSSTMM, 2023).

La fundación OWASP es un proyecto abierto de seguridad de aplicaciones web y es una organización internacional que no tiene el beneficio del lucro y está dedicada a la seguridad de las aplicaciones web, las cuales son un factor importante para cualquier empresa u organización. También muestra como aprender sobre las vulnerabilidades más comunes de las aplicaciones web y cómo se pueden mitigar. Entre los principios en los que se basa OWASP, es tener disponible gratuitamente en el portal web del como poder mejorar la seguridad de una aplicación web (OWASP, 2017). Entre los materiales que ofrece se incluyen documentación, herramientas, vídeos y foros. Por lo que el proyecto más conocido es el de mostrar OWASP Top 10, la cual es la lista del Open Web Application Security Project, y que también es la que describe los problemas de seguridad de las aplicaciones web más frecuentes y que a continuación se enlistan (Sánchez, 2018):

1. Cross Site Scripting (XSS)
2. Problemas de inyección de código
3. Ejecución maliciosa de código
4. Referencias directas inseguras a objetos
5. Cross Site Request Forgery (CSRF)
6. Fuga de información y gestión de errores inapropiada
7. Problemas de autenticación y gestión inapropiada de sesiones
8. Almacenamiento criptográfico inseguro
9. Comunicaciones inseguras
10. Fallos en la restricción de acceso mediante URL.

Hay que destacar que, en la lista anterior, cada año puede variar la posición de cada ataque, inclusive tener en la lista vulnerabilidades que no habían figurado en el OWASP Top 10. Aunque en la lista anterior existan ataques que se encuentren o no, deben ser tomados con suma importancia debido a que siguen siendo problemas que afectan a la seguridad en las aplicaciones web, considerándolos como prioridad, y que cuando son detectados deben ser afrontados en el desarrollo y la explotación en este tipo de ataques.

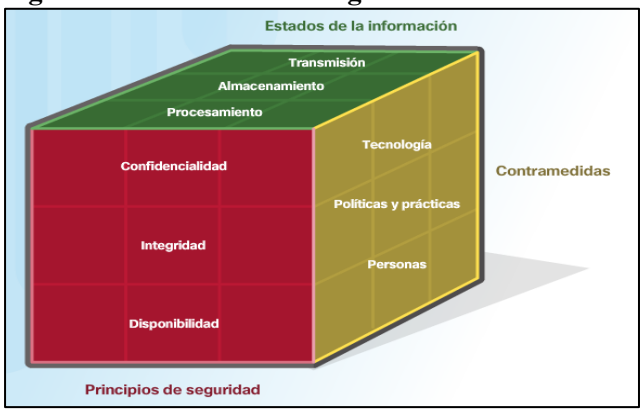
JUSTIFICACIÓN

En el avance y desarrollo de la web como un medio de comunicación, ha generado un incremento de exposición de la información al compartirla entre aplicaciones por medio de transacciones, y donde los criminales informáticos pueden encontrar un punto de intrusión ante las vulnerabilidades que comprometen la confidencialidad de los datos, fracturando la seguridad de las aplicaciones web. Esta trasgresión deja al descubierto los espacios débiles ante cualquier tipo de ataque y denegación de servicio. La finalidad de este trabajo es el del escaneo para encontrar las posibles infiltraciones, reforzando las lagunas que hayan sido localizadas ante los posibles ataques de los ciberdelincuentes. La protección será llevada a cabo por medio de las actuales herramientas disponibles para la comprensión, prevención, solución o mitigación de las amenazas, adoptando diversos enfoques, métodos y estrategias. Según el documento que expone (Naudi, 2016), las organizaciones están bajo intensa presión para entregar aplicaciones y servicios web para satisfacer las demandas de los clientes de las aplicaciones digitales modernas. Por lo anterior descrito la seguridad en aplicaciones web aún no está a la par con el ciclo de desarrollo, y esto amplía la superficie de una amenaza. Actualmente existe un número considerable de vulnerabilidades potenciales que son explotados por atacantes cibernéticos y por lo tanto las organizaciones tienen que tener en cuenta el significado de una vulnerabilidad de alta gravedad, lo que puede posibilitar a un atacante obtener acceso no autorizado a los sistemas y datos potencialmente confidenciales de clientes, datos de salud y secretos comerciales. A lo que también podría aumentar mucho más la trasgresión a otras aplicaciones web, trasladándose a otros sistemas para escalar el ataque aún más.

Objetivo

La seguridad tradicional como la moderna, tienen como objetivo mejorar las tres dimensiones (tres principios) de la ciberseguridad: la confidencialidad, la integridad y la disponibilidad de la información, siendo la confidencialidad el parámetro de seguridad de mayor influencia.

Figura 1 Cubo de la ciberseguridad.



Fuente: Imagen descargada de https://i-networks.com.mx/el-cubo-de-la-ciberseguridad/

Además, será consultado el sitio de la fundación OWASP como apoyo para establecer mecanismos de protección que permitan la detección, disminución y control de las diferentes amenazas y vulnerabilidades que puedan manifestar las Aplicaciones Web para fracturar la seguridad. También se debe implementar una la creación de una política de seguridad informática que permita incorporar controles que protejan y sostengan las aplicaciones web con mayor seguridad y así se aprenderá de los diferentes tipos de amenazas ocasionando que se desarrollen mecanismos y medidas de defensa ante los ciberataques.

METODOLOGÍA

En esta sección trataremos la implementación de la metodología a usar, y la cual consiste en tener la información como primer requisito para poder entender y conocer la situación de vulnerabilidad de la seguridad de las aplicaciones web, enfocando la información obtenida a prevenir y corregir las fallas ante los ataques mediante la activación de métodos, técnicas y herramientas que aminorar y controlar y si es preciso la erradicación de los riesgos y vulnerabilidades (González, 2018).

Y es de esta manera que a continuación se describen las fases en detalle:

- **Fase 1:** Contextualizar la importancia de la seguridad en base a los diferentes conceptos, técnicas y acciones que hacen parte de la Seguridad en las Aplicaciones Web.

- **Fase 2:** Consultar mecanismos de protección de las aplicaciones web, apoyándose en metodologías que propicien la detección, reducción y control de la gran variedad de riesgos y vulnerabilidades que surgen de las aplicaciones web, y estas metodologías son:
  - OSSTMM (acrónimo de *Open Source Security Testing Methodology Manual*, metodología desarrollada por *ISECOM* para llevar a cabo pruebas, análisis y mediciones de la seguridad operativa real. Por lo que es una metodología para ejecutar auditorías técnicas de seguridad (OSSTMM, 2023)).
  - OWASP (Es el acrónimo en inglés de Open Web Application Security Project, "Proyecto abierto de seguridad de aplicaciones web") es un proyecto de código abierto enfocado a diagnosticar y enfrentar ataques que causan la ruptura de la seguridad de las aplicaciones web. OWASP es un organismo sin el interés del beneficio, apoyando y gestionando proyectos e infraestructuras de OWASP (OWASP, 2021).
- **Fase 3:** Identificación de la diversidad de riesgos, amenazas y ataques que surgen de las aplicaciones web.
- **Fase 4:** Implementación de la metodología que denote el uso de métodos de protección, disminución de riesgos, amenazas y vulnerabilidades que surjan de la rastreabilidad de las aplicaciones web.
- **Fase 5:** Se debe de establecer el uso de la metodología para crear una política de seguridad de la información incorporando los controles necesarios que puedan preservar la seguridad de las aplicaciones web.

Figura 2 Fases de la Metodología.



RESULTADOS Y DISCUSIÓN

Desafíos de la seguridad de las aplicaciones web

Las soluciones de protección a las aplicaciones web en base a la activación de métodos y herramientas obtenidos del portal de la fundación del proyecto OWASP (Open Web Application Security Project) y de la metodología OSSTMM (acrónimo de Open Source Security Testing Methodology Manual) para combatir cualquier tipo de ataque contra aplicaciones web, desde DDoS (Denegación de servicio) hasta inyección SQL, basadas en el top 10 de OWASP de las aplicaciones web.

No obstante, uno de los principales desafíos que conllevan los programas contra ataques como los antivirus y firewalls, son el de que los responsables de implementar las protecciones de seguridad deben analizar y adaptarse constantemente a cambios de las aplicaciones y que van desde la evolución de los ataques hasta las actualizaciones que deben estar disponibles, basándose en la disponibilidad con relación al crecimiento de las amenazas, y por otra parte las contramedidas suelen ser un proceso manual, que requieren demasiado tiempo de trabajo, para que estén a la par de los ataques técnicamente. Las políticas de seguridad cuando tienden a ser obsoletas pueden convertirse en un dolor de cabeza, exponiendo la precisión de las alertas de ataques, confundiendo la diferencia entre los ataques falsos y los reales. Aunado a lo anterior también es posible que aquellos que son encargados de la seguridad no sean aptos en aplicar de forma eficiente las normas, provocando que las protecciones sean desactivadas y la infraestructura del sistema de una empresa se vea comprometido a un mayor riesgo y solo por el temor al que los usuarios que son autorizados sean afectados en la interrupción de sus actividades.

Amenazas de las aplicaciones web y contramedidas

Un buen método para analizar las amenazas es el de clasificarlas por aplicación, al organizarlas se muestra una mejor manera de identificar cada amenaza por lo tanto categoriza las vulnerabilidades de las mismas aplicaciones, la *Tabla 1* describe de forma resumida la categoría y las amenazas que las afectan (Curphey et al., 2003).

El incremento de las amenazas o ataques contra las aplicaciones web permiten que los atacantes no necesiten mucha experiencia o conocimiento para atacar e la intrusión en una aplicación web que tiene fallas muy débiles en cuanto a la protección se refiere o no tiene ninguna.

Si bien los ataques comunes, como los scripts entre sitios y la inyección SQL tiene mucho tiempo de existencia, también se siguen descubriendo constantemente nuevos *exploits* (software que ataca una vulnerabilidad) que hacen que las empresas necesiten una mayor seguridad (Bitdefender, 2023).

Tabla 1 Amenazas por categoría de vulnerabilidad de la aplicación.

Categoría	**Amenazas**
Validación de entrada	Desbordamiento de búfer; secuencias de comandos entre sitios; Inyección SQL; canonicalización
Autenticación	Escuchas en la red; ataques de fuerza bruta; ataques de diccionario; repetición de cookies; robo de credenciales
Autorización	Elevación de privilegios; divulgación de datos confidenciales; manipulación de datos; ataques de señuelo
Administración de la configuración	Acceso no autorizado a interfaces de administración; acceso no autorizado a almacenes de configuración; recuperación de datos de configuración en texto claro; falta de responsabilidad individual; cuentas de proceso y servicio con privilegios excesivos
Datos sensibles	Acceso a datos confidenciales almacenados; escuchas en la red; manipulación de datos
Administración de sesiones	Secuestro de sesión; repetición de sesión; hombre en el medio
Criptografía	Mala generación o gestión de claves; encriptado débil o personalizado
Manipulación de parámetros	Manipulación de cadenas de consulta; manipulación de campos de formulario; manipulación de cookies; Manipulación del encabezado HTTP
Gestión de excepciones	Divulgación de información; negación de servicio
Auditoría y registro	El usuario niega haber realizado una operación; el atacante explota una aplicación sin dejar rastro; El atacante cubre sus huellas.

DISCUSIÓN

El trabajo analiza la importancia de establecer un framework de seguridad para aplicaciones web mediante la integración de OWASP y OSSTMM. El tema resulta pertinente porque las aplicaciones web constituyen actualmente una infraestructura esencial para el comercio electrónico, los servicios bancarios, las redes sociales y la gestión institucional de información.

Sin embargo, su creciente complejidad también amplía la superficie de ataque y expone tanto al cliente como al servidor a riesgos relacionados con la confidencialidad, integridad y disponibilidad de los datos.

Discusión del Tema

Uno de los principales aportes del documento consiste en reconocer que la seguridad de una aplicación web no puede depender exclusivamente de herramientas tradicionales como antivirus, firewalls o sistemas de detección de intrusiones. Aunque estos mecanismos son necesarios, resultan insuficientes cuando se aplican de manera aislada o cuando no se actualizan conforme evolucionan las amenazas. La seguridad debe abordarse como un proceso continuo que incluya análisis, pruebas, prevención, monitoreo y corrección.

En este sentido, la incorporación conjunta de OWASP y OSSTMM representa una propuesta metodológica complementaria. OWASP proporciona conocimientos, prácticas y referencias específicas sobre las vulnerabilidades más comunes en aplicaciones web, mientras que OSSTMM permite orientar la evaluación técnica de la seguridad mediante pruebas y mediciones. Por lo tanto, OWASP ayuda a identificar qué debe revisarse y OSSTMM contribuye a definir cómo evaluar la seguridad de manera estructurada.

El documento también destaca que muchas vulnerabilidades no se originan únicamente en fallas técnicas, sino en deficiencias de configuración, administración, capacitación y aplicación de políticas. Por ejemplo, una aplicación puede contar con mecanismos de protección, pero seguir siendo vulnerable si mantiene contraseñas débiles, permisos excesivos, sesiones mal administradas, datos sin cifrar o registros insuficientes. Esto demuestra que la seguridad debe considerarse desde el diseño y durante todo el ciclo de vida del software.

Otro aspecto importante es la clasificación de las amenazas por categorías: validación de entradas, autenticación, autorización, administración de la configuración, datos sensibles, sesiones, criptografía, manipulación de parámetros, gestión de excepciones y auditoría. Esta organización facilita el análisis porque permite relacionar cada componente de la aplicación con los posibles ataques que podría recibir. Así, vulnerabilidades como la inyección SQL y el Cross-Site Scripting se vinculan con una validación deficiente de datos, mientras que el secuestro de sesión se relaciona con controles insuficientes en la administración de sesiones.

Discusión de los Resultados

Los resultados presentados son principalmente de carácter metodológico y conceptual. El trabajo identifica las amenazas más relevantes y propone un conjunto de fases para fortalecer la seguridad de las aplicaciones web:

1. Contextualizar la importancia de la seguridad web.
2. Consultar y aplicar mecanismos de protección basados en OWASP y OSSTMM.
3. Identificar riesgos, amenazas y ataques.
4. Implementar medidas para reducir y controlar las vulnerabilidades.
5. Establecer políticas de seguridad de la información.

La principal conclusión derivada de estas fases es que la seguridad debe gestionarse de manera sistemática. No basta con realizar un escaneo ocasional o corregir una vulnerabilidad aislada; es necesario integrar las pruebas de seguridad en el desarrollo, la implementación, la operación y el mantenimiento de la aplicación.

La tabla de amenazas constituye uno de los resultados más útiles del estudio, ya que muestra que los riesgos abarcan diferentes dimensiones del sistema. La validación de entradas, por ejemplo, puede verse afectada por desbordamientos de búfer, inyección SQL y XSS. La autenticación puede ser comprometida mediante ataques de fuerza bruta, robo de credenciales o repetición de cookies. Por su parte, una autorización deficiente puede permitir la elevación de privilegios o el acceso a información confidencial.

Estos resultados evidencian que las vulnerabilidades están interrelacionadas. Una falla en la autenticación puede facilitar el acceso no autorizado; posteriormente, una autorización deficiente puede permitir que el atacante consulte o modifique información; finalmente, una auditoría insuficiente puede impedir detectar o reconstruir el incidente. Por ello, la protección debe aplicarse en varias capas y no concentrarse en un único mecanismo de defensa.

El trabajo también identifica como desafío la actualización constante de las medidas de protección. Las amenazas evolucionan, aparecen nuevas vulnerabilidades y las aplicaciones cambian con frecuencia. En consecuencia, las políticas, herramientas y procedimientos que fueron adecuados en un momento determinado pueden volverse obsoletos.

Además, el documento señala que los procesos manuales pueden consumir mucho tiempo y generar errores, especialmente cuando no existe personal suficientemente capacitado para interpretar las alertas y aplicar las medidas correctivas.

Valoración Crítica

Aunque el trabajo ofrece una visión amplia y pertinente sobre la seguridad de las aplicaciones web, sus resultados podrían fortalecerse mediante evidencia empírica. El documento explica las amenazas, presenta metodologías y propone recomendaciones, pero no muestra resultados cuantitativos obtenidos a partir de la evaluación de una aplicación específica. Por ejemplo, sería conveniente incluir:

- Número de vulnerabilidades detectadas antes y después de aplicar el framework.
- Clasificación de los hallazgos por nivel de riesgo.
- Tiempo requerido para identificar y corregir cada vulnerabilidad.
- Herramientas utilizadas durante las pruebas.
- Porcentaje de reducción de vulnerabilidades.
- Comparación entre una evaluación inicial y una evaluación posterior.

La ausencia de estos datos limita la posibilidad de medir directamente la eficacia del framework. Por tanto, los resultados deben interpretarse como una propuesta de orientación metodológica y no como una validación experimental completa. Para demostrar su efectividad, sería recomendable aplicar el framework a una o varias aplicaciones web reales, documentar el proceso y comparar los resultados antes y después de la intervención.

También sería conveniente actualizar y precisar algunos conceptos. El documento presenta una lista de vulnerabilidades asociada al OWASP Top 10, pero las categorías de OWASP han evolucionado entre distintas ediciones. Por ello, en una versión final del estudio sería importante indicar claramente qué edición se utiliza y diferenciar entre categorías actuales, vulnerabilidades históricas y amenazas complementarias. Esto evitaría confusiones y permitiría relacionar con mayor precisión cada hallazgo con los controles correspondientes.

Implicaciones prácticas

Los resultados tienen implicaciones importantes para las organizaciones. La adopción del framework puede ayudar a:

- Incorporar la seguridad desde las primeras etapas del desarrollo.
- Detectar vulnerabilidades antes de que sean explotadas.
- Priorizar los riesgos según su impacto.
- Mejorar los controles de autenticación y autorización.
- Proteger los datos sensibles mediante cifrado.
- Fortalecer la administración de sesiones.
- Mantener registros que permitan investigar incidentes.
- Establecer políticas de actualización, respaldo y respuesta ante incidentes.

Las recomendaciones del documento —actualizar las aplicaciones, fortalecer los controles de acceso, realizar pruebas periódicas, validar los datos de entrada, cifrar la información sensible y mantener copias de seguridad— son coherentes con los riesgos identificados. No obstante, su eficacia depende de que se conviertan en procedimientos verificables, con responsables, calendarios, indicadores y revisiones periódicas.

CONCLUSIONES

El estudio sostiene correctamente que la seguridad de las aplicaciones web debe entenderse como un proceso permanente y multidimensional. La combinación de OWASP y OSSTMM ofrece una base útil para identificar vulnerabilidades, realizar pruebas técnicas y establecer controles de protección. Los resultados muestran que los principales riesgos se relacionan con la validación de entradas, la autenticación, la autorización, la gestión de sesiones, la criptografía, la configuración y la auditoría.

Sin embargo, para consolidar la propuesta sería necesario complementarla con una aplicación práctica y resultados cuantificables. En su estado actual, el trabajo proporciona un marco conceptual y metodológico sólido, pero su eficacia quedaría mejor demostrada mediante un estudio de caso que evidencie la reducción real de vulnerabilidades. En conjunto, la investigación confirma que la seguridad debe integrarse al ciclo de vida de las aplicaciones web y asumirse como una responsabilidad compartida entre desarrolladores, administradores, especialistas de seguridad y la organización.

Para establecer el buen funcionamiento de las aplicaciones web se debe tener un cimiento bien fortalecido como característica fundamental de la seguridad de las mismas.

Ante los ataques de los cibercriminales que desean encontrar infiltraciones a través de las vulnerabilidades de algún sistema, intentando causar disminución del uso, popularidad y aceptación por el lado de los usuarios que regularmente obtienen algún servicio, provocando que las aplicaciones llegasen con el tiempo a su final de vida. La manera más conveniente de implementar la seguridad de las aplicaciones web, es el de dotar de conocimiento de las vulnerabilidades más frecuentes, analizarlas en publicaciones conocidas del tema, y llevando a cabo las acciones pertinentes como la prevención y protección ante las intrusiones no deseadas para evitar que la aplicación sea susceptible a las fallas de seguridad ya conocidas. Aunque existen muchas vulnerabilidades, algunas definitivamente son más importantes que otras, de aquí que el diseño y desarrollo de herramientas para detectarlas y corregirlas, debe ser eficiente, Campderrós Vilà (2019).

La tenacidad de los atacantes con base en los riesgos y las amenazas son preocupación de todos los días en los componentes de confidencialidad y control, la seguridad es de suma importancia para que se de una continuidad de existencia de una organización o empresa, la protección de la información valiosa, la sostenibilidad del prestigio de la marca y la adoptación de nuevas tecnologías. El uso de una aplicación web debe ser muy segura para que los usuarios puedan utilizar sus servicios con calidad y al conectarse para ingresar a la información de forma segura y adecuada (CISCO, 2015).

El impulso de la implementación de la ciberseguridad debe ser un compromiso entre los expertos de seguridad y la misma empresa para ofrecer el mejor servicio a los usuarios, es la clave para mejorar las probabilidades de supervivencia de las organizaciones empresariales y así preservar la actual posición de prestigio de la organización (Basque Cybersecurity Centre, 2020).

RECOMENDACIONES

Las recomendaciones para mitigar las amenazas y riesgos ante los ataques de cibercriminales, es siguiendo protocolos, reglas y políticas recomendadas por las fundaciones OWASP y la metodología abierta de Prueba de Seguridad (OSSTMM), con el objetivo de lograr que las aplicaciones web sean de mayor confianza. Además de estas, daremos otras, las que a continuación de describen en la siguiente lista:

- Mantener las aplicaciones actualizadas, las cuales debe incluir últimas versiones por lo que suelen ir implícitas correcciones de seguridad que solucionan vulnerabilidades ya conocidas.
- Implementación de controles de acceso que sean robustos para establecer autenticación y autorización adecuadas al acceso de las aplicaciones web, por lo que se deben utilizar contraseñas robustas.
- Realizar pruebas de seguridad frecuentes de seguridad en las aplicaciones web para identificar posibles vulnerabilidades.
- Validar y filtrar los datos de entrada, esto asegura la prevención de ataques.
- Protección de los datos sensibles, quizás de las técnicas más usuales sea el de la encriptación los datos sensibles que están almacenados las aplicaciones web
- Tener copias de seguridad frecuentes ante cualquier incidente de una pérdida de datos.

REFERENCIAS BIBLIOGRÁFICAS

Basque Cybersecurity Centre (2020), Libro Blanco de la ciberseguridad en Euskadi del Centro Vasco de Ciberseguridad, 2da Edición, publicación 18/08/2020.

Bitdefender (2023), "¿Qué es un Exploit? Prevención de Exploits", https://www.bitdefender.es/consumer/support/answer/22884/, Consumer Support.

Campderrós Vilà, Jaume (2019), "Ataques y vulnerabilidades web", http://hdl.handle.net/2445/143419 , Dipòsit Digital de la Universitat de Barcelona.

Curphey Mark, Scambray Joel, Olson Erik (2003), Improving Web Application Security: Threats and Countermeasures, Microsoft Corporation 2003.

CENGAGE Learning (2017), Web Applications and Data Servers, Book 3 of 4 (CEH), EC-Council | Press.

CISCO (2015), Afrontar las amenazas web avanzadas: Proteja su marca y sus datos, https://www.cisco.com/c/dam/global/es_es/assets/pdf/sc_07_address_web_threats_wp_cte_en_es_es.pdf

Gómez González I. C. (2012), Diseño de Metodología para Verificar la Seguridad en Aplicaciones Web Contra Inyecciones SQL. Universidad Militar Nueva Granada, Bogotá Colombia, Mayo 2012.

González Ruiz Jonnattan Arley (2018), Metodología y Análisis Orientado a la Seguridad Web, Universidad Nacional Abierta y a Distancia Escuela De Ciencias Básicas e Ingeniería Especialización en Seguridad Informática Bogotá D.C. 2018.

Hariyanto, Andysah Putera Utama Siahaan (2016), "Intrusion Detection System in Network Forensic Analysis and Investigation, IOSR Journal of Computer Engineering", vol. 11, número. 5.

Hernández Manuel (2022), "Pentesting con OWASP: fases y metodología", https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Hernández Saucedo Ana Laura, Mejia Miranda Jezreel (2015), "Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web", ReCIBE: Revista electrónica de Computación, Informática Biomédica y Electrónica, 01 de febrero del 2015, ISSN: 2007-5448.

Incibe (Instituto Nacional de Ciberseguridad)(2023), "Google Dorks te ayuda a encontrar información sobre ti en la Red", https://www.incibe.es/ciudadania/blog/google-dorks-te-ayuda-encontrar-informacion-sobre-ti-en-la-red, Oficina de seguridad del internauta, España, 2023.

Khari Manju, Sangwan Parikshit, Vaishali (2016), Web-Application Attacks: A Survey, Proceedings of the 10th INDIACom; INDIACom-2016; IEEE Conference ID: 37465 2016 3rd International Conference on "Computing for Sustainable Global Development", 16th - 18th March, 2016

Naudi Tamara (2016). Segundo informe de seguridad de la aplicación web de Acunetix muestra que el 55% de los sitios web tienen vulnerabilidades graves (y aumentan), Agosto 2016. https://www.acunetix.com/blog/news/web-app-security-report-2016/

OSSTMM (Open Source Security Testing Methodology Manual) (2023),"Manual de la Metodología de Pruebas de Seguridad de Recurso Abierto (Open Source)", https://www.ciberseguridad.eus/ciberpedia/vulnerabilidades/open-source-security-testing-methodology-manual-osstmm, (2023).

OWASP (Open Web Application Security Project) (2017), "Estándar de Verificación de Seguridad en Aplicaciones 3.0.1", https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf OWASP, Abril 2017.

OWASP (Open Web Application Security Project) (2021), “Introducción: OWASP Top 10:2021”, https://owasp.org/Top10/es/A00_2021_Introduction/

Sánchez Cano Gabriel (2018), Seguridad Cibernética: Hackeo Ético y Programación defensiva, 1era Edición, Alfaomega Grupo Editor, S.A. de C.V. México ISBN: 978-607-538-294-4.

Wassermann Gary, Su Zhendong (2007). “Sound and Precise Analysis of Web Applications for injection Vulnerabilities”, Proceedings of the 2007 ACM SIGPLAN Conference on Programming Language Design and Implementation, California, USA, pp. 32 41, 2007.

Yadav Divyani, Gupta Deeksha, Singh Dhananjay, Kumar Devendra, Sharma Upasana (2018), Vulnerabilities and Security of Web Applications, Conference: 2018 4th International Conference on Computing Communication and Automation (ICCCA), https://www.researchgate.net/publication/334767346