Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJOL

Analysis of computer security factors using the OWASP v4.2 methodology: ISTJOL case study

Carlos Vega-Oyola

Afiliación Institucional: Instituto Superior Tecnológico José Ochoa León, Ecuador

ORCID: https://orcid.org/0000-0001-7327-8239

Dirección para la correspondencia: carlos.vega@istjol.edu.ec

Eduardo Tapia Noblecilla

Afiliación Institucional: Instituto Superior Tecnológico José Ochoa León, Ecuador

ORCID: https://orcid.org/0000-0002-1598-401X

Dirección para la correspondencia: eduardo.tapia@istjol.edu.ec

Fabián Gallardo Gonzaga

Afiliación Institucional: Instituto Superior Tecnológico José Ochoa León, Ecuador

ORCID: https://orcid.org/0000-0003-4068-5414

Dirección para la correspondencia: fabian.gallardo@istjol.edu.ec

Líneas de publicación: Marketing, tecnología y comunicación

Fecha de recepción: 11 de noviembre 2021

Fecha de aceptación: 23 de enero 2022

Resumen.

Ante la aparición del COVID-19 y la cuarenta a nivel mundial, se potenció el uso de herramientas de tecnología de información y comunicación en todo ámbito de la sociedad, sobre todo en la educación.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

El uso del Moodle ha sido evidenciado en ser uno de los entornos virtuales de aprendizaje más utilizados por la mayor parte de instituciones de educación superior a nivel mundial, dada las múltiples ventajas que ofrece en el proceso formativo de enseñanza-aprendizaje. Así pues, el Instituto Superior Tecnológico José Ochoa León mantiene sus clases, recursos didácticos y cursos de educación continua mediante el uso de esta herramienta. Al ser utilizada se fluctúan y se transfieren una gran cantidad de información relevante para los actores de la educación, por ello la importancia de mantener seguro y salvaguardar la información generada, compartida y almacenada. La seguridad web enfoca sus pilares fundamentales en mantener la integridad, confidencialidad y disponibilidad de la información, por lo cual se implementó una metodología basada en la guía de pruebas de seguridad web de OWASP, lo cual permitió identificar y corregir vulnerabilidades dentro de las configuraciones, tanto en la aplicación web Moodle como en el servidor web Apache, mediante el uso de herramientas automatizadas como OWASP ZAP, NESSUS, Wireshark y Nmap aplicando testeos, ataques simples, escaneos de puertos, servicios y flujo de datos tanto en la aplicación Moodle como al servidor web Apache.

Según los resultados de las mencionadas herramientas, se concluyó que las configuraciones por defecto en el Moodle y servidor web Apache poseen 7 vulnerabilidades identificadas en este caso de estudio, vinculándose a los riesgos de nivel moderado, dos altos y cuatro bajos, por lo que en la investigación se implementaron las alternativas de solución por cada vulnerabilidad encontrada y así se logró minimizar las amenazas y riesgos de explotación.

Palabras clave: Seguridad web; OWASP; Educación Superior; Vulnerabilidades; Web.

Abstract

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

In view of the emergence of COVID-19 and COVID-40 worldwide, the use of information and communication technology tools in all areas of society, especially in education, was enhanced. The use of Moodle has been evidenced in being one of the virtual learning environments most used by most higher education institutions worldwide, given the multiple advantages it offers in the teaching-learning process. Thus, the José Ochoa León Higher Institute of Technology maintains its classes, teaching resources and continuing education courses through the use of this tool. When used, a large amount of information relevant to education actors is fluctuated and transferred, thus the importance of keeping information generated, shared and stored safe and secure. Web security focuses its fundamental pillars on maintaining the integrity, confidentiality and availability of information, which is why a methodology based on the OWASP web security test guide was implemented, which made it possible to identify and correct vulnerabilities within the configurations, both in the Moodle web application and in the Apache web server, by using automated tools such as OWASP ZAP, NESSUS, Wireshark and Nmap applying tests, simple attacks, port scans, services and data flow in both the Moodle application and the Apache web server.

According to the results of the aforementioned tools, it was concluded that the default configurations in the Moodle and Apache web server have 7 vulnerabilities identified in this case study, linking to moderate level risks, two high and four low, Therefore, the research implemented the alternative solutions for each vulnerability found and thus minimized the threats and risks of exploitation..

Key woks: Web security; OWASP; High Education; Vulnerabilities; Web.

Introducción

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

No es de extrañarse el rol tan importante que ocupan las instituciones de educación superior (IES) en el ámbito educacional de todo un país, estado o nación, ya que forman profesionalmente a estudiantes que deseen alcanzar un título de tercer o cuarto nivel, en conjunto con los conocimientos, habilidades y destrezas. Durante el proceso formativo, se involucran muchos otros procesos, servicios, actividades y demás, todas ellas, en su mayoría, se encuentran automatizadas y soportadas por las tecnologías de información y comunicación mediante la distribución de software más común y utilizado, como son las aplicaciones o plataformas web.

El uso de las tecnologías de información y comunicación se han potenciado aún más en la actualidad dentro del ámbito educativo-académico debido al COVID-19, que obligó a los actores participantes de la educación superior, a efectuar los procesos académicos, vinculación, investigación, de servicios y otros más, a la utilización de herramientas tecnológicas.

Ante el aumento de las necesidades de uso de las herramientas de tecnologías de información y comunicación en la educación superior en la actualidad, las IES han fortalecido e implementado software que ayudan a brindar la asistencia sobre los procesos académicos, científicos, de servicio entre otros más. El problema radica en que la implementación e instalación de software web en conjunto con las configuraciones de despliegue de la misma, únicamente se verifica el correcto funcionamiento y cumplimiento de los requisitos y necesidades de la IES, y en pocas ocasiones, posterior a la implementación, se realiza un análisis exhaustivo sobre la seguridad web de dicha acción, dando la posibilidad de que las amenazas aprovechen las vulnerabilidades poniendo en peligro la información que poseen las aplicaciones y plataformas web.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

Por esta razón, la información que se comparte y almacenan en estas aplicaciones o plataformas web de los procesos, servicios y demás actividades automatizadas, deben caracterizarse en cumplir con la integridad, disponibilidad y confidencialidad, pilares fundamentales de la seguridad en la información. Por tal motivo, el propósito de la presente investigación es identificar vulnerabilidades tomando en consideración los factores de la seguridad informática mediante la implementación de la guía de pruebas de seguridad web en su versión más actual y estable, como es la versión 4.2, publicado por la fundación Open Web Application Security Project (OWASP), tomando como caso de estudio las herramientas tecnológicas educativas web y los servidores que se encuentran implementados físicamente dentro de las instalaciones del Instituto Superior Tecnológico José Ochoa León (ISTJOL).

Con la aplicación de la guía de OWASP se pretende identificar, prevenir y corregir vulnerabilidades, tanto en las aplicaciones y plataformas web, como en los servidores en donde se encuentran alojados, ante el contexto de configuración al momento de desplegar un software web, minimizando y mitigando las amenazas de seguridad que se pueden encontrar en los servicios web que posee el ISTJOL, logrando así el asegurar el correcto funcionamiento del software, evitar interrupciones manteniendo así la disponibilidad y, sobre todo, fortalecer la protección de datos e información. Esto como enfoque principal de la importancia de la presente investigación.

Implícitamente, con esta investigación se alcanza a realizar una validación de la guía que propone OWASP, por lo que los resultados, análisis y propuestas de mejora indicadas, sirven para las demás instituciones de educación superior (IES), ya que estas utilizan aula virtual como Moodle, una de las aulas virtuales más utilizadas en el ámbito educativo de educación superior, siendo un aporte significativo a nivel de seguridad de información en las aplicaciones o plataformas web educativas.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

Estado del arte

Las tecnologías de información y comunicación son una complementariedad durante el ejercicio de enseñanza-aprendizaje en la educación, su aporte es fundamental para brindar apoyo en los procesos pedagógicos con la colaboración de recursos didácticos disponibles. Agnelli Faggioli expresa concisamente que al incorporarse las TICs en la educación brinda un aprendizaje constructivo y significativo (2020), esto no solo para los estudiantes, sino para todos los actores que participan dentro de los procesos de la educación, como son los docentes, que poseen un conjunto de conocimientos sobre el uso de las TICs como son los procesos de comunicación, organización, didáctica, teórico–práctico y la propia utilización de las TICs (Salazar Veloz, 2017).

Dentro de las TICs para la educación actuales, se encuentra el Moodle, que es un sistema gestión de aprendizaje más usado (Maldonado-Mangui et al., 2020), tanto a nivel mundial como local en Ecuador, ya que en este último cuenta con 3710 sitios web con dominios que lo utilizan (Moodle, 2021a), del cual dentro de las ventajas significativas se encuentran el proveer elementos como cuestionarios fáciles de aplicar, informes y seguimiento del progreso fáciles de entender, implementaciones de controles administrativos, entre otros que benefician el proceso enseñanza-aprendizaje de estudiantes y profesores (Evgenievich et al., 2021).

El Moodle al ser un software web, necesita de un servidor web para funcionar, la página oficial del mismo recomienda utilizar el servidor web Apache (Moodle, 2021b). Aquella recomendación no dista de la realidad que el mencionado servidor es uno de los más utilizados a nivel mundial, tal como lo menciona Netcraft, este servidor web se lleva el segundo lugar con un porcentaje del 25% entre más de 1179 millones de sitios que lo utilizan (2021).

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

La gran cantidad de información que manejan las aplicaciones web y, al igual que su servidor para su correcto funcionamiento, deben contar con una buena seguridad, dado que con esto se trata minimizar los riesgos vinculados con el acceso y la utilización de sistemas de forma no autorizada y, la mayor parte de las ocasiones, malintencionadas (Niño Benitez & Silega Martínez, 2018), buscando mantener y salvaguardar la integridad, confidencialidad y disponibilidad, los pilares fundamentales de la seguridad web, además de la permanencia, accesibilidad y aceptabilidad (Quiroz-Zambrano & Macías-Valencia, 2017).

Para cumplir con lo mencionado acerca de la seguridad web y el aseguramiento para las aplicaciones web y servidores web como tal, existen un sinnúmero de estudios, herramientas automatizadas, semiautomatizadas, propuestas de modelos, metodologías, guías y más recursos que permiten, básicamente, identificar vulnerabilidades mediante algún tipo de prueba para así aplicar correctivos y minimizar los riesgos de ataques. Tal es así como el estudio de Rian y Ahmad (2019), que desarrollaron un escáner de seguridad en un software de aplicación web para ayudar a superar los problemas de seguridad en aplicaciones web. También cabe mencionar el estudio sobre las pruebas de penetración en aplicaciones web y conocer que riesgos de seguridad existen al aplicarlas (González Brito & Montesino Perurena, 2021) y así tener en consideración recomendaciones para que las aplicaciones no sufran un problema secundario. Las aplicaciones de modelos basados en metodología, como el caso de la metodología MAGERIT (Jácome Segovia et al.) que en el 2021 al aplicarse un modelo derivado de la mencionada metodología, se gestionaron los riesgos de seguridad informática en servicios web de una empresa, reduciendo así un 87.87% las vulnerabilidades altas encontradas. Destacar también la utilización de herramientas automatizadas como Acunetix 11, identificando algunas vulnerabilidades dentro del top

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

ten de OWASP 2017 (Flores Urgilés et al., 2018). Sin dejar atrás la propuesta de evaluar mediante instrumentos de recolección de información a personal que manipulan sistemas, y también el uso de herramientas aplicando inyección de paquetes y puertos no controlados detectando debilidades e incoherencias en las configuraciones en red (Vega Villacís & Ramos Morocho, 2017).

Existen muchos estudios e investigaciones de lo mencionado en el párrafo anterior por toda la comunidad investigativa y bases de datos científicos, pero en sí, la mayor parte de las investigaciones están relacionadas con el uso de las guías, propuestas, modelos y herramientas que propone OWASP, tal es el caso de (Nanisura Damanik & Sunaringtyas, 2020), que utiliza un conjunto de guías OWASP como el estándar de verificación de seguridad de aplicaciones (ASVS siglas en inglés) y la guía de pruebas de aplicaciones web, identificando vulnerabilidades como Inyección SQL, autenticación rota y accesos de controles rotos, del cual propiamente la guía le indica un valor de nivel de riesgo que posee el código desarrollado e implementado en la aplicación web SIAP analizada. Otro estudio importante que mencionar mediante la utilización de OWASP, es la implementación de técnicas y recomendaciones para evitar ataques de inyección SQL y XXS, en una propuesta de software web cuya validación de diseño, codificación y seguridad fue con herramientas automatizadas, incluidas OWASP ZAP (Guamán et al., 2017). Kumar Lala et al., en su estudio propone una adaptabilidad de desarrollo de aplicaciones web teniendo en consideración las recomendaciones de las guías de OWASP, menciona las vulnerabilidades más comunes en sitios web y propone algunas alternativas de solución para mitigar que las amenazas exploten esta vulnerabilidades (2021).

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

Por ello, esta investigación se centra en analizar e identificar vulnerabilidades en la aplicación web Moodle y en el servidor web APACHE del Instituto Superior Tecnológico José Ochoa León mediante el uso de la guía de pruebas de seguridad web de OWASP.

Materiales y Métodos

Diseño: Ante lo mencionado con anterioridad, la presente investigación tiene por objetivo principal analizar factores de seguridad web de la aplicación web Moodle que posee el Instituto Superior Tecnológico José Ochoa León (ISTJOL), mediante la aplicación de la guía de pruebas de seguridad web de OWASP. Diciéndose por esta guía en su última versión y estable v4.2 a la fecha, debido a que OWASP es una organización que se encuentra diariamente actualizando sus productos, servicios e información a la comunidad, informando lo que en la actualidad está ocurriendo con respecto a la seguridad web.

Esta investigación se considera de tipo aplicada, de profundización explicativa y obtención de datos cualitativos, dado que el diseño del experimento es controlado aplicado a un caso en específico.

Población: Como población se determinó realizar las pruebas de seguridad a una aplicación web Moodle alojado en un servidor Apache del ISTJOL, debido que es una de las más usadas por estudiantes y docentes, no solamente para soporte de sus clases, sino también, utilizada para la ejecución de los cursos de educación continua. Su selección se basó en que es una de las herramientas tecnológicas mayormente utilizada para los procesos formativos de enseñanza-aprendizaje importante del ISTJOL.

El entorno en que se desarrolla la investigación es en una IES como lo es Instituto Superior Tecnológico José Ochoa León, que forma parte de la educación superior.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

Intervenciones: Previo a la aplicación de la guía de pruebas de seguridad web de OWASP, se realizó un procedimiento de lectura comprensiva y exhaustiva acerca de su contenido, identificando 12 categorías y 97 pruebas en su totalidad.

La guía de pruebas de seguridad web de OWASP por cada prueba brinda una sugerencia de herramientas a utilizar para llevar a cabo la obtención de información. Dentro de la investigación se utilizaron las siguientes herramientas automatizadas:

- OWASP ZAP: Es uno de los proyectos más activos de OWASP, reconocida herramienta profesional para pruebas de penetración, que se complementa muy bien a la guía de pruebas de seguridad web, llegando a cumplir la mayor parte de pruebas fijadas en la mencionada guía. Para el uso completo de la herramienta no es necesario adquirir una licencia comercial, debido que es un proyecto sin ánimos de lucro (OWASP, 2021).
- NMAP: Herramienta que sirve para el escaneo de puertos abiertos (NMAP, 2021).
- NESSUS: Herramienta completa para realizar escaneos de vulnerabilidades. Su uso es de licencia comercial, por lo que se debe pagar un coste por acciones que se necesiten para realizar pruebas determinadas (NESSUS, 2021).
- Wireshark: Una de las herramientas que permite analizar protocolos de red más importantes y utilizando a nivel mundial. No hay que pagar una licencia comercial para su uso, ya que cuenta con desarrolladores voluntarios expertos en redes, que colaboran activamente con el proyecto (Whireshark, 2021).

El proceso que se aplicó fue el siguiente:

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

1. Se identificó el dominio URL, puertos y direcciones IP de la aplicación Moodle a analizar.

2. Preparar y ejecutar las herramientas necesarias previo a realizar las pruebas de seguridad web, entre ellas OWASP ZAP, NMAP, NESSUS y Whireshark, en un sistema operativo denominado Kali Linux, debido que se encuentra específicamente desarrollado y especializado en realización análisis de seguridad web.

3. Durante la realización de las pruebas, algunas herramientas, tales como NESSUS y OWASP ZAP, tuvieron un tiempo considerable de demora al momento de ejecutar las pruebas, por lo que la paciencia es fundamental en este caso.

4. Luego de que cada herramienta finalizó sus pruebas, emitieron informes donde se mostraron todas las vulnerabilidades encontradas.

Los resultados fueron consolidados y procesados, los mismos que se muestran a continuación:

Tabla 1

Número y nivel de riesgo de vulnerabilidades encontradas por categoría OWASP

Categoría	Número vulnerabilidades encontr
Recopilación de información	1
Pruebas de gestión de la configuración y la entación	1
Pruebas de gestión de identidad	0
Prueba de autenticación	3
Prueba de autorización	0
Prueba de gestión de sesiones	0
Prueba de validación de entrada	2
Prueba de manejo de errores	0
Prueba de criptografía débil	0
). Pruebas de lógica empresarial	0
l. Pruebas del lado del cliente	0

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

2. Pruebas de API	0

Nota: Información obtenida de los reportes de las herramientas aplicados. Elaborado por los autores.

Tal como se observa en la tabla 1, en los reportes se detectaron 7 vulnerabilidades identificadas en el guía de pruebas de seguridad web de OWASP. Estas vulnerabilidades se detallan a continuación, mostrando el nivel de riesgo que poseen, el código identificador de OWASP y la categoría a la que pertenecen.

Tabla 2.

Detalle de las vulnerabilidades encontradas con su respectivo nivel de riesgo

Categoría	Nombre vulnerabil	Código OWA	Riesgo	Compone
Recopilación de ción	evise los metarchivos web para detectar fu ción	WSTG-INFO	Moderad	Apache
Pruebas de gestión ración y la entación	obar la configuració ructura de red	WSTG-CONI	Alto	Apache
Prueba de autentic	ueba de credenciales tadas a través de un	WSTG-ATHN	Alto	Apache
Prueba de autentic	ueba de mecanismo débil	WSTG-ATHN	Bajo	Moodle
Prueba de autentic	ueba para omitir el a de autenticación	WSTG-ATHN	Bajo	Apache
Prueba de validaci	ueba de secuencias c os de sitios cruzados os	WSTG-INPV	Bajo	Apache
Prueba de validaci	ueba de secuencias c os de sitios cruzados adas	WSTG-INPV	Bajo	Apache

Nota: Información obtenida de los informes de las herramientas al finalizar las pruebas. Elaborado por los autores.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

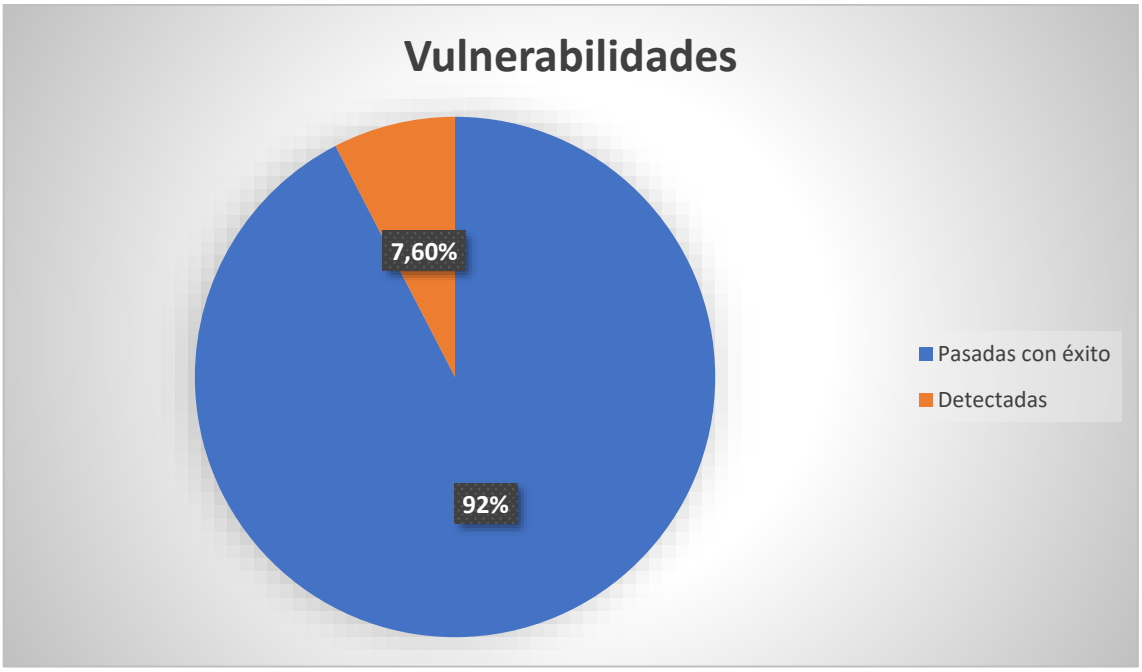
Resultados y Discusión

Resultados

Los resultados obtenidos en los informes de las herramientas, habiendo sido identificados, consolidados y resumidos, se puede identificar que de las 92 pruebas que recomienda la guía de pruebas de seguridad web de OWASP, se han detectado 7 vulnerabilidades, que representa el 7.60% del total encontradas en la aplicación web y en la configuración de su servidor, tal como lo muestra la figura 2.

Figura 1.

Porcentajes de vulnerabilidades pasadas con éxito y detectadas



Nota: Información obtenida de los informes de las herramientas al finalizar las pruebas. Elaborado por los autores

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

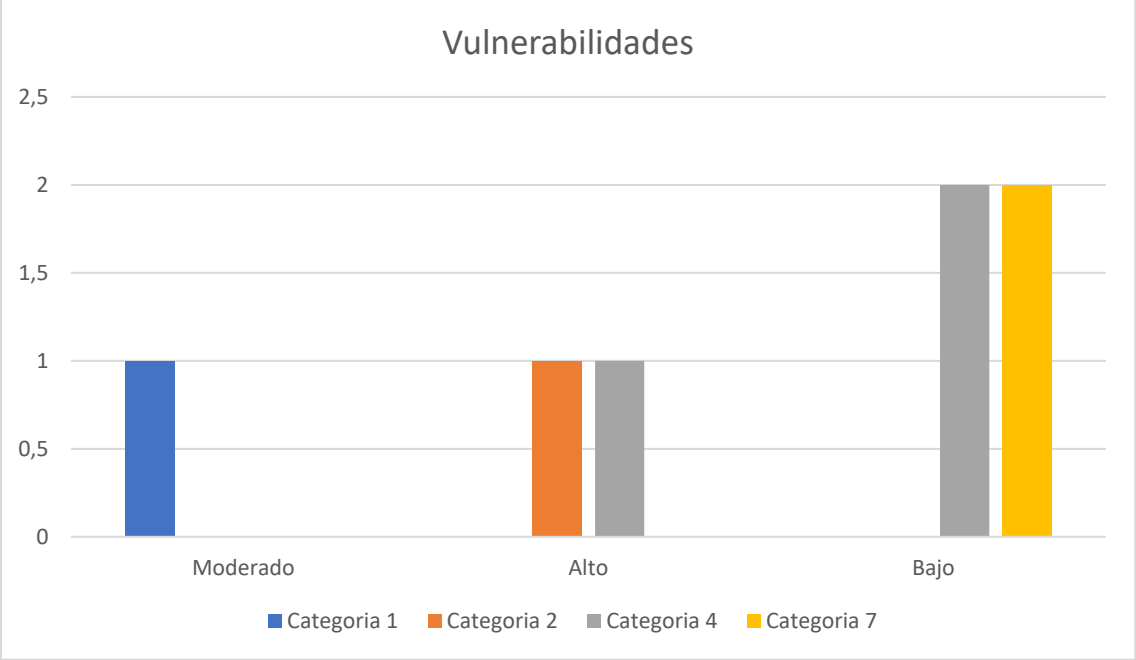
ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

De las vulnerabilidades encontradas, se identificaron

Figura 1.

Vulnerabilidades por categorías y riesgo.



Nota: Las identificaciones de categorías significan 1 = Recopilación de información, 2 = Pruebas de gestión de la configuración y la implementación, 4 = Prueba de autenticación y 7 = Prueba de validación de entrada. Elaborado por los autores.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

Discusión

El *OWASP Testing Guide* es una de las principales guías de detección de vulnerabilidades para cualquier tipo de aplicaciones y servidores, utilizado por diferentes entidades dado su alto nivel de confiabilidad y efectividad con respecto a garantizar la seguridad web y funcionamiento de las aplicaciones. Tal es así que a nivel mundial OWASP es reconocido sobre seguridad informática, presentando un sinnúmero de casos de éxito por lo cual, para la obtención de los resultados de la presente investigación, se consideró algunas de las soluciones de esos casos de éxito que provee la guía, desde su página web oficial.

Es importante mencionar que las vulnerabilidades encontradas atienden a las configuraciones que poseen la aplicación web Moodle y el servidor Apache, cuya solución se basa en aplicar correctivos de configuraciones. Entre las vulnerabilidades encontradas se tiene:

- *Review Webserver Metafiles for Information Leakage*

La vulnerabilidad permite recopilar otra información para identificar la superficie de ataque, los detalles tecnológicos o para su uso en la participación de ingeniería social.

Alternativa de solución: Se implementa la configuración del servidor Apache en el archivo httpd.conf para la eliminación de cabeceras de información.

- *Test Network Infrastructure Configuration*

Con esta vulnerabilidad es posible ver la lista del directorio, dentro de ella se puede revelar scripts ocultos, incluir archivos, archivos de origen de respaldo, etc., a los que se puede acceder para leer información confidencial.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

Alternativa de solución: Se desactiva la exploración de directorios. Si es necesario, se debe asegurar que los archivos enumerados no presenten riesgos.

- *Testing for Credentials Transported over an Encrypted Channel*

Esta vulnerabilidad hace referencia a que un sitio web no pueda realizar la encriptación de datos en la comunicación entre el servidor y el cliente a falta de un certificado SSL, lo cual deja expuesta la información que se comparte, hace cualquier capturador de tráfico de red. **Alternativa de solución:** Se configura certificado SSL, para la implementación del protocolo HTTPS.

- *Testing for Weak Lock Out Mechanism*

La presente vulnerabilidad permite al atacante ingresar un sinnúmero de contraseña (conocida como ataque de fuerza bruta) para dar con las credenciales de usuario y acceder al sitio. **Alternativa de solución:** Se configura el módulo bloqueo de cuenta dentro del Moodle, el cual permite controlar un número determinado de intentos fallidos para ingresar al sitio.

- *Testing for Bypassing Authentication Schema*

La novedad con esta vulnerabilidad identificada por la herramienta, es que muestra el listado de carpetas y archivos que se encuentra estructurado el sitio, al momento de acceder a un documento, salta el esquema de autenticación no permitiendo el acceso al mismo.

Alternativa de solución: Se desactiva la exploración de directorios. Si es necesario, se debe asegurar que los archivos enumerados no presenten riesgos.

- *Testing for Reflected Cross Site Scripting* y *Testing for Stored Cross Site Scripting*

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88
Artículo Científico
Indexada Latindex Catálogo 2.0
ISSN 2602-8093
DOI: 10.33970/eetes.v6.n1.2022.293

Las vulnerabilidades mencionadas, permite la inserción de comandos reflejados entre sitios (XSS), el mismo que produce cuando un atacante inyecta código ejecutable del navegador dentro de una única respuesta HTTP.

Alternativa de solución: Se configura los marcos que escapen automáticamente de XSS por diseño.

Conclusiones

La OWASP Testing Guide v4 4.2 ayuda a publicación de sitios con parámetros básicos para la mitigación de ataques informáticos mediante la aplicación de buenas prácticas en las creación y configuración de aplicaciones web, en el caso de ISTJOL, los resultados de la aplicación de los diferentes test establecidos en esta metodología, se evidencia que las vulnerabilidades encontradas son parte de la configuración propiamente de los componentes web, sin embargo, la aplicación de la guía de la metodología proporciona las herramientas necesarias para encontrar posibles alternativas de solución y neutralizar las vulnerabilidades de los componentes web, posterior a su instalación y y así lograr minimizar las amenazas y riesgos de explotación.

Se considera además que la utilización de equipos con una capacidad superior a la utilizada para la presente investigación proporcionaría un tiempo de respuesta menor en la aplicación de cada test, así como también, se plantea un estudio adicional que permita implementar las configuraciones necesarias para neutralizar las vulnerabilidades encontradas, así mejorar la calidad y la integridad de los servicio, además que permitan tanto al ISTJOL como a las demás IES minimizar los riesgos de su seguridad web en servidores de aplicación y LMS como herramienta de asistencia académica.

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

Referencias Bibliográficas

Agnelli, A. (2020). El progreso de las tecnología de información y comunicación en el ámbito educativo. *Espíritu Emprendedor TES*, *4*(2), 13–20. https://doi.org/10.33970/eetes.v4.n2.2020.196

Evgenievich, E., Petrovna, M., Evgenievna, T., Aleksandrovna, O., & Yevgenyevna, S. (2021). Moodle LMS: Positive and Negative Aspects of Using Distance Education in Higher Education Institutions. *Propósitos y Representaciones*, *9*(SPE2). https://doi.org/10.20511/pyr2021.v9nspe2.1104

Flores Urgilés, C., Zhinin Aguayza, B., Segovia Cantos, A., Mayancela Zhinin, M., & Marlene García, J. (2018). Evaluación de seguridad de la información en las páginas web pertenecientes a los municipios de la provincia del Cañar. *Killkana Técnica*, *2*(1), 13–18. https://doi.org/10.26871/killkana_tecnica.v2i1.286

González Brito, H. R., & Montesino Perurena, R. (2021). Riesgos de seguridad en las pruebas de penetración de aplicaciones web. *REVISTA CUBANA DE TRANSFORMACIÓN DIGITAL*, *2*(2), 98–117. https://rctd.uic.cu/rctd/article/view/114

Guamán, D., Guamán, F., Jaramillo, D., & Sucunuta, M. (2017). Implementación de técnicas y recomendaciones de seguridad OWASP para evitar ataques de tipo inyección SQL, XSS utilizando J2EE y WS-Security. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*. https://doi.org/10.23919/CISTI.2017.7975981

Jácome Segovia, D., Castillo Fiallos, J., Mantilla Cabrera, C., & Vaca Barahona, B. E. (2021). Aplicación de MAGERIT para reducir riesgos en servicios Web en un contexto académico en Ecuador. *AlfaPublicaciones*, *3*(2.2), 66–82. https://doi.org/10.33262/ap.v3i2.2.60

Kumar Lala, S., Kumar, A., & Subbulakshmi, T. (2021). Secure web development using OWASP guidelines. *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*, 323–332. https://doi.org/10.1109/ICICCS51141.2021.9432179

Maldonado-Mangui, S. P., Peñaherrera-Acurio, W. P., & Espinoza-Beltrán, P. S. (2020). Los Entornos Virtuales de Aprendizaje (EVA´s), como recurso de aprendizaje en las clases asíncronas de las IES. *Dominio de Las Ciencias*, *6*(4), 1279–1291. https://doi.org/10.23857/dc.v6i4.1536

Moodle. (2021a, October 20). *Statistics*. https://stats.moodle.org/

Moodle. (2021b, October 21). *Instalación de Moodle*. https://docs.moodle.org/all/es/35/Instalaci%C3%B3n_de_Moodle

Nanisura Damanik, V. N., & Sunaringtyas, S. U. (2020). Secure code recommendation based on code review result using owasp code review guide. *2020 International Workshop on Big Data*

Espíritu Emprendedor TES 2022, Vol 6, No. 1 enero a marzo 70-88

Artículo Científico

Indexada Latindex Catálogo 2.0

ISSN 2602-8093

DOI: 10.33970/eetes.v6.n1.2022.293

and Information Security, IWBIS 2020, 153–157. https://doi.org/10.1109/IWBIS50925.2020.9255559

NESSUS. (2021, October 22). *NESSUS*. https://www.tenable.com/products/nessus

Netcraft. (2021, October 15). *October 2021 Web Server Survey*. https://news.netcraft.com/archives/category/web-server-survey/

Niño Benitez, Y., & Silega Martínez, N. (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas*, *12*(Especial UCIENCIA), 205–221. http://scielo.sld.cu/scielo.php?pid=S2227-18992018000500015&script=sci_arttext&tlng=pt

NMAP. (2021, October 22). *NMAP.ORG*. https://nmap.org/

OWASP. (2021, October 22). *OWASP ZAP*. https://owasp.org/www-project-zap/

Quiroz-Zambrano, S., & Macías-Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de Las Ciencias*, *3*(5), 676–688. https://doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688

Rian, A., & Ahmad, F. (2019). Security Scanner for Web Applications Case Study: Learning Management System. *Jurnal Online Informatika*, *4*(2), 63–68. https://doi.org/10.15575/join.v4i2.39

Salazar Veloz, T. M. (2017). Preparación del Docente en la era digital. *Espíritu Emprendedor TES*, *1*(2), 9–18. https://doi.org/10.33970/eetes.v1.n2.2017.24

Vega Villacís, G., & Ramos Morocho, R. A. (2017). VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DELA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO. *3C Tecnología*, *6*(1), 53–66. https://doi.org/http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21.53-66/

Whireshark. (2021, October 22). *Whireshark*. https://www.wireshark.org/