SATHIRÍ Sembrador

PRUEBAS DE PENETRACIÓN PARA LA SEGURIDAD INFORMÁTICA AL SERVIDOR WEB DEL LABORATORIO DE CIBERSEGURIDAD EN LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

PENETRATION TESTS FOR COMPUTER SECURITY TO THE WEB SERVER USING OWASP METHODOLOGY FOR THE DETECTION OF VULNERABILITIES IN THE CYBERSECURITY LABORATORY AT THE UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Recibido: 21/ 12/ 2021 - Aceptado: 13/06/2022

ÁLVARO STEEBE CASTILLO ENRÍQUEZ

Investigador Independiente
Tulcán - Ecuador

Ingeniero en Informática
Universidad Politécnica Estatal del Carchi

alvaro.castillo@upec.edu.ec
https://orcid.org/0000-0002-9993-2339

JAIRO VLADIMIR HIDALGO GUIJARRO

Docente en la Universidad Politécnica Estatal del Carchi
Tulcán - Ecuador

Magíster en Redes de Comunicaciones
Pontificia Universidad Católica del Ecuador

jairo.hidalgo@upec.edu.ec
https://orcid.org/0000-0001-8165-0192

CARLITOS ALBERTO GUANO CÁRDENAS

Docente en la Universidad Politécnica Estatal del Carchi
Tulcán - Ecuador

Magíster en Gerencia en Sistemas
Universidad de las Fuerzas Armadas

carlos.guano@upec.edu.ec
https://orcid.org/0000-0002-7571-2972

Cómo citar este artículo:

Castillo, A., Hidalgo, J. & Guano, C. (Julio - diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Resumen

La presente investigación denominada “Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi” profundizó en el estudio de las vulnerabilidades presentes en los servidores web y su relación con los procesos de seguridad. El objetivo principal fue diagnosticar las vulnerabilidades existentes en los servidores web tales como inyecciones SQL, XXS Cross Site Script, ataques de fuerza bruta, entre otras. Mediante herramientas de pentest se dio a conocer los riesgos y amenazas presentes. Para cumplir esta meta se planteó un enfoque cualitativo en conjunto con la investigación de campo y documental que permitieron recolectar datos a través de la técnica de una entrevista al coordinador del laboratorio de ciberseguridad, dando como resultado información detallada de los procesos de seguridad y los problemas más comunes que se producen en los servidores web. A partir de los resultados obtenidos se estableció varias pruebas utilizando una metodología para desarrollar los procesos, la metodología Owasp y Owasp Zap fueron las herramientas principales para encontrar alertas de amenazas, como también la ejecución de procesos tales como: recolección de información, uso de motores de búsqueda para verificar análisis, enumeración de las aplicaciones del servidor, revisión de comentarios hacia el sitio web para verificar la presencia de información vulnerable, identificación de puntos de entrada, alertas y análisis de la arquitectura de la aplicación, test de manejo de configuración y desarrollo, test de configuración e infraestructura, test de extensiones de archivos, test método http, test de seguridad estricto Hsts, test de validación de entradas, entre otras más. Como también la utilización de Kali Linux como sistema operativo que permitió la utilización de técnicas de pentest y correcciones de seguridad al servidor. Por otra parte, se estableció una comparativa de los servidores web con un valor alcanzado del 80% para Apache y el 30% para Microsoft IIS, como también una comparación final de las vulnerabilidades del 5,33% para manejo, configuración y desarrollo, 8% manejo de identidad y método http, 7% fuerza bruta y Cross Site Scripting, 5% inyección SQL y DoS y finalmente 4,67% Owasp Zap/directorios. El uso de estas técnicas fusionado con la gestión de las fases de la metodología Owasp permitió organizar, orientar de manera rápida y confiable técnicas básicas para proteger contra amenazas comunes e importantes, obteniendo como referencia la documentación generada que puede ser reutilizable para proyectos futuros o en trabajos de implementación.

Palabras clave: *vulnerabilidad, seguridad, servidor web, sitios web, Owasp*

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Abstract

This research called "Penetration tests for computer security to the web server of the cybersecurity laboratory at the Carchi State Polytechnic University" delved into the study of the vulnerabilities present in web servers and their relationship with security processes, the objective The main part of the project was to diagnose existing vulnerabilities in web servers such as SQL injections, XXS Cross Site Script, brute force attacks, among others. Through pentest tools, the risks and threats present were made known, to fulfill this goal a qualitative approach was proposed in conjunction with field and documentary research that allowed data to be collected through the technique of an interview with the laboratory coordinator cybersecurity, resulting in detailed information on security processes and the most common problems that occur on web servers. From the results obtained, several tests were established using a methodology to develop the processes, the Owasp and Owasp Zap methodology were the main tools to find threat alerts, as well as the execution of processes such as: information collection, use of engines search to verify analysis, enumeration of the server applications, review of comments towards the website to verify the presence of vulnerable information, identification of entry points, alerts and analysis of the application architecture, configuration management test and development, configuration and infrastructure test, file extension test, http method test, strict Hsts security test, input validation test, among others. As well as the use of Kali Linux as an operating system that allowed the use of pentest techniques and security corrections to the server. On the other hand, a comparison of the web servers was established with a value reached of 80% for Apache and 30% for Microsoft IIS, as well as a final comparison of the vulnerabilities of 5.33% for management, configuration and development, 8% handling of identity and http method, 7% brute force and Cross Site Scripting, 5% SQL injection and DoS and finally 4.67% Owasp Zap / directories. The use of these techniques combined with the management of the phases of the Owasp methodology allowed to organize, guide quickly and reliably basic techniques to protect against common and important threats, obtaining as a reference the generated documentation that can be reusable for future projects or in implementation work.

Keywords: *vulnerability, security, web server, web sites, Owasp*

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Introducción

En la actualidad organizaciones, laboratorios y páginas web que brindan servicios a los usuarios procesan a diario una gran cantidad de amenazas y vulnerabilidades por parte de atacantes informáticos que tratan de robar, alterar y sacar provecho de la información. Partiendo de esta necesidad, los expertos se enfocan cada vez más en el desarrollo de sistemas tecnológicos y la aplicación de técnicas de seguridad para el cuidado de los datos de la organización y así proteger la ejecución de los procesos que ofrece a sus usuarios. En este sentido esta investigación se realizó con el fin de brindar pautas, métodos y técnicas a cada individuo que quiera conocer y aprender a incrementar la seguridad mediante procesos y configuraciones a los servidores web, aplicaciones web y además identificar y analizar las vulnerabilidades que se presentan en cada una de ellas.

En Sudamérica se realizó un estudio enfocado a los problemas latentes de inseguridad informática y el robo de la información, vulnerabilidad, hackeo, phishing entre otras amenazas en organizaciones financieras y de otra índole. Esta investigación de acuerdo con el Índice Global de Ciberseguridad (IGC) en el Ecuador ocupa el puesto 79 de 127 países respecto a la seguridad en el ranking internacional relacionado a la vulnerabilidad y evaluación de riegos con un indicador del 37% de seguridad y ocupando el puesto 74 para el año 2020 frente a la pandemia del Covid-19 (Deep Knowledge Group, 2020). En este sentido existe un elevado índice de inseguridad informática posicionando a Ecuador en el sexto lugar de 19 países con un indicador del 31,57% de seguridad que se encuentra por debajo de los países como Perú, Venezuela, Chile, Paraguay, El Salvador, Nicaragua y Bolivia de acuerdo con la Unión Internacional de Telecomunicaciones (ITU) (Troein y Acayo, 2020).

Sánchez y Santander (2016) determinaron que, para el proceso de mejorar el nivel crítico de la infraestructura, tuvieron que identificar los problemas que hacen que incremente la vulnerabilidad, realizaron un proceso de pentesting en ambientes de control industrial finalmente el uso de herramientas de pentesting para la ejecución permitiendo suplantar de manera correcta comandos enviados por la estación administradora. Al terminar el artículo de "Herramientas DNP3 Pentesting para redes de infraestructura crítica", se obtuvo las siguientes conclusiones:

El proceso de pentesting permitió una mejor interacción, más eficaz en la infraestructura crítica porque facilitó que los responsables de ciberseguridad puedan realizar verificaciones de las configuraciones en los dispositivos de seguridad; con el propósito de disminuir la probabilidad de ocurrencia, factibilidad en la suplantación y estación administrativa, lo cual ayudará a constatar que los atacantes no podrán cambiar los controladores en la infraestructura (Sánchez y Santander, 2016).

Pérez y Quiñones (2017) en su investigación "Uso de herramientas de Pentesting para el análisis de vulnerabilidad de las operadoras ubicadas en la ciudad de Guayaquil", explican el diagnóstico de las vulnerabilidades que se presentan a los sistemas de comunicaciones móviles, conociendo los ataques relacionados con cada vulnerabilidad con el objetivo de proponer una solución que avale identificar cualquier tipo de amenazas que se encuentra aplicado en la localidad. La contribución de este estudio con respecto a la investigación se enfoca en la elaboración de análisis de los requerimientos, los procesos y técnicas que completan las pruebas de penetración brindando una apariencia más profunda con relación al uso de estas herramientas. Igualmente, demuestra la extensa aplicabilidad de estos métodos de pentest en diferentes áreas como en este caso, a la ciudad de Guayaquil.

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

El proyecto realizado permitirá cumplir con el proceso de evaluación de las vulnerabilidades presentes en los sistemas de comunicaciones móviles mediante un test de intrusión, ayudando a identificar el nivel de seguridad en la infraestructura y ver el nivel de riego y amenaza al cual se está expuesto, de tal manera que un cracker realice un ataque cibernético y violente con la integridad, confidencialidad, y disponibilidad a la información, y finalmente evaluar vulnerabilidades a los sistemas de comunicaciones móviles con todas las técnicas de protección para cubrir fallos de seguridad detectados.

Otro de los antecedentes investigativos forma parte del repositorio de la Universidad de Guayaquil, elaborado por Briones y Hernández (2018), trata acerca de "Auditoria de seguridad del servidor web de la empresa Publinext S.A. Utilizando mecanismo basados en OWASP".

En esta investigación se menciona los varios tipos de servicios que han ganado popularidad en los mercados tecnológicos y han conllevado a que la información proporcionada sea robada y alterada sino se utilizan medidas de seguridad necesarias para un buen manejo en los servicios que han sido incorporados en los últimos años gracias a la tecnología, como es el caso de sitios de comercio electrónico, servicios web, bancos entre otras más. Por lo que, con el pasar de los días las amenazas han sido ejecutadas por piratas informáticos que ponen en riegos a los sistemas informáticos, de la misma manera se han creado procesos o metodologías como es el caso de OWASP, OSSTMM, que son entre otras buenas prácticas, que se han encargado de crear métodos y técnicas que evalúen los riegos y analicen todo tipo de vulnerabilidades.

El laboratorio de ciberseguridad es una de las áreas de la Universidad Politécnica Estatal del Carchi que se encarga de realizar pruebas de investigación por las configuraciones y servicios que se quieran desarrollar; actualmente cuentan con equipamientos e infraestructura que permiten a los estudiantes y docentes realizar pruebas orientadas a la seguridad de los dispositivos, configuraciones de redes, entre otros. En este sentido se configuró los servidores que se encontraban con malos procesos de seguridad. La subutilización de recursos provocaba la vulnerabilidad a los sistemas. La importancia de esta investigación se fundamenta en el provecho de conocimiento sobre herramientas utilizadas para el análisis de vulnerabidades y fases que documenten de una mejor manera sus procesos, traducido en la elaboración metodológica Owasp con el fin de identificar y proteger contra debilidades comunes e importantes. La construcción de la propuesta está totalmente enfocada al análisis de vulnerabilidad a los servidores web donde fue guiada por metodologías y la información recolectada con los instrumentos de investigación, dando lugar al manejo de técnica y herramientas que se centran en el sistema operativo Kali-Linux para asegurar la coherencia entre los componentes.

Materiales y métodos

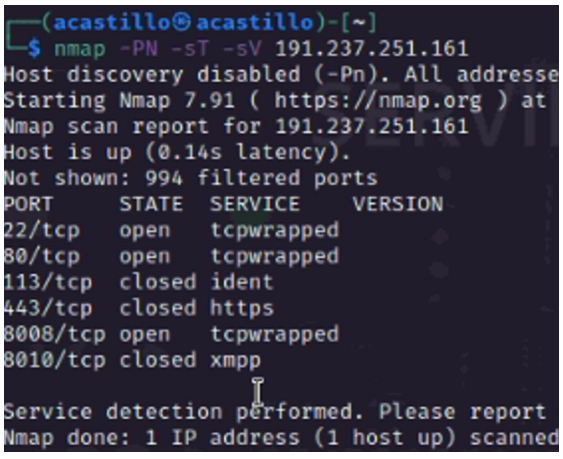
El presente proyecto utilizó un enfoque cualitativo el cual permite analizar la realidad estudiada acerca del uso de pruebas de penetración (Pentest) para el análisis al laboratorio de ciberseguridad y determinar como la incidencia afecta en la ejecución de estos procesos. Además, la dependencia entre la investigación y el fenómeno estudiado se trata de una relación de interdependencia porque el investigador influye directamente en el desarrollo y ejecución de estos procesos de Pentest. De esta manera ya que se puntualizó el análisis de las vulnerabilidades en los sitios web, inicialmente se solicitó el permiso para la creación de los servidores, para realizar el proyecto en el laboratorio de ciberseguridad. Además, se

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

hizo la entrevista con el director del área, para conocer los procesos manejados, normativas y metodologías y así comenzar con la ejecución de las técnicas de vulnerabilidad. También, se comparó los servidores que serían analizados, para evaluar su eficiencia al momento de instalar y configurar un servidor web, se cumplieron criterios de evaluación, en total 8 criterios correspondientes a cada una de las fases propuestas por la metodología Owasp, se ejecutó las pruebas oportunas y se documentó todo el proceso. Por otro lado, se aplicó un checklist de verificación respecto a la seguridad encontrada en los servidores, además se procede a realizar un test de resultados para verificar las vulnerabilidades que tienen mayor riesgo en los servidores web y finalmente como resultante una escala de cumplimiento para comprobar el antes y el después del proceso.

Esta metodología se basa en la contribución de datos por empresas que son netamente especializados en la seguridad de aplicaciones; a través de ranking de debilidades hacia sitos web que sucede con mayor frecuencia en Internet, es una de las tantas colecciones de datos sobre vulnerabilidades más grandes que se haya conseguido coleccionar de manera pública. Estas vulnerabilidades son recogidas por cientos de organizaciones, así como también más de cien mil aplicaciones y APIs del mundo en la actualidad. Las principales categorías son escogidas y priorizadas mediante datos de prevalencia, con consecuencias consensuadas de explotabilidad, detectabilidad e impacto; con el fin de educar a los desarrolladores, diseñadores, arquitectos, gerentes y organizaciones sobre técnicas básicas para protegerse contra debilidades comunes e importantes, así como también de problemas de riesgo alto, ofreciendo orientación para continuar con su aplicación.

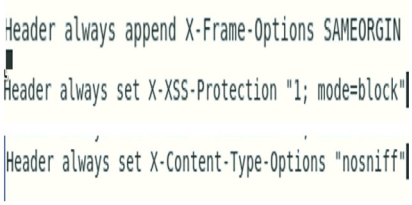
Como parte de las pruebas de penetración y herramientas utilizadas están:



Nmap

Nmap se usó para verificar los puertos que se encontraban abiertos y cerrados independientemente de cada servicio que presenta la aplicación web. Uno de los comando más necesarios fue: nmap -PN -sT -Sv + dirección sitio web.

-sP (sondeo de ping): establece cuantos dispositivos se encuentran activos.
-P0 (No realiza ping): realiza un escaneo de puertos.
-Ps (lista de puertos): envía un paquete logrando establecer conexión con la máquina objetivo.
-PU (lista de puertos): permite observar que dispositivos se encuentran online u offline.
-PR (ping ARP): realiza este escaneo cuando se detecta una red local.



Hardening

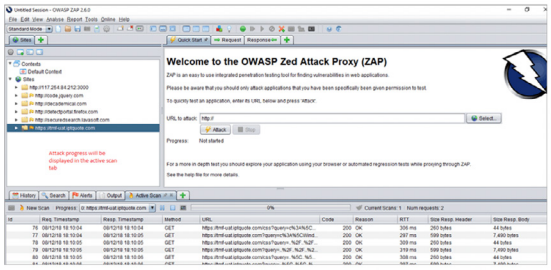
Este método permitió a la investigación configurar y desarrollar técnicas para mejorar la seguridad en el servidor web. Los métodos necesarios que se utilizaron fueron: Http Trace, Eliminación de ETAG, Clickjacking attack, bloqueo de inyección XXS y X-Content-Type-Options

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

```
[root@localhost /]# yum install fail2ban
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
```

Fail2ban

-Función del servidor mejorado: modifica configuraciones incorrectas e incompatibles.
-Mejor seguridad: Permite la reducción de amenazas impidiendo la entrada de filtración de datos, ingreso no autorizado y acceso de malware.
Se usó esta herramienta para procesos de baneo al sitio web y jaulas para mitigarlas.
En las jaulas de http se desactivan componentes como: apache-nohome y apache-botsearch para evitar baneo o detención al sitio web, como también la configuración en mod_security para la protección al servidor web.
-Previene ejecuciones de bots, scripts, entre otros atacas de servidores
-Bloque direcciones IP temporalmente ingresos maliciosos

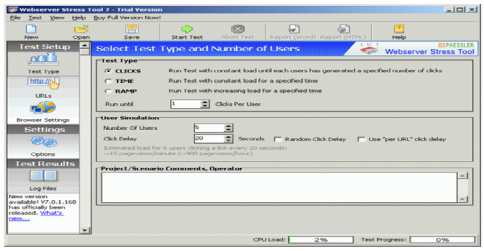


Fail2ban

-Gratuito
-Código abierto
-Realiza pruebas de penetración como SQL, XSS, descubrimiento de ficheros
-Ataques de fuerza bruta
-Organización sin fines de lucro
- Inyección
-Perdida de autenticación y gestión de sesiones
Este software permitió cumplir con la fase de recolección de información requerida por la metodología Owasp.

WPScan

Se utilizó esta herramienta para escanear la página con el gesto de contenido: Wordpress.
Cumpliendo de manera óptima con el escaneo de temas, plugins, usuarios, y hasta contraseñas generadas para la obtención del ingreso a la base de datos.
Comando utilizados como:
wpscan --url http://172.20.24.53:8080/wordpress --enumerate u
wpscan --url http://172.20.2.12 --enumerate vt



WebServer Stress Tool

Este software facilitó comparar con el servidor Apache y el servidor Microsoft IIS la cantidad de usuarios que pueden soportar si ingresan al mismo tiempo.

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Resultados y discusión

Los resultados obtenidos fueron positivos, las tareas ejecutadas para el análisis de vulnerabilidad han sido identificados de la manera más precisa. En este sentido se puede identificar los riesgos encontrados en los servidores web (antes y el después), el valor alcanzado de los sistemas operativos tanto para **Apache** como para **Microsoft IIS** y el resultado de la vulnerabilidades con mayor riesgo, tomando en cuenta el porcentaje de cada uno de ellos.

La meta principal de esta investigación fue diagnosticar los problemas de seguridad presentados hacia los servidores web, que se logró con la aplicación de la metodología Owasp (Proyecto de seguridad de aplicaciones web abiertas), que facilitó recolectar información con la utilización de pruebas y herramientas tales como: Owasp Zap, Nmap, SQLmap, Nessus, Acunetix, Hardening, Fail2ban, Nikto y WPScan. A partir de los cuales se manejó la configuración y desarrollo, manejo de identidad, validación de entradas, conjunto de actividades para reforzar la seguridad al servidor (Hardening) concluyendo con una fase final de los resultados conseguidos en el análisis de vulnerabilidad, de esta manera se compararon los riesgo con mayor impacto y las amenazas presentes en los servidores web, estas vulnerabilidades son las siguientes

- Con el porcentaje superior a 7% son: fuerza bruta, Cross Site Scripting, Método Http y manejo de identidad.

- Con el porcentaje inferior al 6% son: Manejo de configuración y desarrollo, Owasp/ directorios visibles, inyección SQL y Denegación de servicios DoS.

Todo este proceso dio como resultado la identificación de amenazas latentes en los servidores, tomando en cuenta que aquellas que encuentran sobre el 8% son vulnerabilidades que deben ser corregidas a tiempo para evitar daños, robos y ataques al sistema. Por otra parte, una vez concluido y obtenido los resultados de las vulnerabilidades se procedió a realizar una escala de cumplimiento de riesgos con el fin de comparar y evaluar mediante un checklist el nivel de seguridad que se obtuvo antes y después de los procesos realizados en la investigación, en este sentido se logró aumentar el nivel de seguridad a los servidores web en un 60%. Finalmente se establece una propuesta que responda los levantamientos de seguridad y brinden a los servicios de aplicaciones y servidores web una mejora de seguridad en sus sistemas informáticos.

Tabla 1.
Escala de cumplimiento y riesgos: ***Antes.***

	Riesgo		
	Alto	Medio	Bajo
No cumplen: 11	5	5	1
Sí cumplen: 4	-	3	1

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Tabla 2.
Escala de cumplimiento y riesgos: **Después.**

	Riesgo		
	Alto	Medio	Bajo
No cumplen: 6	1	5	-
Sí cumplen: 9	-	3	6

En la escala de cumplimento y riesgos se reflejó un 73,34% de incumplimiento a los indicadores, tomando en cuenta que la evaluación se la realizó antes de ejecutar la metodología Owasp y sus procesos, posteriormente se logra un 60% de mejora, disminuyendo las vulnerabilidades y amenazas del servidor.

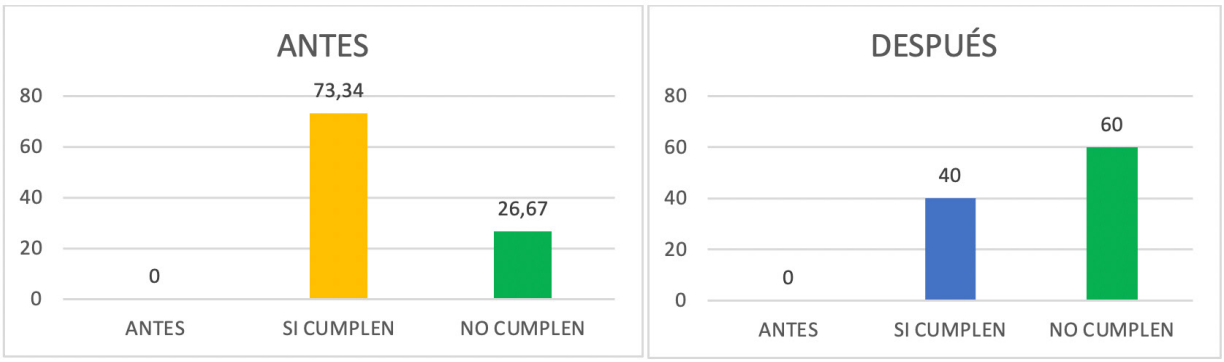


Figura 1. Cumplimiento de riesgos

Se identificó mediante un cuadro comparativo y una evaluación de las características a los sistemas operativos obteniendo como resultado el valor alcanzado, ver tabla 3.

Tabla 3.
Valor alcanzado.

Valor Alcanzado	
Apache	80%
IIS	30%

Identificación de la vulnerabilidades mediante los procesos tomados de la metodología OWASP, obteniendo como resultado vulnerabilidades con riesgos baja, media y mayor grado de amenaza, tabla 4.

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Tabla 4.
Resultado de la vulnerabilidades.

Comparación Final de las Vulnerabilidades según OWASP	
Manejo de configuración y desarrollo	5,33%
Manejo de identidad	8%
Fuerza bruta	7%
Owasp/ vulnerabilidad a directorios	4,67%
Cross Site Scripting	7%
Inyección SQL	5%
Sobrecarga de Buffer (DOS)	5%
Método Http	8%

Fórmula: Valor de Riesgo = Promedio (explotabilidad + prevalencia + detección) * impacto

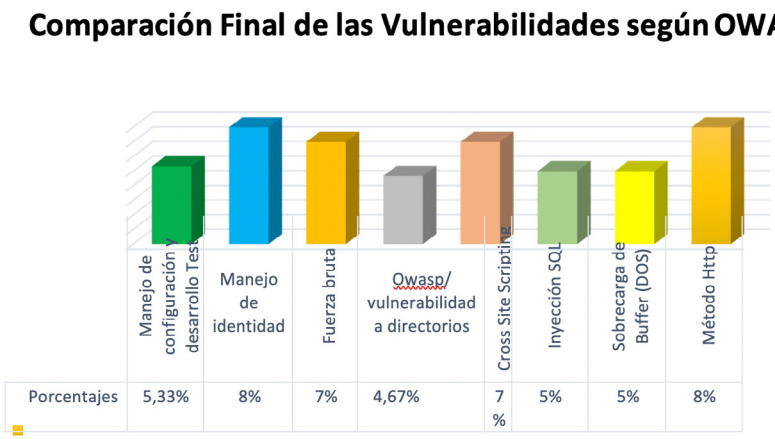


Figura 2. Comparación de vulnerabilidades

Finalmente se verifica con una matriz de trazabilidad para dar solución a las amenazas encontradas en los servidores web.

Tabla 5.
Matriz de trazabilidad de soluciones a las vulnerabilidades identificadas

anti-clickjacking X-Frame-Options	Header always append X-Frame-Options SAMEORGIN
X-XXS-Protection Header	Header always set X-XSS-Protection “1, mode=block”
X-Content-Type-Options Header	Header always set X-Content-Type-Options “nosniff”
Http Trace	TraceEnbale Off ServerSignature Off SererTokerns Pro[uctOnly]: / ServerTokens Full ServerTokens Major / ServerTokens OS

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Con estos resultados se ha demostrado que el servidor web más factible a la hora de su configuración e instalación fue para Apache con el 80% del valor alcanzado, además las vulnerabilidades detectadas con mayor riesgo están por encima del 7% como son: fuerza bruta, manejo de identidad, Cross Site Scripting y Método Http. Sin embargo, las vulnerabilidades que presentan menos del 6% como son: Inyección SQL y Denegación de servicio DoS también deben ser protegidas mediante configuraciones adecuadas a los servidores web, con el fin de evitar que se produzcan daños al sistema. Por otra parte, hubo un aumento de seguridad mediante una escala de cumplimiento del 60%, en comparación de los resultados obtenidos en las tablas 1 y 2. Finalmente, se realiza una matriz de trazabilidad para dar solución a las amenazas detectadas. Con los resultados expuestos se ha formado una referencia para trabajos futuros que pueden tomar como base el diagnóstico de los problemas de seguridad en los servidores, para analizar el posible impacto de su implementación en el área de estudio o en otros departamentos, organizaciones afines que estén relacionadas con los procesos de seguridad estudiados.

Conclusiones

A través de la aplicación de instrumentos de recolección de datos se estableció una relación con los procesos de seguridad existentes en los servidores web, y parámetros clave de las vulnerabilidades presentes y la manera en que pueden afectar. Además, se realizó un análisis de seguridad mediante parámetros de evaluación para la identificación de vulnerabilidades y así ejecutar procesos de seguridad como Hardening que permiten reducir el riesgo de amenaza en el servidor web. El uso de la metodología Owasp (Open web Application Security Project) facilitó en la organización sus procesos para el cumplimiento de las fases de seguridad, con las cuales se identificó y disminuyó los riesgos más relevantes que presentaron los sistemas. Finalmente, la utilización de criterios de evaluación y escala de cumplimento de riesgos permitieron en la investigación obtener resultados óptimos al momento de cumplir con los indicadores de evaluación con un aumento de seguridad del 60%.

Recomendaciones

La investigación está encaminada hacia el desarrollo de una propuesta, de esta manera se recomienda ampliar el proceso investigativo tomando como referencia la documentación generada en este proyecto y estudiar la posible implementación en otras organizaciones similares y medir el impacto real que pueden causar los atacantes cibernéticos. Por otra parte, dar a conocer mediante conferencias pautas de seguridad, donde se recomiende a los analista de aplicaciones y servidores utilizar herramientas como Owasp Zap, para resolver las vulnerabilidades y alcanzar soluciones optimas. Dentro de la metodología Owasp es recomendable mantener el análisis de vulnerabilidades de forma constante para comprobar de manera más efectiva y verdadera que los procesos se ejecuten de forma esperada cumpliendo con las pruebas de resultado. Finalmente es recomendable basarse en indicadores de riesgos y herramientas Open Source para tener diferentes tipos de procesos de seguridad en calidad de los sistemas informáticos.

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138

Referencias

Briones, G., y Hernández, E. (2018). *Auditoría de Seguridad del Servidor Web de la Empresa Publinext S.A. Utilizando Mecanismos Basados en OWASP* (tesis de grado). Universidad de Guayaquil. Ecuador http://repositorio.ug.edu.ec/bitstream/redug/26837/1b-cint-ptg-n.249%20briones%20pincay%20gerson

Hidalgo, J. (2015) Diseño de una red Wi-Fi para proporcionar servicios de una ciudad digital para Tulcán (Tesis de grado). Pontificia Universidad Católica del Ecuador, Quito. Ecuador http://repositorio.puce.edu.ec/handle/22000/7661

Pérez, C., y Quiñones, J. (2017). *Uso de herramientas de pentesting para el análisis de vulnerabilidades en las comunicaciones móviles de las operadoras ubicadas en la ciudad de Guayaquil (*Tesis de grado). Universidad de Guayaquil. Ecuador http://repositorio.ug.edu.ec/bitstream/redug/22444/1/B-CINT-PTG-n.190.p%c3%a9rez%20falcon%c3%ad%20carolina%20victoria.qui%c3%b1ones%20mo nta%c3%b1o%20jairo%20alexander.pdf

Consultores en Seguridad de la Información. (2016). Seguridad Informática vs Seguridad de la Información. Recuperado el 03 de marzo de 2017, de https://www.maestrodelacomputacion.net/seguridad-informatica-seguridad-de-la-informacion/

Gonzalez, J. (2011). ¿Seguridad Informática o Seguridad de la Información? Recuperado el 02 de febrero de 2016, de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-oseguridad-de-la.html

ISOTools Excellence. (2017) ¿Seguridad informática o seguridad de la información? Recuperado el 05 de marzo de 2017, de http://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Rojas Valduciel, H. (2016). Seguridad de la Información, Seguridad Informática y Ciberseguridad: ¿Son sinónimos? Recuperado el 20 de febrero de 2017, de https://infobyteabyte.wordpress.com/2016/04/20/seguridad-de-la-informacion-seguridadinformatica-y-ciberseguridad-son-sinonimos/

Cómo citar este artículo:
Castillo, A,. Hidalgo, J. & Guano, C. (Julio - Diciembre de 2022). Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi. *Sathiri* (17),2 177-189. https://doi.org/10.32645/13906925.1138