UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ESTRATEGIA PARA LA EVALUACIÓN DE VULNERABILIDADES DEL SISTEMA DE NOTAS UTILIZANDO TÉCNICAS DE HACKING ÉTICO EN LA ESCUELA MAHATMA GANDHI

ESTUDIO DE CASO:

CARLOS ARATH CAMPI DOMINGUEZ

TUTOR:

ING IVÁN RUBÉN RUIZ PARRALES

AÑO 2023

Contenido

1. PLANTEAMIENTO DEL PROBLEMA

Gracias al rápido desarrollo de la tecnología y de Internet, la divulgación y protección de la información se ve directamente afectada por los estándares de seguridad. Las amenazas a la seguridad de la información continúan creciendo hasta el punto en que no se puede decir que un sistema informático sea inmune a los ataques cibernéticos.

Actualmente, según OWASP, los ataques más comunes contra aplicaciones web son URL semánticas, cross-site scripting, falsificación de solicitudes entre sitios, solicitudes HTTP falsificadas, inyección SQL, etc. [4].

Sin embargo, las empresas están poniendo más énfasis en hacer que sus aplicaciones informáticas sean eficientes, rápidas, usables, accesibles e inclusivas, pero pocas se preocupan por incluir la seguridad necesaria. De esta manera, la integridad, confidencialidad y disponibilidad quedarán expuestas, generando consecuencias como pérdidas financieras, adquisición y robo de información privada, retrasos en la ejecución y gestión de procesos.

Según ITRC Data Breach , la distribución de informes de ataques en 2018 fue la siguiente: empresas privadas 46%,instituciones de salud 29%, instituciones financieras 11%, entidades públicas 1,8% e instituciones educativas 6%. Esto demuestra que las instituciones educativas son uno de los grupos vulnerables a los ataques tecnológicos.

Además, el portal fue visitado por la comunidad educativa para ver y manipular información, académica, y, el.ataquelogró realizar cambios que provocaron que algunos servicios dejaran de funcionar temporalmente.

Existe desconocimiento en relevante para impedir que pueda tener la vulnerabilidad del sistema de notas ya que estas no presentan sus técnicas En la Unidad Educativa Mahatma Gandhi,, Por lo tanto, es importante establecer estrategias para la evaluación de vulnerabilidades del sistema de notas por parte de usuarios no autorizado para este trabajo se utilizará Owasp, un escáner de vulnerabilidades de uso libre, para la identificación y corrección de fallas de seguridad

El gestor es el servicio que realiza a cabo las tareas como el filtrado **o** clasificación de los resultados del análisis que se realizara, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles. Por su lado, el escáner ejecutara, las pruebas de vulnerabilidades de red, conformadas por rutinas que comprueban la presencia de un problema de seguridad específico conocido o potencial en los sistemas.

2. JUSTIFICACIÓN

El presente caso de estudio permite realizar un análisis y evaluación de las vulnerabilidades en el sistema de notas de la escuela Mahatma Gandhi, con el conocimiento y la información adquirida, se creará una estrategia que sirva para establecer las vulnerabilidades existentes en la aplicación académica.

Las instituciones educativas, en la actualidad se han visto en la necesidad de resguardar la información de los estudiantes, teniendo que procesar y generar un sistema de anotación, lo cual es una herramienta de utilidad, dentro del proceso académico

Para certificar que se establezca este procedimiento, el análisis debe pasar las siguientes etapas:

- Reconocimiento
- Escaneo
- Obtención de acceso
- Mantener el acceso
- Cubrir o Borrar huellas

Entre los principales ataques informáticos podemos nombrar, los ataques de monitorización el mismo que permite observar a la víctima y a su sistema de información, ataques de validación mediante el cual se suplanta la identidad del usuario, tomando sus credenciales de acceso al sistema, ataque de denegación de servicios en el que se pretende colapsar los recursos de la víctima con el propósito de impedir los servicios ofrecidos por el mismo.

Posteriormente, el ataque de modificación tiene como finalidad la manipulación no autorizada de la información de los sistemas de información de la víctima. Las aplicaciones de auditoria informática que más se utilizan para el hacking ético son Kali Linux y OWASP debido a que forman un ambiente apropiado para la analítica y el pentesting esperado.

3. OBJETIVOS

• Objetivo general

- Desarrollar una estrategia para la evaluación de vulnerabilidades del sistema de notas utilizando técnicas de hacking ético en la Escuela Mahatma Gandhi

• Objetivos Específicos

- Investigar las técnicas de hacking ético para la evaluación de vulnerabilidades en sistemas informáticos.
- Estudiar las vulnerabilidades que afectan directa e indirectamente a el sistema de notas en la Escuela Mahatma Gandhi
- Evidenciar las vulnerabilidades encontradas por cada técnica de hacking ético realizado al sistema informático de notas.

4. LÍNEA DE INVESTIGACIÓN

Este presente caso de estudio se encuentra enmarcado en la línea de investigación de establecida por la carrera, la misma que se refiere a los sistemas de información y comunicación, emprendimiento e innovación.

La sublínea de investigación está relacionada a las redes y tecnologías inteligentes de software y hardware.

5. ARTICULACION DEL TEMA

El presente estudio de caso se encuentra articulado con las practicas realizadas en vinculación con la comunidad, las cuales realice en la unidad educativa Aldon Calderón muñoz, encontrándome con falencias suscitadas en el sistema académico de la institución, por lo cual me pareció interesante la realización de estrategias para la evaluación de vulnerabilidades del sistema de notas utilizando técnicas de hacking ético en la escuela Mahatma Gandhi.

6. MARCO CONCEPTUAL

1. • Que son las estrategias

Mero variado de practicas que permiten a una empresa hacer mejor uso de sus insumos, disminuyendo, Por ejemplo, Los defectos de los productos o desarrollando mejores productos con mayor rapidez. Por el contrario, el posicionamiento estratégico implica realizar actividades diferentes de aquellas de los rivales o bien realizar actividades similares de manera diferente. (porter, 2021, p.4)

es un plan general para lograr uno o más objetivos a largo plazo o generales con el fin de realizar mejor la actividad, pero con un mejor tiempo, pero será similar lo que se realizará asi se obtendrá mejor resultado

2. • Que es la evaluación

Actualmente, la evaluación es un concentrado de evidencias que permiten obtener información valiosa del desempeño de los alumnos en relación a los objetivos planteados. Asimismo, la evaluación como parte del trabajo docente, muestra una secuencia construida a lo largo de un tiempo determinado, es decir, por bimestre, por semestre, o anual. (fernandez, 2018).

Es un proceso que determina el tipo de conocimiento en conclusión es como. Una evaluación de impacto y se verifica el rendimiento de una persona al valor de algo o de alguien.

3. • Vulnerabilidades

En primer lugar, alguien vulnerable es alguien susceptible de ser dañado o herido. Así lo indica su evolución etimológica: el vocablo latino vulnus, -eri significa «herida, golpe» y también «desgracia, aflicción». (liedo, 2021, p. 244)

Es decir, este puede ser dañado tanto fisica o mentalmente sin tener la suficiente fuerza y debido a eso no opta por ser estable

4. ● Escaneo de vulnerabilidades*.*

Metodologías de auditoria: está utilizando, los firewalls, los sistemas de detección de intrusos, los diferentes servidores y servicios que se ejecutan en esos servidores, dispositivos de límites, topologías de enrutamiento y otras topologías utilizadas en la red de la organización objetivo. Al utilizar la técnica de foot printing, podemos rastrear la dirección IP de la organización objetivo. Una vez que se encuentra la dirección IP, la exploración de los puertos TCP y UDP del sistema de destino se vuelve bastante fácil para el hacker ético para mapear la red **(**SANCHEZ, 2019, p. 5)

5. ● Evaluación de vulnerabilidades de notas

Una de estas brechas se ubica en el rendimiento académico alcanzado por las instituciones como medida de la calidad educativa, hecho que se evidencia en los procesos de aprendizaje que promueve la escuela, los cuales deben garantizar a todos sus estudiantes las mismas oportunidades para acceder a los conocimientos, teniendo en cuenta sus estilos de aprendizaje, sus diversas capacidades, el contexto social y cultural de procedencia; esperando que los resultados no afecten la aprobación de cursos o asignaturas. (cortes, 2018, p. 10).

6. • *Sistemas de notas*

Tiene como objetivo central obtener su propio Sistema de Gestión de Notas, que suministre la información clara, concisa e inmediata a los docentes del centro educativo y así lograr resolver todas las dificultades relacionadas con el mismo, a través de un modelo lineal secuencial (Ramos, 2020, p. 17)

En conclusión, es el medio utilizado por las instituciones educativas para expresar los resultados de una evaluación. Hay quienes lo consideran arbitrario, ya que depende del criterio

7. ● ¿Que son las técnicas de hacking ético?

Según (darias, 2023) “se define como aquellas prácticas realizadas por profesionales o también denominados *hackers éticos de la seguridad*, con el objetivo de ayudar a las empresas a identificar vulnerabilidades que puedan poner en riesgo la protección de sus sistemas.

Por lo consiguiente, muchas empresas y las instituciones se preocupan cada vez más por referir con defensas resistentes que les permitan exceder los posibles ataques a los que deban hacer frente y que, en muchos sucesos, se pueden evitar por medio del hacking ético. (Obregón, 2018).

8. ● Funciones

El procedimiento del hacking ético por lo general esta empieza con el resumen de información que se va a llevar a cabo sobre los sistemas que se tomara la respectiva evaluación. El hacker ético usaría unas de sus herramientas una de ellas es el escaneo para guardar los datos y sus sistemas con fallas (tejedor, 2023).

Después de generar la información el hacker ético explorar las vulnerabilidades del sistema eso involucraría el rendimiento de vulnerabilidades este hacking ético es considerado muy importante en todo el mundo por los beneficios que realiza de acuerdo a la información sería muy interesante porque ayudaría a los sistemas de instituciones como sería el caso de la institución que se ejecutaría (galarza, 2020, p. 4).

9. • ¿En qué consiste un ejercicio de hacking ético? Conozcamos sus fases

1. **Reconocimiento** (Investigación y recolección de información)
2. **Escaneo** (Identificación de vulnerabilidades)
3. **Obtención de acceso** (Explotación de vulnerabilidades)
4. **Mantener acceso** (Despliegue de puertas traseras y obtención de privilegios administrativos del sistema)
5. **Eliminación de evidencias** (Eliminación de huellas sobre la intrusión al sistema) (darias, 2023).

10. ● Tipos de Hacker que existen

- **Los White Hat o hackers de sombrero blanco**, son todos aquellos profesionales que realizan buenas prácticas con el objetivo de mejorar la seguridad empresarial y detectar continuamente brechas en ella.
- **Los Black Hat o hackers de sombrero negro,** hace referencia cuyos propósitos son la infección de sistemas mediante malwares, robo de datos, paralización de servicio u obtención de ganancias financieras.

- **Los Grey Hat o hackers de sombrero gris, se** sitúan entre el bien y el mal. Hablamos de un perfil que no tiene reparos en realizar una actividad ilegal. (darias, 2023).

11. • IMPACTO DEL HACKEO ÉTICO EN LA SOCIEDAD

. Impacto en la educación

Muchas personas o jóvenes que están iniciando en el proceso de aprendizaje dentro de las diferentes áreas de tecnología, tienden a investigar y a complementarse en diferentes procesos de la sociedad que pueden influir con la tecnología (Redes sociales, páginas web, bases de datos etc), con ello adquieren muchas destrezas, permitiendo mejorar su entendimiento sobre la sociedad y cobertura de información que se puede estar generando en el mundo. (SANCHEZ, 2019, p. 7).

- **. Impacto en la sociedad.**

Con el apoyo de la tecnología toda la información se crea, modifica y envía de forma electrónica. Debido a esta razón, se puede decir que todas las transacciones comerciales se realizan de forma electrónica. Con el crecimiento de la Internet, existen una serie de sitios web de compras y subastas que influyen en los clientes para vender sus productos en línea. Estos sitios están dando muy buenas ganancias y agilizan en la adquisición de nuevos productos sin importar la ubicación de los clientes (SANCHEZ, 2019, p. 7).

- **. Impacto en la Tecnología.**

El hacker ético puede obtener fácilmente las direcciones IP de cualquier sistema y dañarlo. Para los hackers éticos, existen muchas herramientas disponibles en el mercado global para ayudarles a realizar su trabajo de manera efectiva. (SANCHEZ, 2019).

-Escaneo de Red. En el escaneo de la red se identifican todos los hosts activos que están presentes en una red. El propósito de este ejercicio es atacarlos o evaluar la seguridad de la red. (SANCHEZ, 2019)

En el escaneo de vulnerabilidades, el hacker ético conocerá el sistema operativo del sistema y otros detalles relacionados con el sistema operativo, como su versión, el paquete de actualización, si está instalado. El escáner de vulnerabilidades identificará la debilidad del sistema operativo para que luego pueda ser atacado. El escaneo de vulnerabilidades generalmente se refiere al escaneo de sistemas que están conectados a Internet. (SANCHEZ, 2019, p. 5).

- **Impacto en la información confidencial.**

Un informe reciente reveló que el spam contribuyó con el 70% de todos los correos electrónicos en Internet [7]. Es realmente un gran problema para un hacker ético rastrear todos los escenarios. A veces se observa que tener acceso a la cuenta en efecto culpará a un hacker ético incluso si no han hecho nada. Es realmente muy importante saber que el hacker es diferente del hacker ético. A veces, para un hacker ético se vuelve tan difícil demostrar que él no es el responsable. (SANCHEZ, 2019, p. 8)

¿Qué es el OWASP ZAP?

(Zed Attack Proxy) es el escáner web de vulnerabilidades más utilizado en todo el mundo, es completamente gratuito y de código abierto, por tanto, podrás adaptarlo a tus necesidades. Este programa es mantenido activamente por una comunidad internacional de voluntarios, los cuales trabajan para ir mejorando la herramienta poco a poco y también incorporando nuevas características. Hoy en RedesZone os vamos a enseñar todo lo necesario para comprobar la seguridad de tu web para evitar vulnerabilidades que pongan en riesgo tu servidor y tus datos. (genes, 2021)

Metodología OWASP

Es una organización muy transversal, como tal establece metodologías para la securización de aplicaciones web en todo el ámbito del ciclo de desarrollo del software. Todo lo explicado en la sección 3 - Testing de aplicaciones web está basado en la guía de testing de OWASP [20]. Por lo tanto, forma parte de la metodología de OWASP, pero no es la única, existen más referencias. Por ejemplo, una guía completa para desarrolladores, además de varios artículos de menor tamaño que complementan a estos dos. (gonzales, 2020)

Principales características de OWASP ZAP

Lo primero que debemos indicar es que OWASP ZAP no es una herramienta comercial, es completamente gratuita y de código abierto, además, es una herramienta multiplataforma, siendo compatible con sistemas operativos Windows (de 32 y 64 bits), Linux, MacOS, e incluso podemos descargarnos un contenedor Docker que incorporará todo lo necesario

para ejecutarlo correctamente. Este programa es muy sencillo de instalar, tan solo necesitaremos tener Java instalado en nuestro equipo para poder ejecutarlo, otras características son que esta herramienta está traducida en más de 12 idiomas entre los que se incluye el español. (genes, 2021)

¿Por qué usar OWASP?

Las aplicaciones web son un objetivo habitual para los ataques cibernéticos. Las vulnerabilidades de seguridad web pueden dar lugar a la pérdida de datos, el robo de identidad y otros daños. La importancia de OWASP radica en su papel fundamental en la defensa contra las crecientes ciberamenazas (garcia, 2022).

¿La aplicación es vulnerable?

Una aplicación es vulnerable a ataques de este tipo cuando:

• Los datos suministrados por el usuario no son validados, filtrados o sanitizados por la aplicación.

• Se invocan consultas dinámicas o no parametrizadas, sin codificar los parámetros de forma acorde al contexto.

• Se utilizan datos dañinos dentro de los parámetros de búsqueda en consultas Object-Relational Mapping (ORM), para extraer registros adicionales sensibles

. • Los datos dañinos se usan directamente o se concatenan. (blog owasp, 2019)

Estándar de verificación de seguridad de aplicaciones OWASP

El estándar proporciona una base para diseñar, construir y probar controles de seguridad de aplicaciones técnicas, incluidas cuestiones de arquitectura, ciclo de vida de desarrollo seguro, modelado de amenazas, seguridad ágil que incluye integración/implementación continua, sin servidor y cuestiones de configuración. (github, 2020)

OPEN WEB APPLICATION SECURITY PROJECT OWASP

La guía de pruebas de seguridad de aplicaciones web de OWASP propone una metodología de pruebas de intrusión, se basa en el enfoque de caja gris. El probador no sabe nada o tiene muy poca información sobre la aplicación a probar, y las divide en dos fases.

- **Pruebas pasivas**

Se pretende comprender la lógica de la aplicación y los puntos de acceso de la aplicación web.

- **Pruebas activas**

Durante las pruebas activas un probador comienza a utilizar las metodologías descritas en diferentes secciones. (carvaca, 2022)

7. MARCO METODOLOGICO

- ## Diseño de investigación

El diseño de la investigación es de tipo descriptivo, por cuanto es un método que permite observar y referir en base a la selección, análisis y exposición de datos extraídos de varias fuentes.

- ## Tipo de investigación

- **Investigación descriptiva**

Este estudio de caso no necesariamente se basa mostrar un informe detallado sobre el sujeto de estudio, amenazas y vulnerabilidades, sino que buscara establecer los diferentes criterios que existen respecto al objeto de estudio el cual se ejecutará por medio de diferentes técnicas.

- **Investigación de campo**

Esta investigación admite la interacción entre el objeto de estudio y herramientas tecnológicas en el área, para conseguir tener una información incontrastable que ayude a la recopilación de la información, en este caso en la escuela Mahatma Gandhi.

Método cuantitativo

A través de este método se recopilará información obtenida en base a la información procedentes de las encuestas los cuales serán demostrados en datos estadísticos para obtener a la deducción de la investigación, mismas que se realizaron en la escuela Mahatma Gandhi.

Técnicas de investigación

En este estudio de caso se utilizaron técnicas tales como

- **Observación**

Esta técnica admitió la percepción directa al objeto de estudio y en base a ello tomar información y registrar para su posterior análisis.

- **Encuestas**

La encuesta es quizás la técnica más eficaz, que se lleva a cabo a través de un cuestionario de preguntas a población determinada, la misma que se aplicó a los docentes de la escuela Mahatma Gandhi., en la cual se consiguió identificar varios criterios y necesidades.

- **Población**

La encuesta fue elaborada a 22 docentes de la escuela Mahatma Gandhi.

ESTRATEGIAS

Crear un plan que sirva de guía para elaborar de manera efectiva el análisis de vulnerabilidades realizando las siguientes actividades que son: identificar el alcance del análisis de vulnerabilidades, identificar los activos, análisis de amenazas y vulnerabilidades propias del sistema de notas, análisis del impacto y probabilidad y, finalmente, cálculo del riesgo.

Identificación del alcance

El estudio de vulnerabilidades en el sistema de nota de la institución educativa tiene como propósito generar una guía especifica que permita realizar este asunto analítico de forma secuencial, ordenada y documentada, teniendo indicadores que permitan realizar evaluaciones y prevenir ataques informáticos.

Identificación de los activos

estos, se describen los activos tecnológicos ya que cuenta la unidad educativa mahatma Gandhi. Los cuáles serán sometidos al análisis de vulnerabilidades de acuerdo con el alcance también la escuela cuenta con servicios en línea.

Secretaría académica

Este servicio en línea que también significa "secretaría académica", se encarga de los procesos para los ingresos, actualizaciones, reportes, encuestas, documentos de matriculación y coordinación de la evaluación al docente

Estudiantes

El servicio en línea para estudiantes permitirá consultar las calificaciones que pertenecen a los dos últimos periodos El estudiante podrá ingresar también a servicios para verificar sus respectivas notas por asignatura.

Docentes

Este otro servicio en línea permitirá al docente generar la información académica. Esta información será creada, analizada y actualizada dependiendo del evento que se vaya a realizar la que utilizarían con mayor frecuencia son: ingreso de notas y autoevaluación docente.

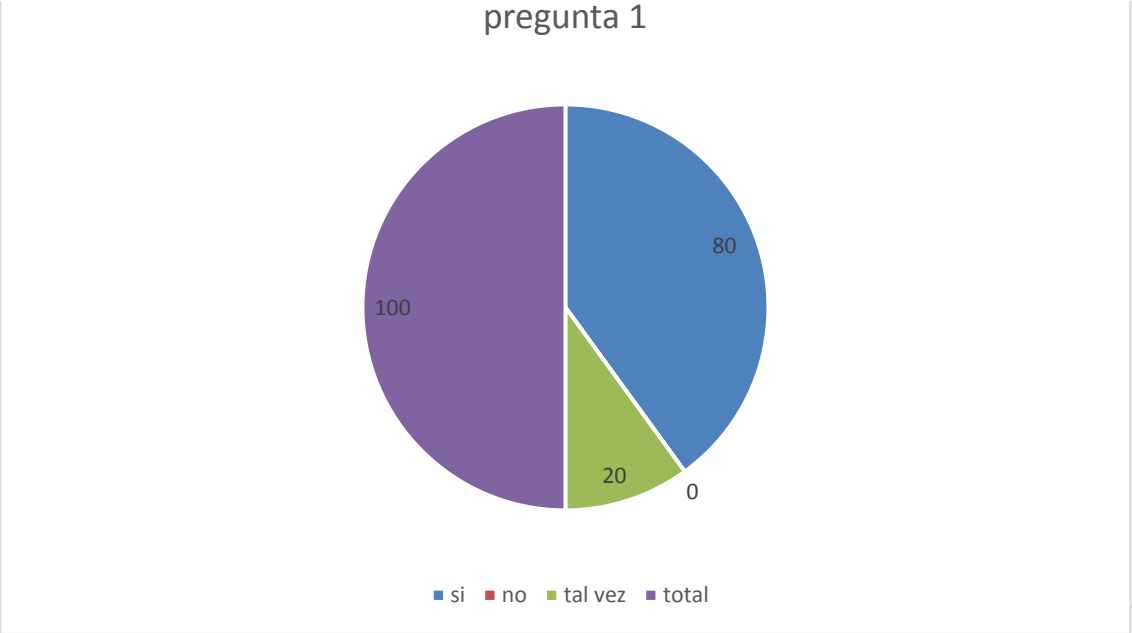
8. RESULTADOS

En la siguiente tabla se muestra el total de las personas encuestadas que son por directivos y docentes de la escuela Mahatma Gandhi

Tabla 1 Total de población encuestada

Población	Cantidad
directivos **docentes**	**10**

¿considera que es importante evaluar la seguridad de los sistemas de notas en la escuela mahatma Gandhi, especialmente en un entorno educativo en línea?



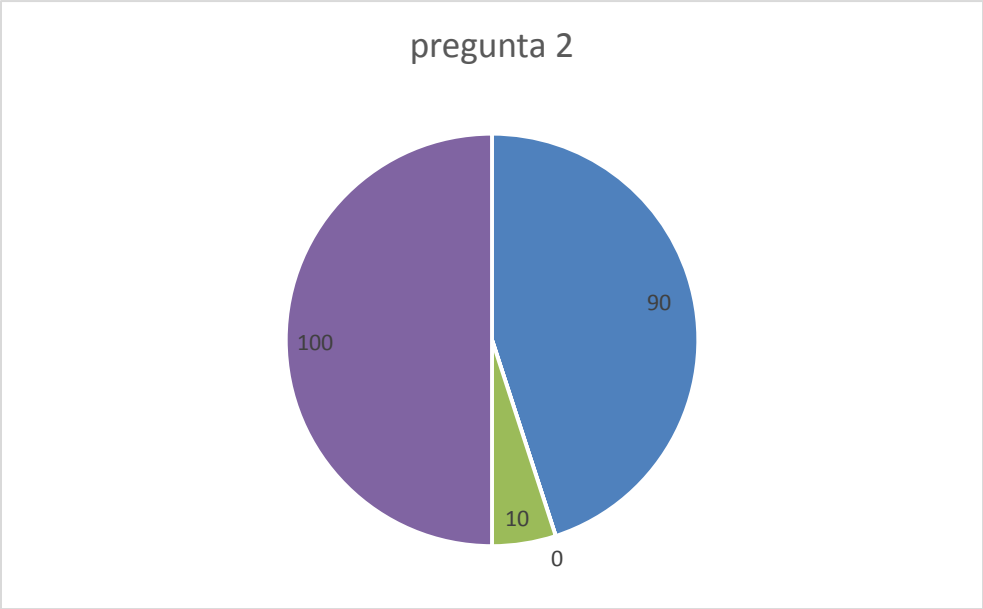
Fuente: Carlos campi

Del 100% de los encuestados el 80% si tienen conocimiento sobre evaluar la seguridad de los sistemas de notas en la escuela mahatma Gandhi, especialmente en un entorno educativo en línea ? , el 20% evaluó como tal vez y el 0 % evaluó no.

Si	80%
no	0%
Tal vez	20%
Total	100%

¿cree que la implementación de técnicas de hacking ético es una medida efectiva para identificar y corregir posibles vulnerabilidades en el sistema de notas de la institución?

Tabla 2 Tabulación pregunta 2Conocimiento



Fuente: Carlos campi

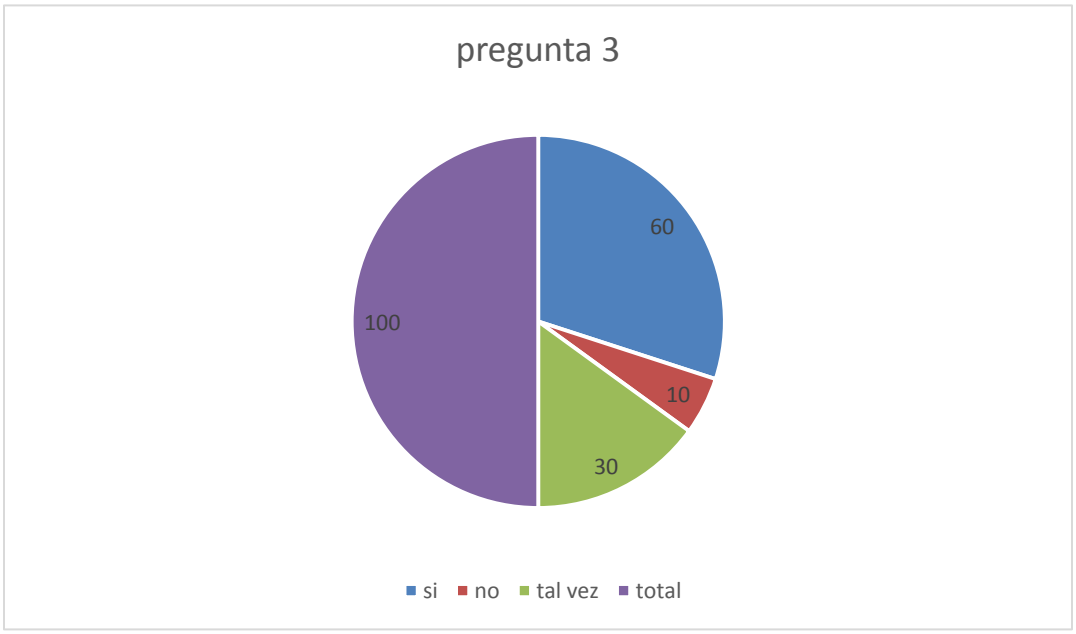
Del 100% de los encuestados el 90% si cree que la implementación de técnicas de hacking ético es una medida efectiva para identificar y corregir posibles vulnerabilidades en el sistema de notas de la institución, el 10% evaluó como tal vez de conocimiento y el 0% evaluó no.

Si	90%
no	0%
Tal vez	10%
Total	100%

¿existen preocupaciones éticas y legales que surgen al utilizar técnicas de hacking ético para evaluar la seguridad de los sistemas de notas en una institución educativa?

Tabla 3 Tabulación pregunta 3Conocimiento

Fuente: Carlos campi



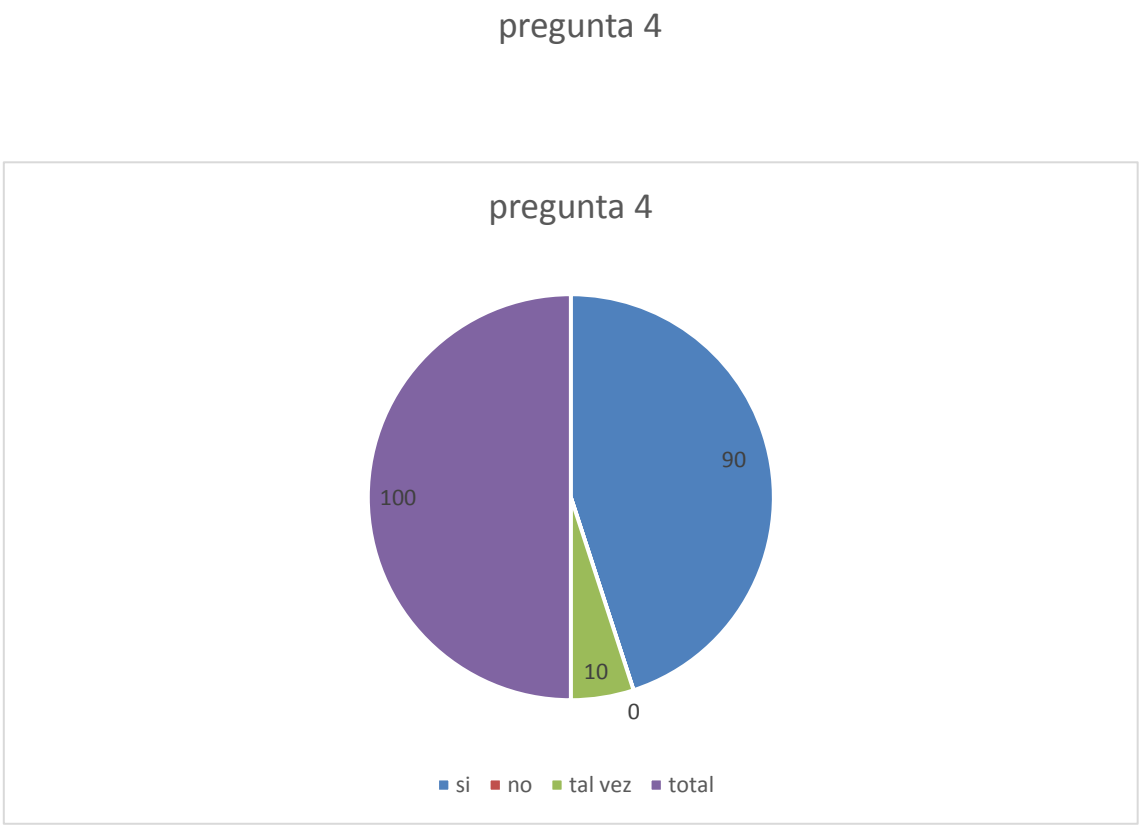
Fuente: Carlos campi

Del 100% de los encuestados el 60% si existen preocupaciones éticas y legales que surgen al utilizar técnicas de hacking ético para evaluar la seguridad de los sistemas de notas en una institución educativa sobre los problemas de los docentes de pasar las notas a los estudiantes, el 30% evaluó como tal vez y el 10 % evaluó como no.

Si	60%
no	10%
Tal vez	30%
Total	100%

¿piensa que los posibles beneficios de incorporar la evaluación de vulnerabilidades como parte de la estrategia de ciberseguridad en la escuela mahatma Gandhi superan los beneficio?

Tabla 4 Tabulación pregunta 4



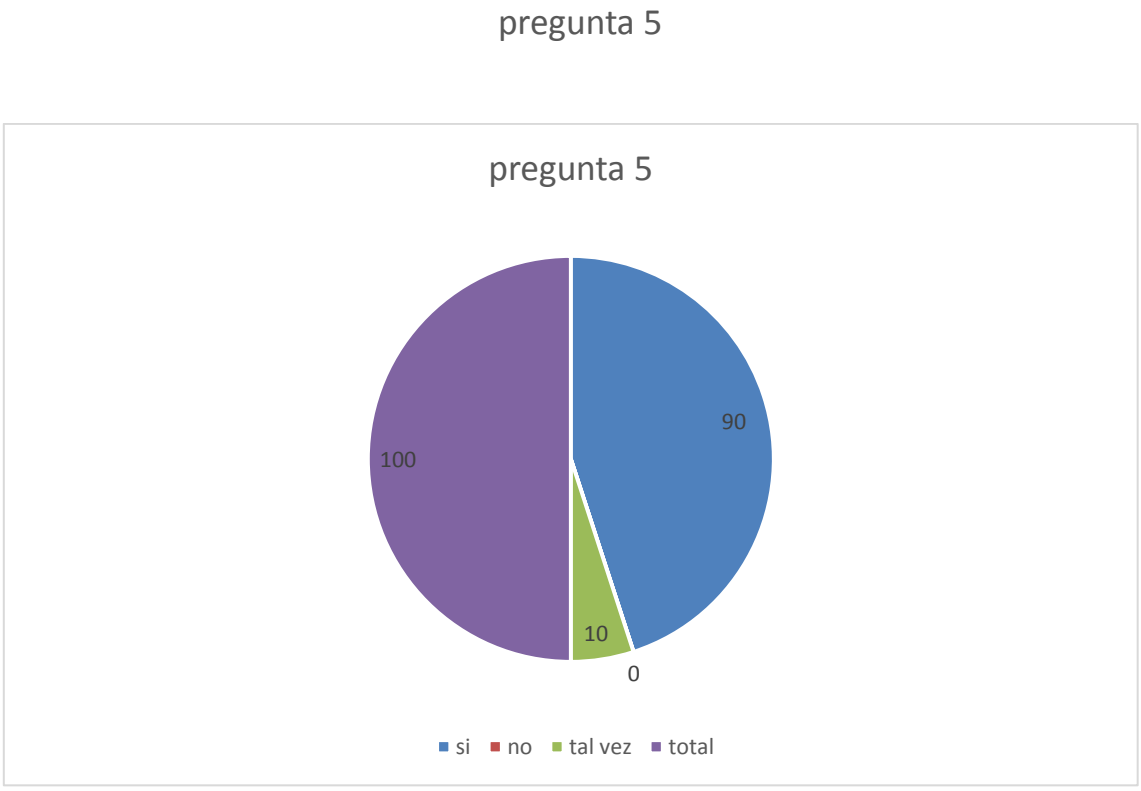
Fuente: Carlos campi

Del 100% de los encuestados el 90% si piensa que los posibles beneficios de incorporar la evaluación de vulnerabilidades como parte de la estrategia de ciberseguridad en la escuela mahatma Gandhi superan los beneficio el 10% evaluó como tal vez de conocimiento y el 0 % evaluó como no.

Si	90%
No	0%
Tal vez	10%
Total	100%

¿Cree que los resultados de la evaluación de vulnerabilidades se utilizaran de manera efectiva para mejorar la seguridad del sistema de notas y proteger los datos de los estudiantes en la institución?

Tabla 5 Tabulación pregunta 5

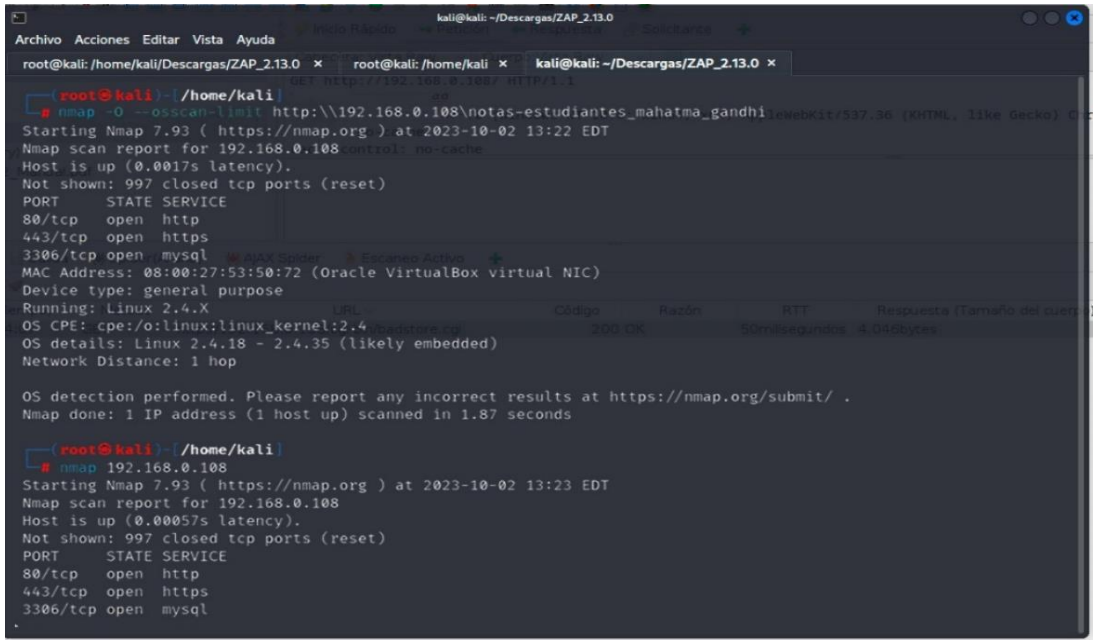


Fuente: Carlos campi

Del 100% de los encuestados el 90, % evaluó como si Cree que los resultados de la evaluación de vulnerabilidades se utilizaran de manera efectiva para mejorar la seguridad del sistema de notas y proteger los datos de los estudiantes en la institución el 10, % evaluó como tal vez y el 0 % evaluó como no.

si	90%
no	0%
Tal vez	10%
Total	100%

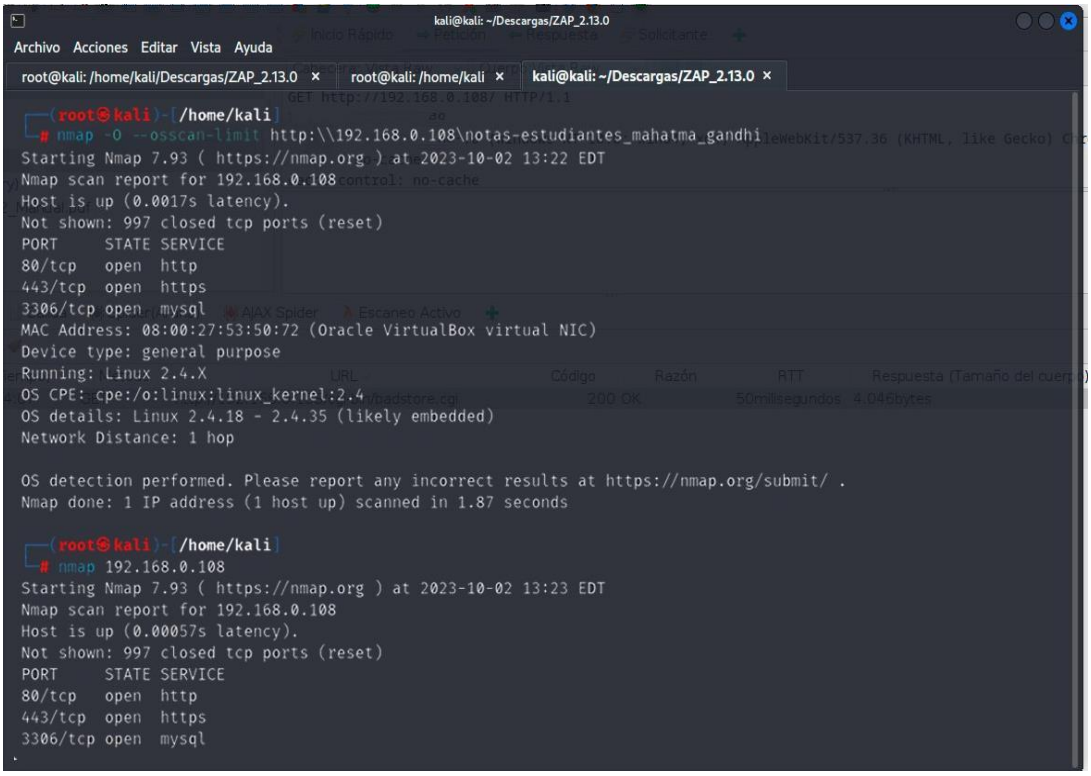
Imagen 1: Mapeo de puertos con Nmap, previo al uso de Owasp.



Fuente: 1 carlos campi

La ejecución de esta herramienta entregó la información sensible tal como la IP del servidor en la red local y demostró que el servidor es vulnerable, lo cual serán elaboraciones para la etapa de explotación de vulnerabilidades, por lo que el impacto es elevado debido a que ya presenta técnicas para el ataque y también muestra la IP del servidor dentro de su propia red.

Fuente: 2 Nmap vista previa

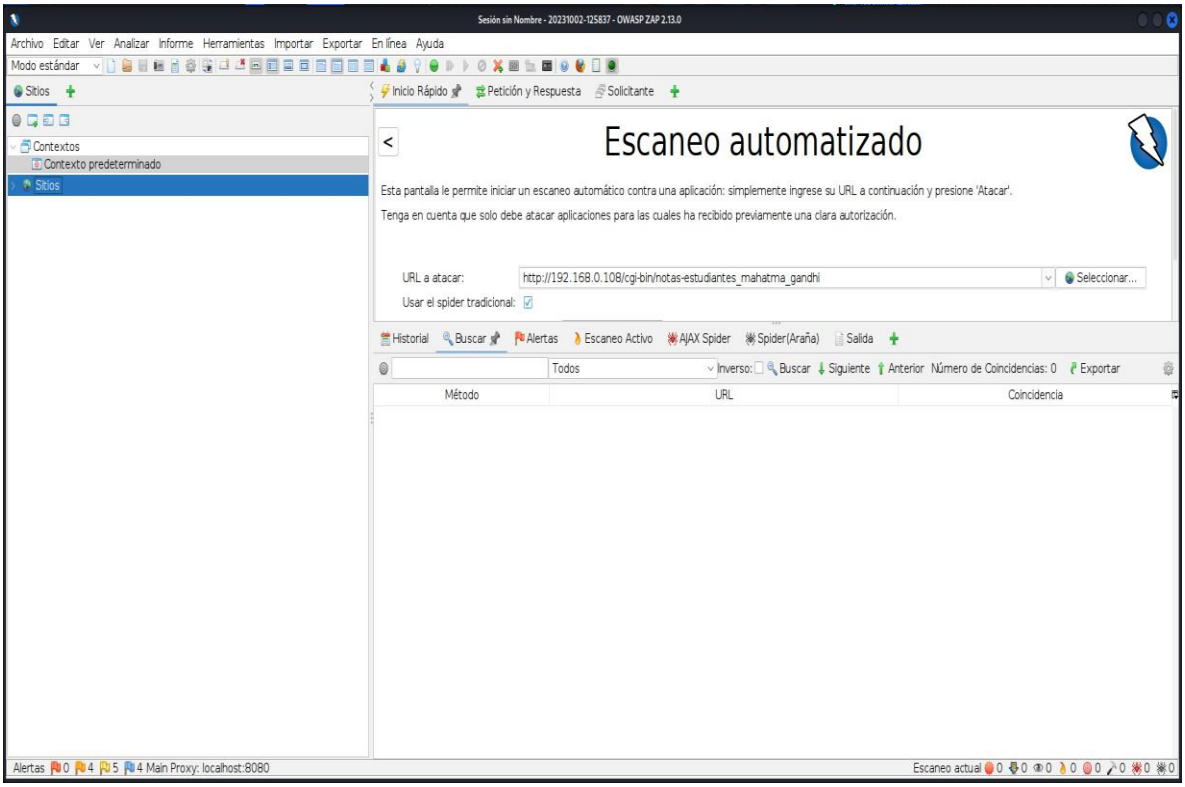


Fuente: 2 Carlos campi

Vista previa

Ya aquí en vista previa se sigue visualizando que la probabilidad de ocurrencia es media ya que se necesita un razonamiento técnico para la ejecución e interpretación de la herramienta y los respectivos resultados, por lo que el peligro se encuentra en una zona muy importante.

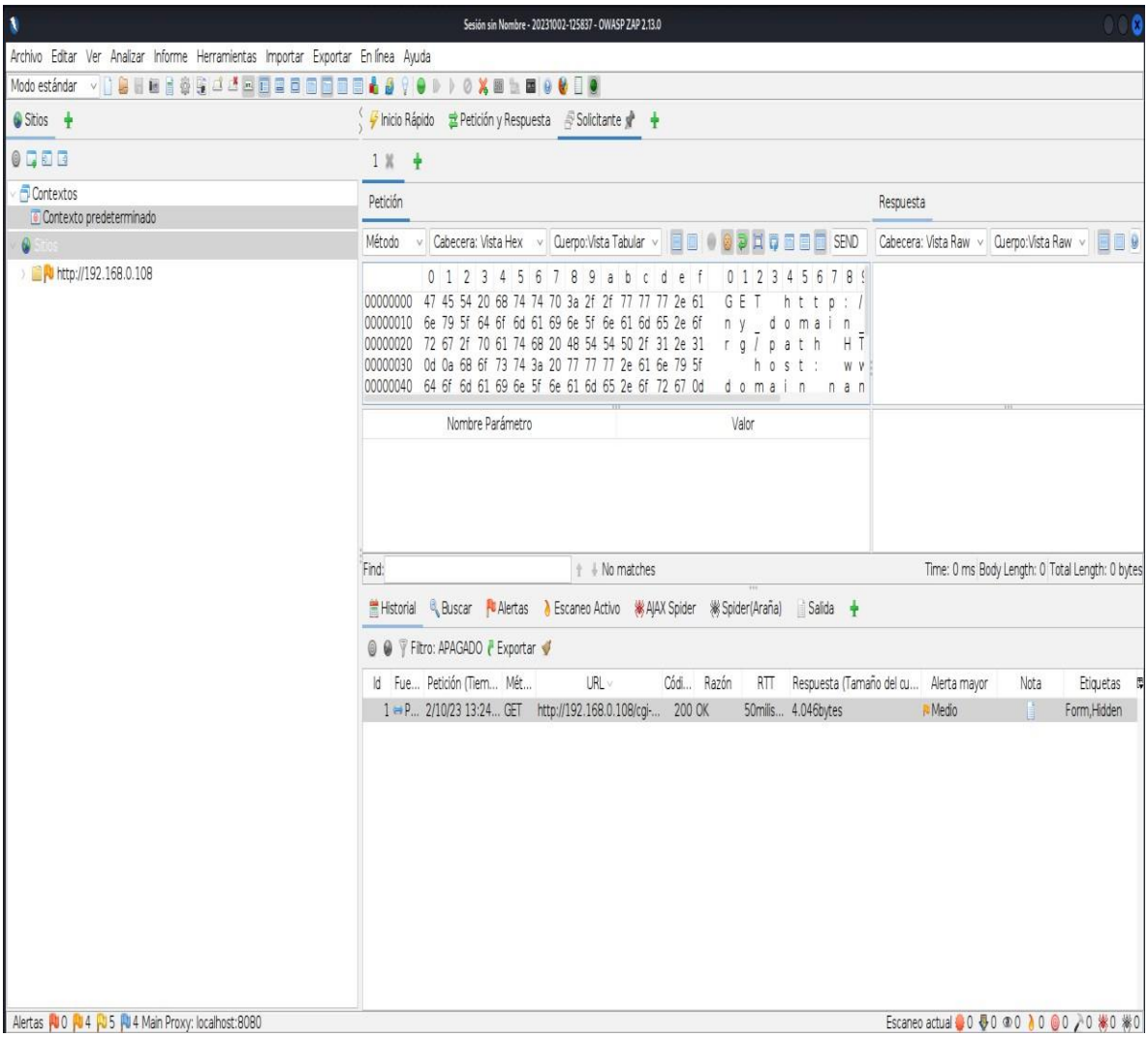
Fuente: 3 Inicio de análisis automático



Fuente: 3 carlos campi

El automatizado se coloca una url atacar usar el spidey tradicional y simplemente con el botón atacar despliega una seria de ataques para buscar vulnerabilidades dentro de esas url que se utilizó en donde en el apartado de historial búsqueda alerta escaneo spidey va a salir o a mostrarse en pantalla todas las vulnerabilidades que se encontró y las posibles soluciones a arreglar dentro de esas páginas web

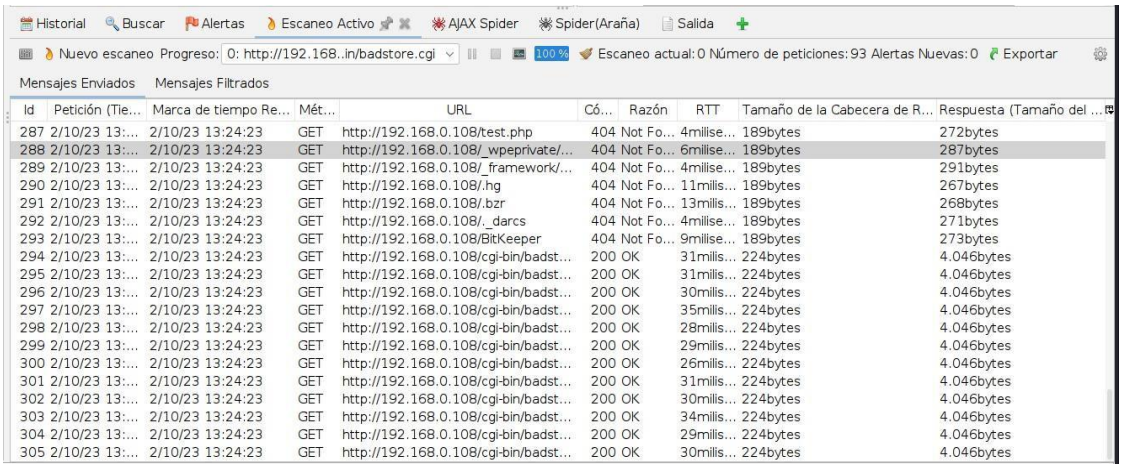
Fuente: 4 historial de análisis



Fuente: 4 carlos campi

Historial de análisis se está atacando la url que se ingresó enante como se puede ver ahí está la petición el tiempo el método get la url el código el rtt el tiempo de respuestas en tamaño bytes si es medio bajo o alto en este caso salió medio.

Fuente: 5 escaneo activo de owasp

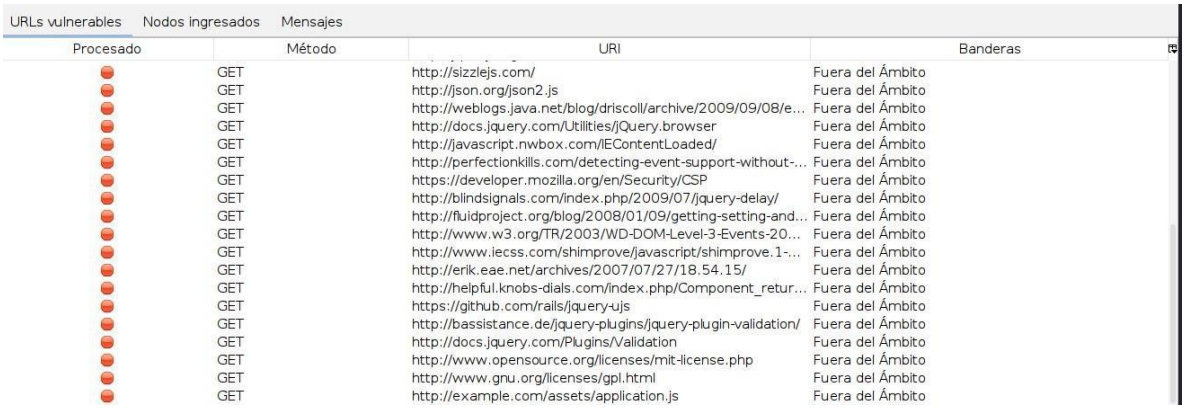


Id	Petición (Tie...	Marca de tiempo Re...	Mét...	URL	Có...	Razón	RTT	Tamaño de la Cabecera de R...	Respuesta (Tamaño del ...
287	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/test.php	404	Not Fo...	4milise...	189bytes	272bytes
288	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/_wpeprivate/...	404	Not Fo...	6milise...	189bytes	287bytes
289	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/_framework/...	404	Not Fo...	4milise...	189bytes	291bytes
290	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/.hg	404	Not Fo...	11milis...	189bytes	267bytes
291	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/.bzr	404	Not Fo...	13milis...	189bytes	268bytes
292	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/._darcs	404	Not Fo...	4milise...	189bytes	271bytes
293	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/BitKeeper	404	Not Fo...	9milise...	189bytes	273bytes
294	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	31milis...	224bytes	4.046bytes
295	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	31milis...	224bytes	4.046bytes
296	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	30milis...	224bytes	4.046bytes
297	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	35milis...	224bytes	4.046bytes
298	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	28milis...	224bytes	4.046bytes
299	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	29milis...	224bytes	4.046bytes
300	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	26milis...	224bytes	4.046bytes
301	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	31milis...	224bytes	4.046bytes
302	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	30milis...	224bytes	4.046bytes
303	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	34milis...	224bytes	4.046bytes
304	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	29milis...	224bytes	4.046bytes
305	2/10/23 13:...	2/10/23 13:24:23	GET	http://192.168.0.108/cgi-bin/badst...	200	OK	30milis...	224bytes	4.046bytes

Fuente: 5 carlos campi

Scaneo activo son todos los ataques que se están ejecutando en ese momento con la marca del tiempo los métodos que se usaron la url de destino que fue enviado ese ataque y los tamaños bits.

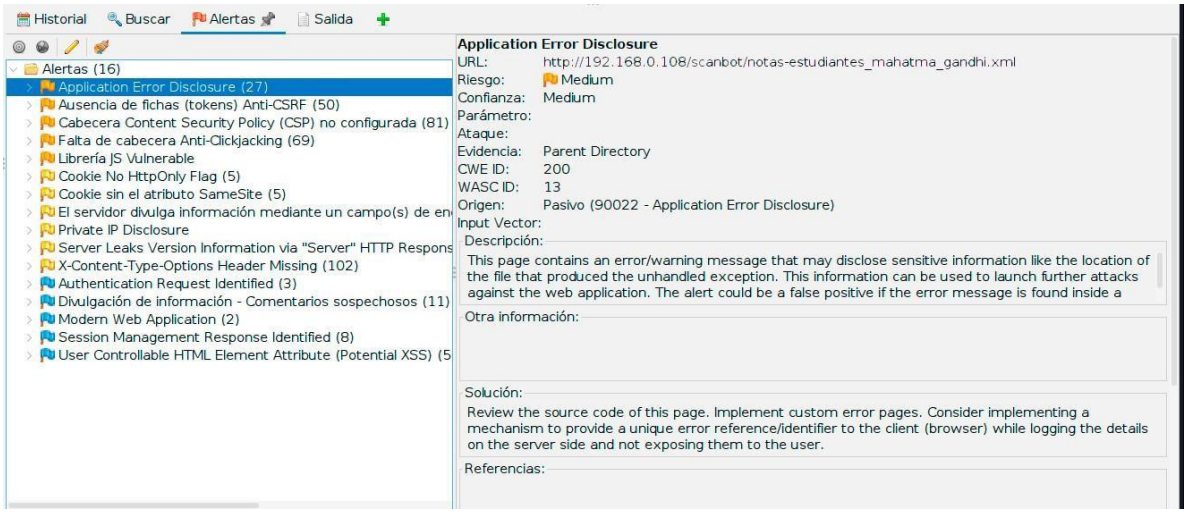
Fuente: 6 etiqueta roja indicando vulnerabilidad



Fuente: 6 carlos campi

Etiqueta roja es el procesado que indica que hay una vulnerabilidad por ejemplo la url es vulnerable que dicen procesados método url y las banderas el procesado si está en rojo significa que hay una url vulnerable en el método get porque aplication error hay otro método pos y la url en la cual ha ejecutado ese análisis.

Fuente: 7 alerta de vulnerabilidad



Fuente: 7 carlos campi

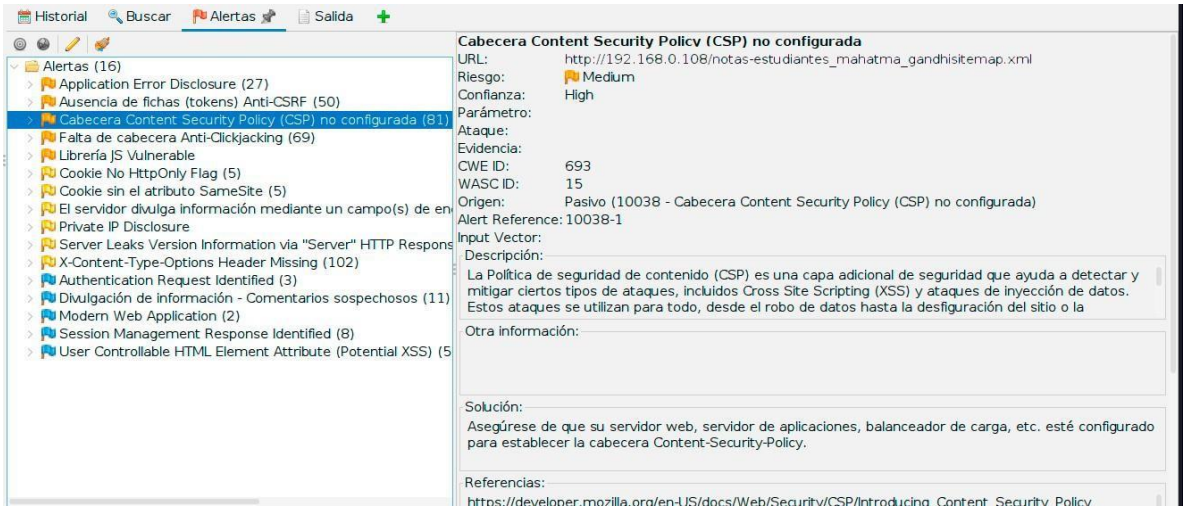
aplication error y ahí da una posible solución Esta página contiene un mensaje de error/advertencia que puede revelar información confidencial, como la ubicación del archivo que produjo la excepción no controlada. Porque esta información se puede utilizar para lanzar más ataques contra la aplicación web.

Fuente: 8 imagen 2

Fuente: 8 carlos campi

ausencia de fichas Token CSRF no válido o faltante este mensaje de error significa que tu navegador no pudo crear una cookie segura o no pudo acceder a esa cookie para autorizar tu inicio de sesión.

Fuente: 9 imagen 3



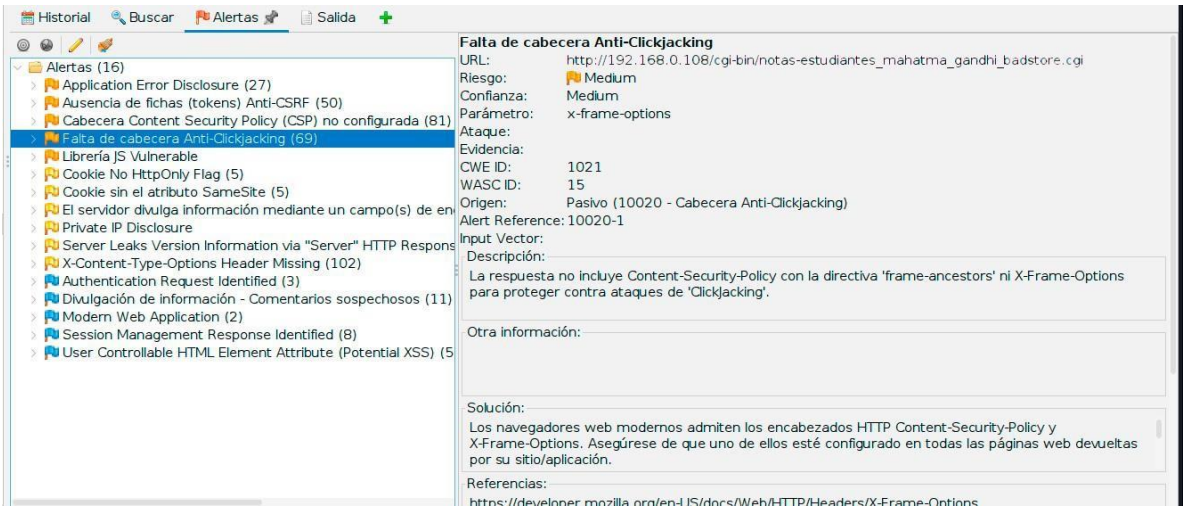
Fuente: 9 carlos campi

Es una capa de seguridad adicional que ayuda a prevenir y mitigar algunos tipos

de ataque, incluyendo Cross Site Scripting (XSS (en-US)) y ataques de inyección de datos.

Estos ataques son usados con diversos propósitos, desde robar información hasta desfiguración de sitios o distribución de malware.

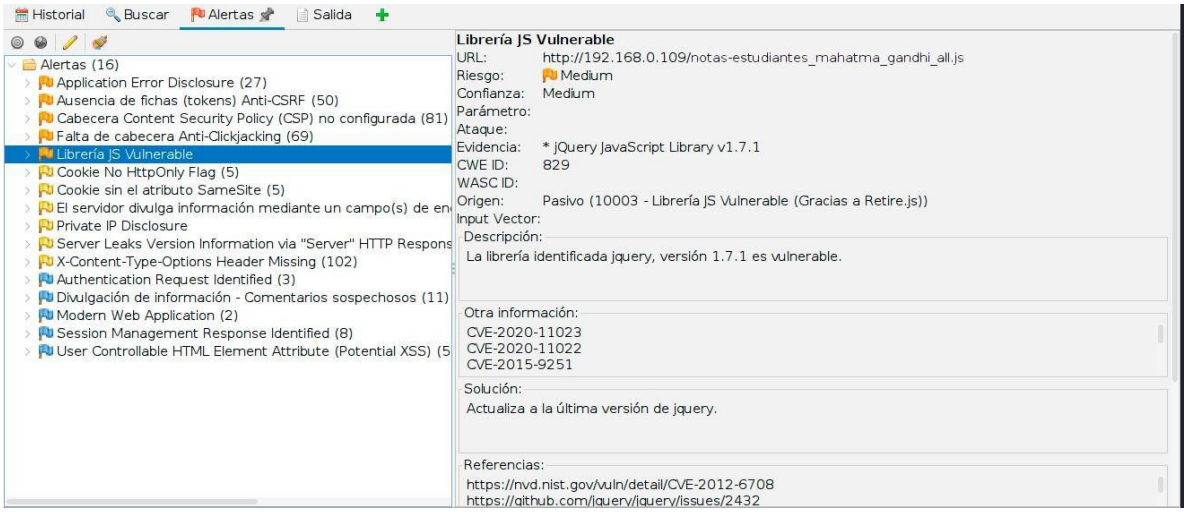
Fuente: 10 imagen 4



Fuente: 10 carlos campi

falta de cabecera anti-clickjacking Esta cabecera es utilizada para evitar que la web sea cargada en HTTP. El servidor indica al navegador que nuestra web solo se debe cargar en HTTPS y **el navegador bloqueará futuros accesos** si se intenta acceder al dominio mediante HTTP.

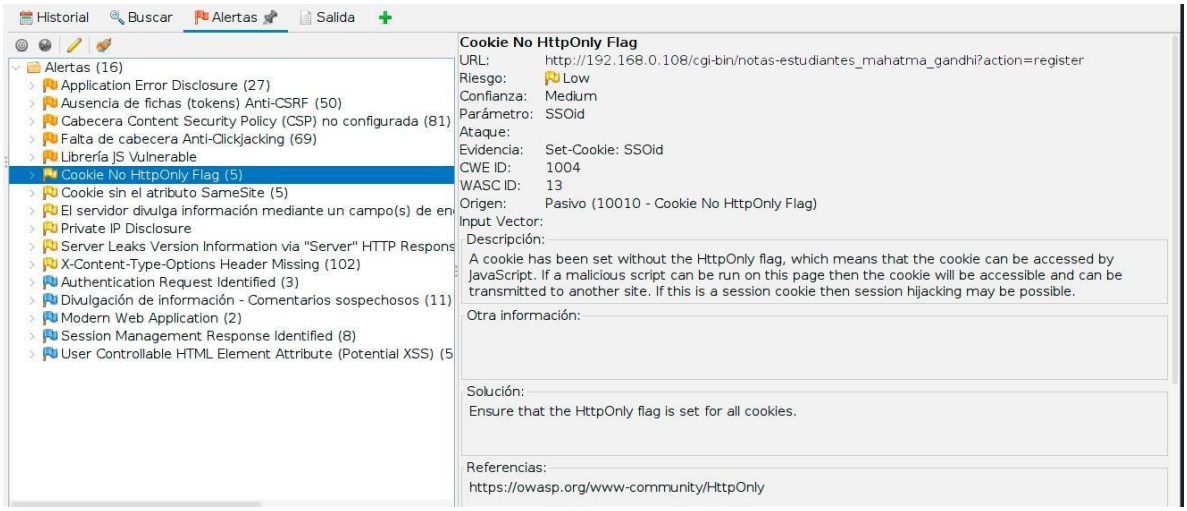
Fuente: 11 imagen 5



Fuente: 11 carlos campi

librería js vulnerable Esto simplifica enormemente las cosas, pero tenemos que mantenernos actualizados sobre las correcciones de seguridad. "El uso de componentes con vulnerabilidades conocidas" forma ahora parte del Top 10 de OWASP y las bibliotecas inseguras pueden suponer un gran riesgo para su webapp. El objetivo de Retire.js es ayudarle a detectar el uso de versiones con vulnerabilidades conocidas.

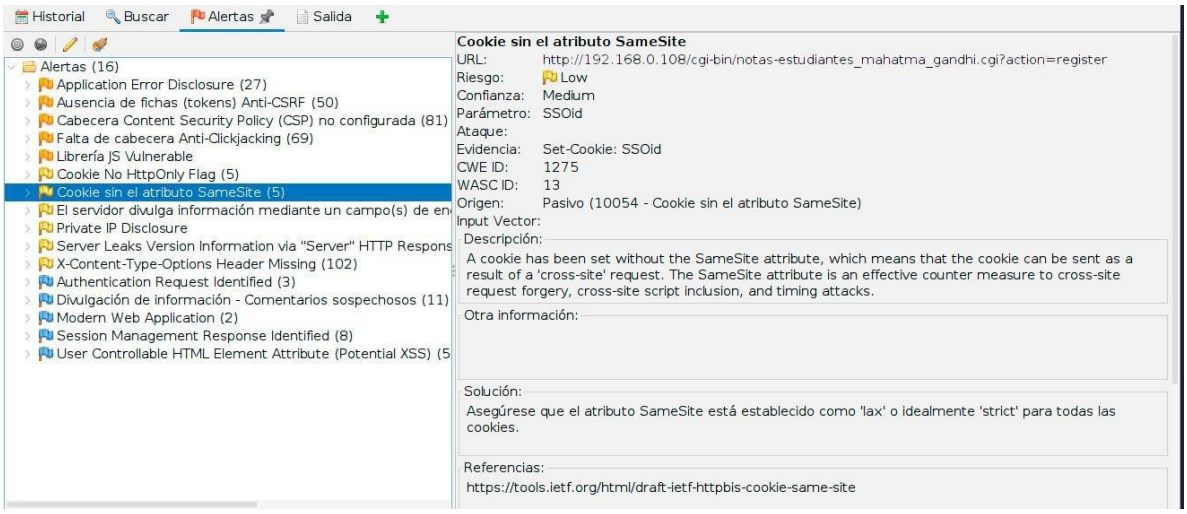
Fuente: 12 imagen 6



Fuente: 12 carlos campi

cookie no httponly flag Se ha configurado una cookie sin el indicador HttpOnly, lo que significa que se puede acceder a la cookie mediante JavaScript. Si se puede ejecutar un script malicioso en esta página, se podrá acceder a la cookie y podrá transmitirse a otro sitio. Si se trata de una cookie de sesión, es posible que se produzca un secuestro de sesión

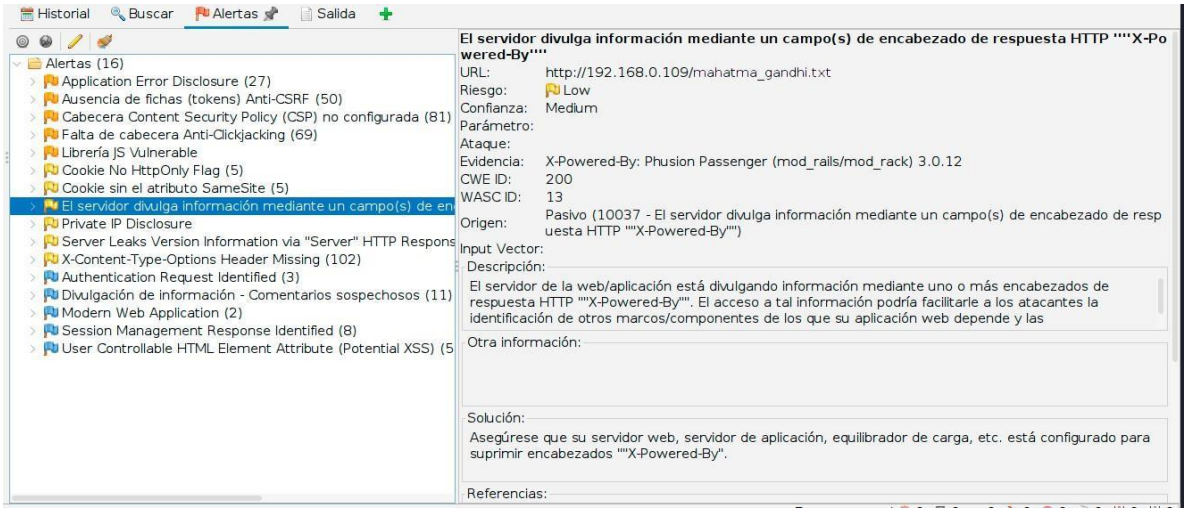
Fuente: 13 imagen 7



Fuente: 13 carlos campi

cookies sin el atributo samesite se debe incluir un atributo Secure adicional para que solo se pueda acceder a las cookies de varios sitios mediante conexiones HTTPS. Con esta medida no se mitigarán todos los riesgos asociados al acceso de varios sitios a las cookies, pero si se protegerán a los ataques de red

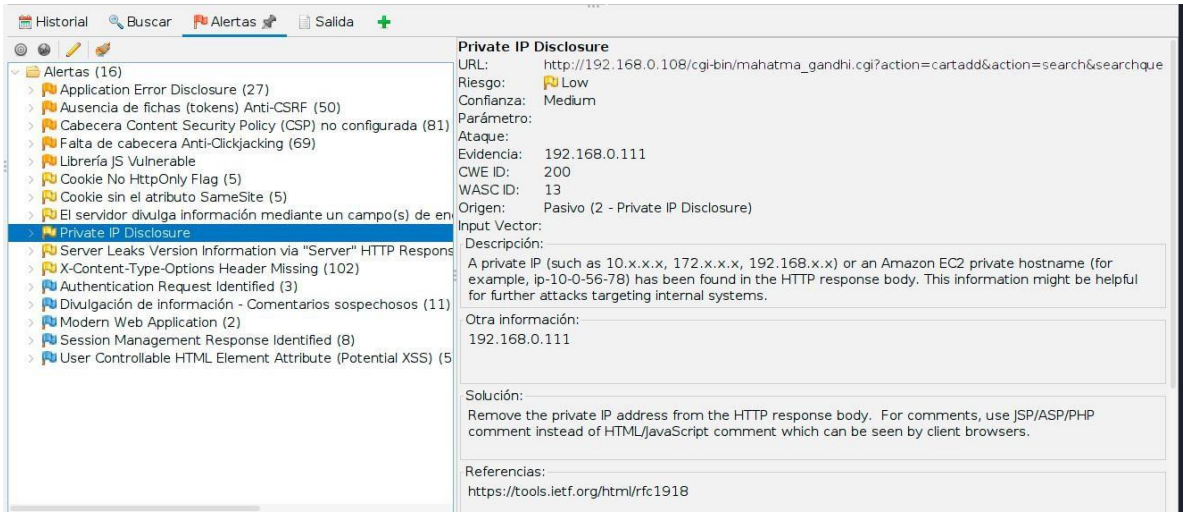
Fuente: 14 imagen 8



Fuente: 14 carlos campi

el servidor divulga información mediante un campo de encabezado de respuesta htt ““‘x-powered-by”” el servidor de la web está divulgando información mediante uno o más encabezados de respuestas de http el acceso a tal información podría facilitarte a los atacantes la identificación de otros marcos componentes de los que su aplicacion web depende

Fuente: 15 imagen 9

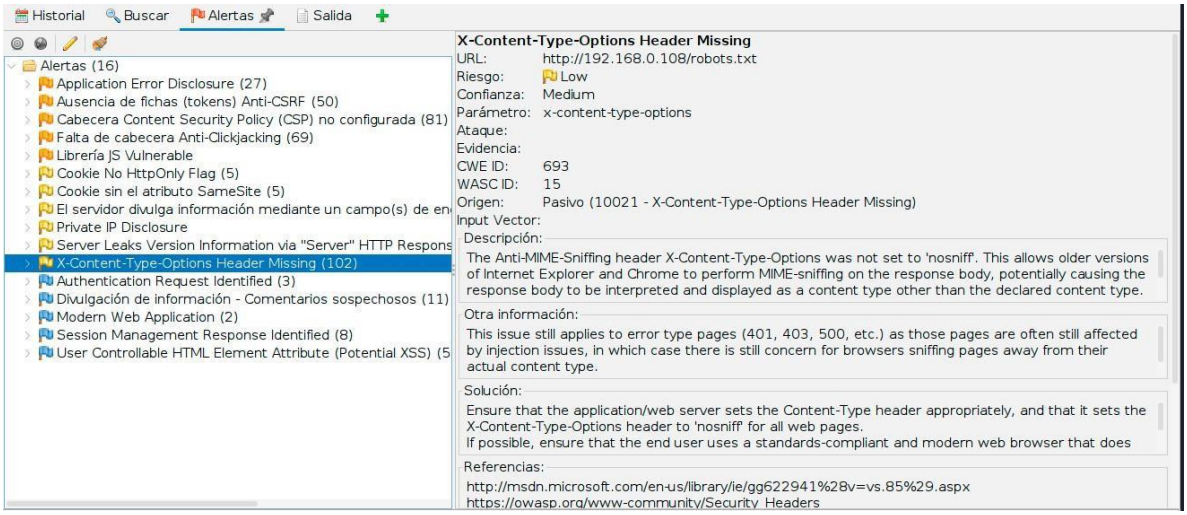


Fuente: 15 carlos campi

private ip disclousure

La divulgación de IP privada es una vulnerabilidad que un atacante puede aprovechar para obtener información sobre las direcciones IP internas de una aplicación web. Un atacante puede utilizar esta información para lanzar más ataques a la red interna.

Fuente: 16 imagen 10



Fuente: 16 carlos campi

x-content-type-options header missing La vulnerabilidad 'Falta el encabezado X- Content-Type-Options' es un problema de seguridad común en las aplicaciones web. Esta vulnerabilidad surge cuando un servidor web no configura el encabezado 'X-Content-Type-Options' en su respuesta, lo que permite a los atacantes realizar ataques de rastreo de tipo de contenido

9. DISCUSION DEL RESULTADO

Con los resultados obtenidos con los métodos y técnicas que se realizaron en este proyecto.

Se pudo observar que mediante la encuesta los docentes y directivo de la escuela

Consideran que es importante evaluar la seguridad de los sistemas de notas y en especial si es en línea y también se encontró un gran porcentaje que si esta de acuerdo con la medida efectiva para asi identificar y corregir posibles vulnerabilidades es por esa razón que existen preocupaciones éticas y legales que surge al utilizar las técnicas hacking ético que ha sido de mucha importancia para la protección datos que se usan hoy en día.

También en la tesis Según Por lo general, las empresas que más intentos de hackeo reciben, son las empresas del sector financiero, pues son las que manejan dinero. Los sistemas financieros son los más fortalecidos y robustos en temas de seguridad de la información, entonces los ataques tienden a irse hacia el otro lado del sistema que corresponde a los usuarios, quienes en muchas ocasiones terminan siendo el eslabón más débil de la cadena de la seguridad por su falta de conocimiento respecto al tema. Debido a las malas prácticas de seguridad por parte de la gente del común, su vulnerabilidad es tan grande que los hace presa fácil para el robo, otorgando así un buen botín para los hackers. Igualmente, se presentan muchos casos de espionaje industrial, en el que a través de las técnicas de hackeo se busca encontrar el punto débil de la competencia para sacar provecho de esa información. Por otro lado, son muy comunes los casos en los que organizaciones de hackers tratan de buscar que los equipos de hogares o empresas pequeñas sean manipulados como robots, creando legiones que en determinado momento son orientados hacia un mismo objetivo (SANCHEZ, 2019)

10. CONCLUSIONES

De acuerdo a la investigación se concluye que

•Se obtuvieron después de hacer el análisis de vulnerabilidades en el sistema de notas se presentan a continuación

• Las vulnerabilidades que se localizaron en el sistema de notas se pudieron realizar gracias al estudio, investigación y aplicación de conocimientos técnicos que averiguaron las fallas.

podemos rastrear la dirección IP de la organización objetivo.

• Las técnicas de hacking ético aplicadas en la etapa de explotación de vulnerabilidades resultaron ser eficientes al 100% por lo que se concluye que el sistema de notas del caso de estudio es totalmente vulnerable.

11. RECOMENDACIONES

• Se recomienda capacitar a todo al personal que se encuentra encargado de la seguridad informática en la institución educativa referente a técnicas de hacking ético con el objetivo de evaluar periódicamente el sistema de notas.

• Es recomendable llevar de manera periódica la guía para el análisis de vulnerabilidades en el sistema de notas presentado en este trabajo de titulación con el fin de dar una respuesta ejecutada ante posibles riesgos de seguridad.

• Es recomendable dar capacitaciones de seguridad informática a todas las entidades de las instituciones educativas con el plan de generar la responsabilidad compartida referente a el sistema de notas.

12. Referencias

blog owasp. (2019). Obtenido de blog owasp: https://www.incibe-cert.es/blog/owasppublica-el-top-10-2017-riesgos-seguridad-aplicaciones-web. [Accessed: 01- Nov2019].

carvaca, a. (2022). *repositorio.upse.edu.ec.* Obtenido de repositorio.upse.edu.ec: https://repositorio.upse.edu.ec/

communnity attacks. (1 de enero de 2020). Obtenido de communnity attacks: https://owasp.org/www-community/attacks/SQL_Injection. [Accessed: 08- Jan2020].

cortes, c. (2018). *tecnologica de antioquia.* Obtenido de tecnologica de antioquia: https://dspace.tdea.edu.co/bitstream/tda/330/4/ESTRATEGIAS%20DE%20ENSENANZA%20Y%20APRENDIZAJE%20EN%20ESTUDIANTES%20CON%20BAJO%20RENDIMIENTO.pdf

darias, s. (7 de febrero de 2023). *intelequia.* Obtenido de intelequia: https://intelequia.com/blog/post/hacking-%C3%A9tico-qu%C3%A9-es-y-cu%C3%A1l-es-su-utilidad-para-la-ciberseguridad

fernandez, f. (23 de febrero de 2018). *nexos.* Obtenido de nexos: https://www.uv.mx/personal/jomartinez/files/2011/08/LA_EVALUACION_EDUCATIVA.pdf

galarza, d. (2020). *A EVALUACIÓN DE VULNERABILIDADES.*

garcia, f. (8 de junio de 2022). *arsys.* Obtenido de arsys: https://www.arsys.es/blog/owasp

genes, g. (6 de mayo de 2021). *https://seguridadpy.info/.* Obtenido de https://seguridadpy.info/: https://seguridadpy.info/2021/05/owasp-zap-audita-la-seguridad-de-webs-y-evita-vulnerabilidades/

gonzales, c. (2020). *CHAVARRIA GONZALEZ, Víctor. Estudio de los ataques contra website. OWASP. 2020.* Obtenido de CHAVARRIA GONZALEZ, Víctor. Estudio de los ataques contra website. OWASP. 2020.

liedo, b. (2021). *EUNOMÍA. Revista en Cultura de la Legalidad.* Obtenido de EUNOMÍA. Revista en Cultura de la Legalidad: https://doi.org/10.20318/eunomia.2021.6074

Obregón, B. (16 de octubre de 2018). Obtenido de blog de tecnologia: https://blogs.imf-formacion.com/blog/tecnologia/hacking-etico-201810/

porter, m. (2021). *dspace.utpl.edu.ec.* Obtenido de dspace.utpl.edu.ec: https://dspace.utpl.edu.ec/bitstream/20.500.11962/28281/1/2.%2BQue%CC%81%2Bes%2Bestrategia.pdf

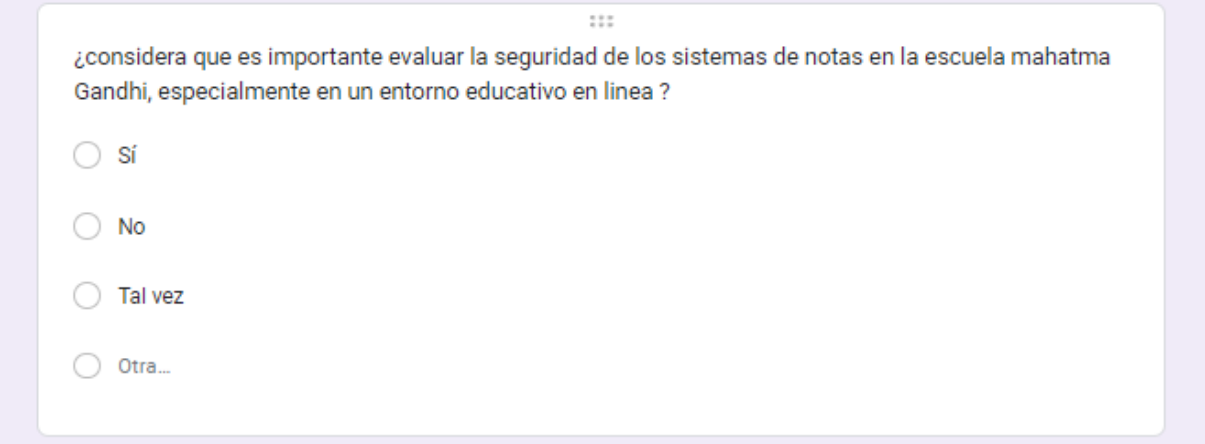
Ramos, M. (agosto de 2020). *UNIVIDA FUP VIRTUAL.* Obtenido de UNIVIDA FUP VIRTUAL: http://univida fup.edu.co/repositorio/files/original/53018ccfc14a066a678ef340fd6922f9.pdf

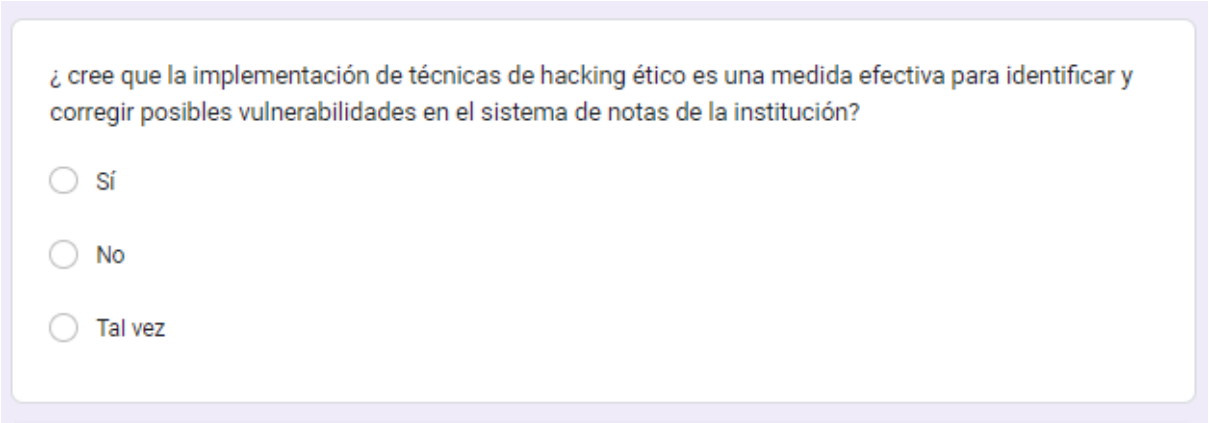
rodriguez, l. (7 de marzo de 2021). *UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA* . Obtenido de UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA : https://repositorio.upse.edu.ec/bitstream/46000/5977/1/UPSE-TTI-2021-0026.pdf

SANCHEZ, M. (2019). *UNIVERSIDAD DE PILOTO DE COLOMBIA.* Obtenido de UNIVERSIDAD DE PILOTO DE COLOMBIA: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4919/00005096.pdf?sequence=1

tejedor, j. (17 de agosto de 2023). *linked in*. Obtenido de linked in: https://es.linkedin.com/pulse/qu%C3%A9-es-el-hacking-%C3%A9tico-y-cu%C3%A1l-su-funci%C3%B3n-jose-tejedor

13. ANEXOS


¿considera que es importante evaluar la seguridad de los sistemas de notas en la escuela mahatma Gandhi, especialmente en un entorno educativo en linea ?
Sí
No
Tal vez
Otra...


¿ cree que la implementación de técnicas de hacking ético es una medida efectiva para identificar y corregir posibles vulnerabilidades en el sistema de notas de la institución?
Sí
No
Tal vez

¿ existen preocupaciones éticas y legales que surgen al utilizar técnicas de hacking ético para evaluar la seguridad de los sistemas de notas en una institución educativa?

- si
- no
- tal vez
- Otra...

¿piensa que los posibles beneficios de incorporar la evaluación de vulnerabilidades como parte de la estrategia de ciberseguridad en la escuela mahatma Gandhi superan los beneficio?

- si
- no
- tal vez
- Otra...

¿ Cree que los resultados de la evaluación de vulnerabilidades se utilizaran de manera efectiva para mejorar la seguridad del sistema de notas y proteger los datos de los estudiantes en la institución?

- ○ Sí
- ○ No
- ○ Tal vez