UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

Estudio de Seguridad informática en el Sistema Académico del Ministerio de Educación

Egresada:

Guisela Jaqueline Pérez Rueda

Tutor:

Ing. José Teodoro Mejía Viteri, MSC

Año 2017

INTRODUCCIÓN

La seguridad informática son técnicas desarrolladas para proteger los equipos informáticos y la información que se asimilan con la seguridad aplicada a otros medios, para tratar de reducir los riegos agrupados y la utilización de los sistemas que no son autorizado que por lo regular ocasionan problemas malintencionados. (Galdamez, 2003)

Es decir que la seguridad informática es la encargada de proteger la integridad y la información almacenada en los sistemas informáticos por cualquier tipo de ataque.

La seguridad informática intenta proteger el almacenamiento, y los procesamientos en la transmisión de información digital. (Buendia, 2013)

La seguridad informática protege los recursos valiosos que se encuentra dentro de una Empresa u Organización tales como: Información, Recurso de hardware y software. Esta adaptación de medida de prevención permite que la empresa cumpla con su objetivo de seguridad siendo este así un medio de apoyo. Esta medida de seguridad previene potencial perdida de información o a su vez niega el acceso a persona no autorizada. Al incorporar seguridad informática a las empresas minimizan los riesgos de pérdida de información y sus recursos asociados.

Un sistema de información es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargado de facilitar el funcionamiento global de una entidad pública o de otra actividad humana para conseguir sus objetivos.

Estos elementos son:

Recursos: pueden ser físicos y lógicos.

Equipo humano: compuesto por las personas que trabajan para la organización.

Información: conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.

Actividades: que se realizan en la organización, relacionadas o no con la informática. (Lopez, 2010)

Las amenazas que afectan a las características principales de la seguridad como la confidencialidad, integridad y disponibilidad de la información pueden ser internas o externas, originadas accidentalmente o con un fin malicioso dejando al sistema con problemas como la paralización de sus actividades cotidiana que deja como resultado una cuantiosa pérdida de tiempo y dinero a sus usuarios al momento de acceder a los servicios del sistema.

Por lo tanto, la seguridad informática debe ser dada por una colaboración entre los encargados de la seguridad de información, que deben de disponer de las medidas al alcance de las manos y los usuarios, que deben de ser conscientes de los riesgos que implican en los sistemas ya que pierden tiempo de producción y horas de recuperación de las actividades normales en muchos casos es irrecuperable.

Un sistema informático puede ser definido como un conjunto de procedimiento, dispositivo y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información e intentar reducir las amenazas que pueden afectar al mismo. Existe un gran número de razones para aplicar y afianzar la seguridad informática debido a que la actualidad los sistemas informáticos prácticamente no existe ordenadores aislado como

sucedía en ordenadores de generaciones anteriores. (Garcia, Seguridad Informatica, 2011, pág. 2)

Todos los servicios avanzados que utilizamos están implementados sobre sistema informáticos concreto, configurado adecuadamente y conectado mediante redes de comunicaciones. Cualquiera de estos elementos es susceptible de ser atacado por un hackers o simplemente fallar. La seguridad informática intenta evitarlo y en caso de q ocurra minimizar los daños para poder recuperar el servicio lo ante posible. (Buendia, 2013)

PLANTEAMIENTO DEL PROBLEMA

Ataques de vulnerabilidad hacia el sistema académico del Ministerio de Educación

¿Cómo mejorar la seguridad del sistema académico del Ministerio de Educación?

Atreves de la herramienta de Owasp-Zap de Kali Linux vamos a realizar un escaneo completo detectando las vulnerabilidades y posibles amenazas que contiene el sistema, ya q debido a debilidades q posee el sistema puede causar daño al hardware y software para esto la herramienta detecta las posibles fallas dando como resultado riesgos medio que se encuentra en el sistema, y a su posible solución que se debe emplear el sistema.

DESARROLLO

CLASIFICACIÓN DE SEGURIDAD

Cuando hablamos de la seguridad en un sistema informático, podemos encontrar diversos tipos de seguridad, dependiendo de la naturaleza material de los elementos que

utilicemos o de si se ocupan de evitar el ataque o incidente o de recuperar el sistema una vez que se haya producido. (Garcia, 2011, pág. 3)

Se pueden hacer diversas clasificaciones de la seguridad informática en función de distintos criterios.

Según el activo a proteger, es decir, todos los recursos del sistema de información necesarios para el correcto funcionamiento de la actividad de la empresa, distinguiremos entre seguridad física y lógica; en dependencia del momento preciso de actuación entre seguridad pasiva y activa, según se actué antes de producirse el percance, de tal manera que se eviten los daños en el sistema, o después del percance, minimizando los efectos ocasionados por el mismo. (Cesar Seoane Ruano, 2010)

SEGURIDAD FÍSICA Y LÓGICA

La seguridad física cubre todo lo referido a los equipos informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red. La seguridad lógica se refiere a las distintas aplicaciones que ejecutan en cada uno de estos equipos. (Buendia, 2013, pág. 14)

Las amenazas contra la seguridad física pueden ser provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales. Dentro de las provocadas por el ser humano, encontramos amenazas de tipo:

Accidentales, como borrado accidental, olvido de clave, etc.

Deliberadas como robo de la clave, borrado deliberado de la información, robo de datos confidenciales, etc.

Dentro de las provocadas por factores naturales, podemos encontrar: incendios, inundaciones, etc.

Amenazas

Desastres naturales (incendios, inundaciones, hundimientos, terremotos).

Robos proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, con todas estas medidas pretendemos evitar la entada del personal no autorizado.

Fallos de suministro: los suministros utilizan corriente eléctrica para funcionar y necesitan redes externas para la comunicación. (Gomez J. M., 2016)

> Las amenazas contra la seguridad lógica son muchas tales como los troyanos y malware: (software está diseñado para implementarse y causar daño.). Por lo general ocurre con el spam (correos electrónico malicioso), son aquellos correos electrónicos falso para filtrarse y causar molestias, por lo tanto, los malware son software no deseado y que debemos que eliminar.
>
> Perdida de datos: Un defecto de una aplicación, o una configuración defectuosa de la misma, puede ocasionar diferentes modificaciones en la información obtenida, incluso la pérdida de las mismas. Para reducir estos riesgos, las empresas deben probar una aplicación antes de implementarla y, sobre todo, realizar diferentes copias de seguridad. Ataques a la aplicación de los servidores: Los hackers intentan entrar aprovechándose de cualquier vulnerabilidad en los sistemas operativos o de las aplicaciones para robar la información. (Gomez J. M., 2016)

SEGURIDAD ACTIVA Y PASIVA

La seguridad pasiva es aquel mecanismo que, al instante de tolerar un ataque, nos permite recuperar razonablemente la información, minimizando así todos los riesgos posibles.

La seguridad activa protege de todos los ataques mediante medidas de adaptación para proteger todos los activos de una empresa, equipos informáticos, encriptación de datos, aplicaciones, datos y comunicación. (Gomez J. M., 2016)

La seguridad activa se la puede definir como conjunto de medidas que previenen los daños en los sistemas informáticos. (Cesar Seoane Ruano, 2010, pág. 16)

Las Amenazas contra la Seguridad Activa y la Seguridad Pasiva

Seguridad Activa	Seguridad Pasiva
• Uso de contraseñas: Prevenir el acceso y recursos por parte de personas no autorizadas	• Técnicas de seguridad pasiva: Podemos restaurar información que no es válida ni consistente
• Listas de control de acceso: Prevenir el acceso a los ficheros por parte de personal no autorizados	• Realización de copia de seguridad
• Encriptación: Evita que personas sin autorización puedan interpretar la información	• Utilizar herramienta de limpieza
• Uso de software de seguridad informática: Previene de virus informáticos y de entradas indeseadas al sistema informático	• Minimizar los efectos de riesgos
• Mantener el equipo limpio • Utilizar antivirus • Encriptar los datos	

Elaborado por: Guisela Pérez Rueda

Tabla 1. Amenazas de las seguridades activa y pasiva

CONFIDENCIALIDAD, DISPONIBILIDAD, INTEGRIDAD Y NO REPUDIO

La confidencialidad de la información, es la que garantiza la seguridad informática cuando el sistema es inherentemente inseguro que puedan leer, copiar, descubrir o modificar la información sin autorización.

Para así garantizar la confidencialidad requiere disponer de tres tipos de componentes:

Autenticación: Confirmar que un individuo o máquina, no debe hablar con un impostor.

Autorización: Verificar la autenticación, de los distintos usuarios de la información para obtener privilegios, a la lectura y a la innovación.

Cifrado: La información estará cifrada para que no sea útil a tercera persona que no tengan el permiso debido de los dueños de la empresa.

El objetivo de la integridad es que la información guardada y que no sean alterados por ningún motivo. Un ejemplo será el identificador de las cuentas bancarias, que posee cuatro grupos de dígitos:

- Dígitos del código de banco
- Digito del código de la sucursal del banco donde se abierto la cuenta

La disponibilidad requiere que los usuarios puedan acceder los servicios sin ningún inconveniente.

El no repudio se refiere a una relación entre dos partes, intentaremos evitar que cualquiera de ellas pueda negarse al participar con la relación. (Gomez J. M., 2016)

OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

El objetivo principal de la seguridad informática es proteger todos los sistemas informáticos, como la información, los equipos en sí, y los usuarios del sistema.

- **Información**: Dentro de cualquier sistema informático, ya sea para defender su integridad como su privacidad. Por integridad es evitar perdida, y por privacidad del que cualquier persona no autorizada pueda acceder a ella y hacer un mal uso de la misma.
- **Equipo físico**: Se hace referencia a la parte física del sistema para que no se estropee, ya sea por un ataque físico, o por causas accidentales.
- **Usuarios:** Dentro de su seguridad es una parte primordial asegurar, a los usuarios, como no autorizados, para lo que se utilizan perfiles de usuario, restricciones físicas de acceso a ciertos lugares. (hurtado, 2011)

TIPOS DE AMENAZAS

Dentro de las amenazas al sistema informático, podemos encontrar diferentes tipos de amenazas. Entre ellas podemos destacar:

Amenazas software: dentro de este tipo de amenazas podemos encontrar cualquier tipo de software malintencionado, como virus, espías, troyanos, gusanos, etc.

Amenazas físicas: se pueden encontrar todos aquellos posibles daños causados al sistema informático por razones físicas y naturales, como robos, catástrofe natural.

Amenazas humanas: además de las amenazas anteriores, las amenazas puramente humanas, pueden venir desde dos tipos de amenazas:

- Intrusos como piratas informáticos, que pueden entrar vía web, es decir de forma remota o físicamente al sistema.
- Fallos humanos de los propios usuarios del sistema informático. (hurtado, 2011)

TIPOS DE ATAQUES

Es un intento de filtración de una o más personas para así causar molestias a los sistemas informáticos o también a la red. Una vez que alguien está decidido a atacarnos, puede elegir alguna de estas formas:

Interrupción. - Consiste provocar un corte en la prestación de un servicio: ya sea en el servidor web para que no esté disponible y solo se pueda leer, etc.

Interceptación: El atacante accede por medio del canal de comunicación y copiar la información que se está transmitiendo.

Modificación: Ha conseguido acceder a la información, para modificarla y alterándola los datos y así provocar algunos problemas a los distintos de los usuarios.

Fabricación: es aquel que engaña haciéndose pasar por el receptor, para obtener la información valiosa para lograr su objetivo malicioso. (Gomez J. M., 2016)

Para conseguir su objetivo se puede aplicar una de estas técnicas:

Ingeniería social: Se basa en la interacción humana haciéndose pasar por familiares o amigos con el fin de violar los procedimientos de seguridad y así poder obtener información necesaria para hacer daño a los demás.

Phishing: Consiste en ponerse en contacto con la victima por medio de los correos electrónicos haciéndose pasar por una empresa. En la cual es una web muy parecida a la original, así convenciendo a los usuarios a llenar formularios con la información necesaria. (Gomez J. M., 2016)

Keyloggers: Es un software o troyano que puede tomar nota de todas las teclas que pulsamos, buscando el momento en que introducimos el usuario y contraseña.

Los ataques de fuerza bruta hay varias medidas de contrarrestar:

- Siempre utilizar passwords con combinaciones de letras mayúsculas, minúsculas, números combinados y signos de puntuación.
- Cambiar la contraseña con frecuencia.
- Establecer un máximo de fallos y después bloquear todos los accesos.

Sniffing: consiste en enlazarse en el mismo tramo de la red y el equipo y de este modo tener acceso a toda la información o conversación que está siendo transmitida.

DoS: Radica en derribar un servidor saturándolo con falsas peticiones de conexión. Sobrecargando al servidor de trabajo varias veces superior a la normal.

TIPOS DE ATACANTES

Se suele hablar de hacker de manera genérica para referirse a un individuo que se salta las protecciones de un sistema. A partir de ahí podemos distinguir entre:

Hacker: son personas que se dedican al hurto de información con el fin de perjudicar a las personas.

Cracker: También es un atacante que puede desactivar los servicios y poder extraer la información necesaria para sus objetivos. (Buendia, 2013, pág. 20)

ANÁLISIS DE VULNERABILIDAD

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas.

Vulnerabilidades ya conocidas sobre una aplicación o sistemas instalados, son vulnerabilidades de las que ya tienen conocimientos las empresas que desarrollan el programa al que afecta y para las cuales ya existe una solución, que se ubica en forma de parche. (Cesar Seoane Ruano A. B., 2010, pág. 20)

LISTAS DE HERRAMIENTAS DE ESCANEO EN LAS PÁGINAS WEB

Grabber: Es un escáner de aplicaciones web, que puede detectar muchas vulnerabilidades de seguridad. Realiza exploraciones y nos muestra donde está el error.

Cross site scripting

Inyección SQL

Pruebas de Ajax

La inclusión de archivos

JS analizador de código fuente

Comprobación del archivo de copia de seguridad

No es rápido en comparación con otros escáneres, pero es simple y portátil. Esto se debe utilizar sólo para probar pequeñas aplicaciones web, ya que toma demasiado tiempo para escanear grandes aplicaciones. (El_Andaluz, 2016)

Vega: Es otro escáner de vulnerabilidades web de código y de código abierto. Con esta herramienta, puede realizar pruebas de seguridad de una aplicación web. Esta herramienta está desarrollada en Java y ofrece un entorno basado en GUI. Está disponible para OS X, Linux y Windows.

Se puede utilizar para encontrar inyección SQL, inyección de cabecera, listado de directorios, inyección cáscara, Cross site scripting, la inclusión de archivos y otras vulnerabilidades de las aplicaciones web. Esta herramienta también se puede ampliar mediante una potente API desarrollada en JavaScript.

Ataque Zed Proxy: También se conoce como ZAP. Esta herramienta es de código abierto y es desarrollado por AWASP. Está disponible para las plataformas de Windows, Unix / Linux y Macintosh. Se puede utilizar para encontrar una amplia gama de vulnerabilidades en aplicaciones web. (El_Andaluz, 2016)

WebScarab: Es un software de seguridad basado en Java para el análisis de aplicaciones web usando HTTP o HTTPS. Con plugins disponibles, se puede ampliar la funcionalidad de la herramienta. Esta herramienta funciona como un proxy de interceptación. Así, puede revisar la solicitud y la respuesta que viene a su navegador y va a thw servidor. También puede modificar la solicitud o la respuesta antes de que sean recibidos por el servidor o el navegador.

Skipfish: Es también una herramienta de seguridad de aplicaciones web agradable. Se arrastra el sitio web y compruebe cada página para diversas amenazas a la seguridad y al final se prepara el informe final. Esta herramienta fue escrita en C#. Es altamente optimizado para el manejo de HTTP y la utilización de CPU mínimo. Se afirma que puede manejar fácilmente 2.000 solicitudes por segundo sin agregar una carga en la CPU. (Gomez, 2015)

Owasp-Zap: Es uno de los productos de OWASP (Open Web Application Security Project), sus siglas ZAP corresponden a Zad Attack Proxy. Zap es una herramienta para pruebas de penetración, de fácil uso y con múltiples componentes, para encontrar vulnerabilidades en aplicación web. (Gonzales, 2013)

Para el escaneo de vulnerabilidad de la página del CAS (Centros Autorizados de Servicio del Ministerio de Educación) vamos a realizarlo con la herramienta Owasp-Zap de Kali Linux

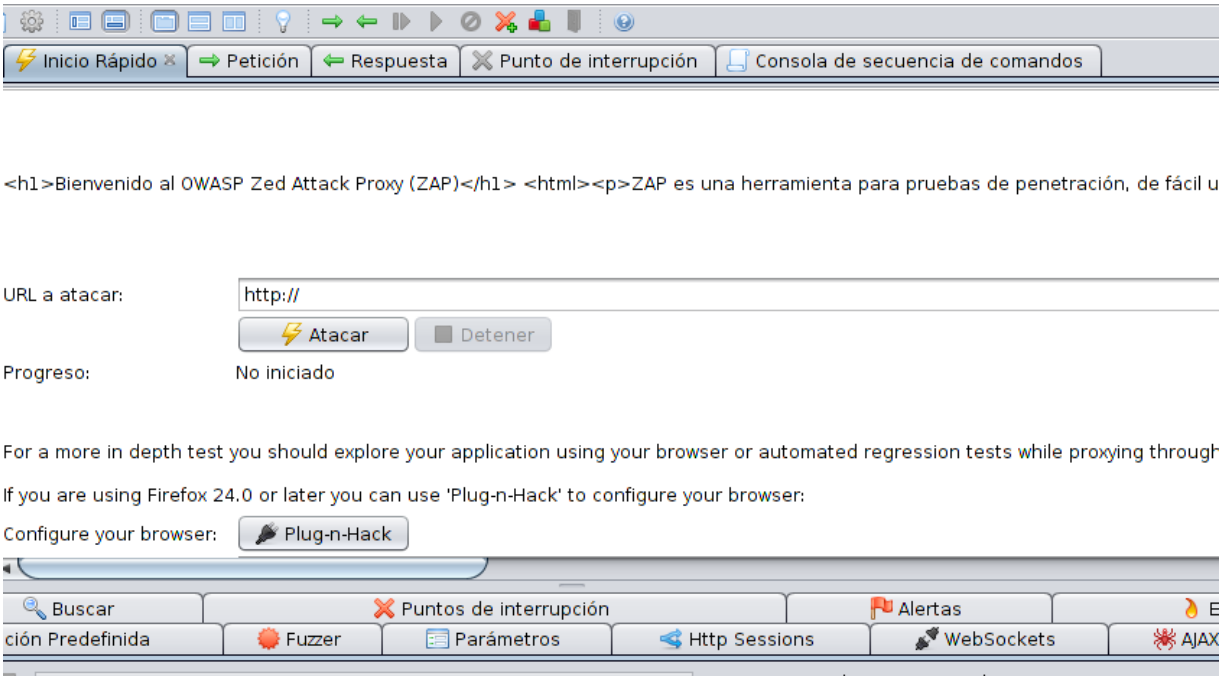
Ingresamos a la página del ministerio de educación

Elaborado por: Guisela Pérez Rueda
Figura 1. Página principal del ministerio

Para el escaneo de la vulnerabilidad con la herramienta de Kali Linux introduciremos la URL de la página del Ministerio de Educación y empezar atacar.

(http://servicios.educacion.gob.ec/cas-educacion/login?service=http%3A%2F%2Fservicios.educacion.gob.ec%3A80%2Fasignacion-cupos-web%2Fj_spring_cas_security_check%3Bjsessionid%3D5ncxr693Y4mw%2BIYCmlw7Rqrx.ce71cf2d-eab7-3262-8397-bea5da6ee86b)

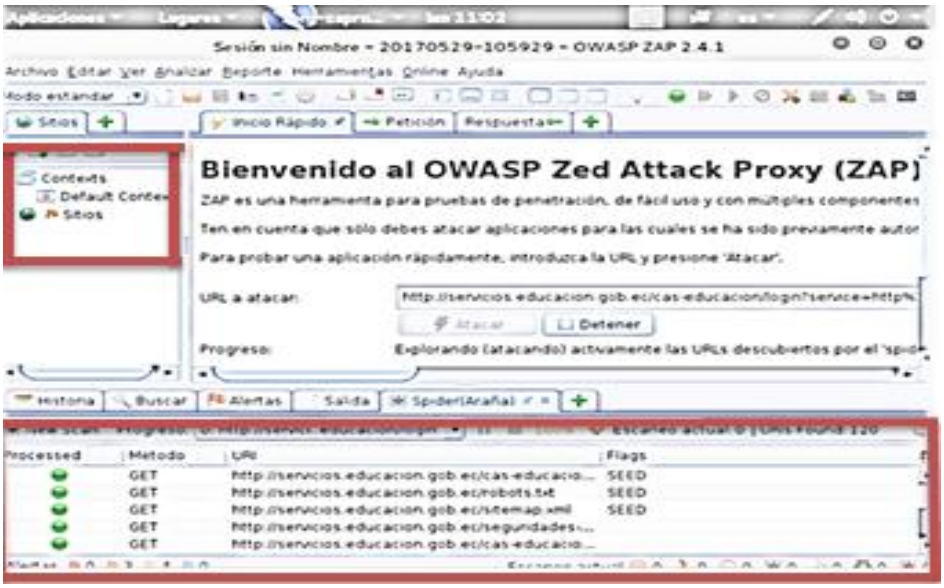
Posiblemente su facilidad de uso sea el que le ha convertido en uno de los buscadores de vulnerabilidades en aplicaciones web.



***Elaborado por*:** Guisela Pérez Rueda

***Figura 2*.** Página principal de Owasp Zap

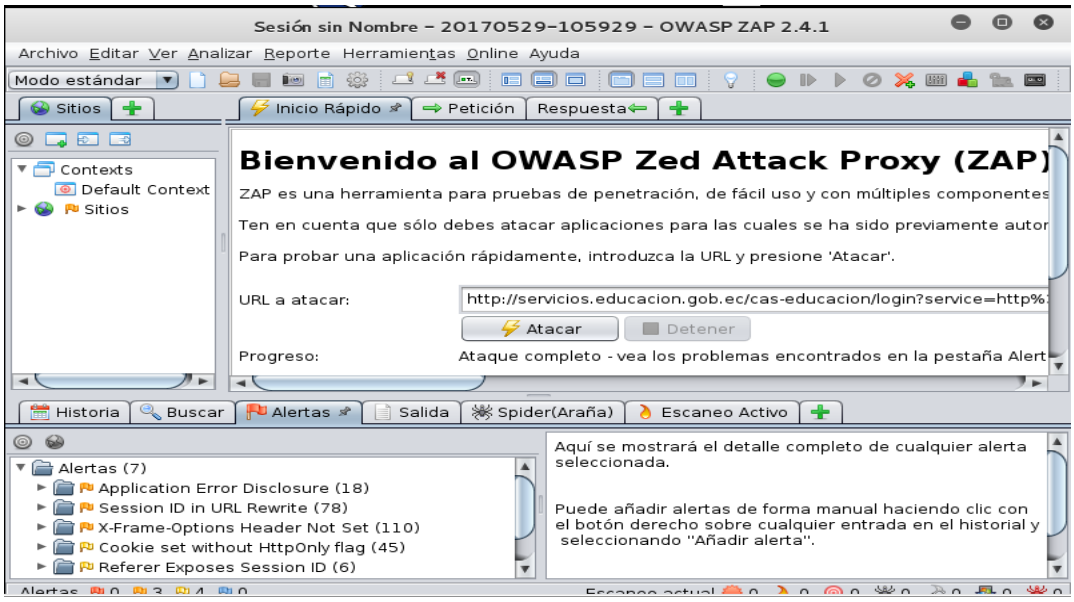
A partir de ese momento OWASP ZAP empezara a buscar vulnerabilidades indiscriminadamente. Lo primero que hará será reconocer todas las URL del sitio a través del Spider (programa que recorre la www y recorre páginas web, visitando los enlaces que tienen de forma automática). De esta forma podremos tener un mapa de la web.



Elaborado por: Guisela Pérez Rueda

Figura 3. Recorrido de la URL a través del Spider

Cuando se hace este recorrido por todas las URLs a través del Spider, se van a analizando cada una de ellas las URL encontradas en busca de información sensible, se mostrará una alerta indicando su grado de riesgo, es decir, si la vulnerabilidad es grabe, media o casi sin importancia.



Elaborado por: Guisela Pérez Rueda

Figura 4. Escaneo de vulnerabilidades

Este escáner permitirá si existe una vulnerabilidad o no, pero nunca atacará directamente sobre el servidor. El escáner, de la misma manera que el spider, ira recorriendo todas las URL e ira probando “ataques” sin llegar a ejecutarlos.

Al finalizar este proceso, habrá terminado la búsqueda automática de vulnerabilidades.

En este panel donde se muestra las posibles vulnerabilidades y el riesgo que conlleva, muestra además, información sobre cómo se puede vulnerar, y qué medidas se pueden tomar para evitar que dicho fallo de seguridad sea vulnerable.

Elaborado por: Guisela Pérez Rueda

Figura 5. Alerta de vulnerabilidades

Una vez escaneado del lado izquierdo de la pantalla nos aparece unas notificaciones en forma de banderilla en color amarillo indicando que es riesgo medio.

Elaborado por: Guisela Pérez Rueda
Figura 6. Notificaciones de riesgos medio

Al dar clic en una de las banderillas se despliega un sub menú indicando la descripción del riesgo y la posible solución

CONCLUSIONES

- En este trabajo se ha estudiado los ataques más comunes que afectan a los sistemas web. Así como también dando a conocer sobre los diversos riesgos que puede tener un sitio en este caso el **Sistema Académico del Ministerio de Educación,** debido a la constante amenazas en que se encuentre, es necesario enfocarse en las herramientas de seguridad, en los tipos de amenazas que puedan realizar posibles ataques informáticos.

  Dando como objetivo principal las protecciones de todos los recursos tanto hardware como software brindando una seguridad estable para el sistema.

- La evaluación del escaneo del sistema realizada con la herramienta Owasp Zap trata de buscar las vulnerabilidades que se encuentra en el sitio analizando cada una de las URL, implicando una búsqueda de configuraciones hasta un simple parámetro de algunos archivos que compone la web, mostrando la alerta sobre la vulnerabilidad que tiene el sistema.

- Mostrando los errores en notificaciones (banderillas) podemos dar una solución efectiva al sistema permitiendo reducir el grado de vulnerabilidad, ofreciendo un sistema más seguro para la empresa.

Bibliografía

(2013). Obtenido de Analisis de vulnerabilidad: http://www.etic-solutions.net/etic/servicios/analisis-de-vulnerabilidad

Andrade, S. R. (13 de 11 de 2013). *Sistemas Operativos*. Obtenido de https://prezi.com/a9wzy2rlyrg7/sistemas-operativos/

Buendia, J. F. (2013). Seguridad Informatica. En G. B. Jose Roa Buendia, *Seguridad Informatica Mc-Graw-Hill* (pág. 8). España: Ariadna Alles, Paloma Sanchez, Maria Dolores Espin.

Castillo, J. (13 de 09 de 2016). *Estudio Cientifico*. Obtenido de https://prezi.com/ens3rgolz9ah/colegio-de-estudios-cientificos-y-tecnologicos-del-estado-de/

Cesar Seoane Ruano, A. B. (2010). Seguridad Informatica. En A. B. Cesar Seoane Ruano, *Seguridad Informatica McGraw-Hill* (pág. 13). España: Ariadna Alles, Paloma Sanchez, Maria Justicia Waldo.

Cesar Seoane Ruano, A. B. (2010). *Seguridad Informatica.* España: Ariadna Alles, Paloma Sanchez, Maria Justicia Waldo.

El_Andaluz. (1 de 09 de 2016). *Tipos de Escaneadores de vulnerabilidad*. Obtenido de https://foro.elhacker.net/seguridad/tipos_de_escaneadores_de_vulnerabilidad-t457012.0.html

Galdamez, P. (2003). *Seguridad Informatica.*

Garcia, A. (2011). *Seguridad Informatica.*

Garcia, A. (2011). *Seguridad Informatica.* Filipinas: Copyright 1 edicion.

Gomez, J. M. (30 de 09 de 2016). *Conceptos de Seguridad*. Obtenido de http://blogconceptosdeseguridad.blogspot.com/2016/09/conceptos-de-seguridad.html

Gomez, V. (10 de Abril de 2015). *Internet Seguridad Software*. Obtenido de Los mejores 8 scanners de vulnerabilidades web: https://desarrollo-geek.net/sistemas-operativos/linux/soft-linux/los-mejores-8-scanners-de-vulnerabilidades-web/

Gonzales, I. (26 de Diciembre de 2013). *Kontrolo The underway security*. Obtenido de Owasp Zap: http://www.kontrol0.com/2013/12/owasp-zap-asi-funciona-su-busqueda.html

hurtado, a. g.-c. (2011). *seguridad informatica.* españa: carmen lara.

Lopez, A. (2010). Introduccion a los Sistemas Informaticos. En A. Lopez, *Seguridad Informatica* (pág. 9). Editex S.A.

Los Sistemas Informaticos. (2014). Obtenido de Los Sistemas Informaticos: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&sqi=2&ved=0ahUKEwiCjZj5oJDUAhVPfiYKHfD6CgMQFgg6MAQ&url=https%3A%2F%2Fticsjujuy.files.wordpress.com%2F2014%2F03%2Fsistemas-de-informacion.pdf&usg=AFQjCNGkOCX2QURh4qRppRQ72rTX_KJ-JA&cad=rja

ANEXOS

Descripción de las notificaciones del riesgo medio y la posible solución del escaneo de la página del Ministerio de Educación

APPLICATION ERROR DISCLOSURE	
DESCRIPCIÓN	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. Esta información se puede utilizar para lanzar nuevos ataques contra la aplicación web. La alerta puede ser un falso positivo si el mensaje de error se encuentra dentro de una página de documentación.	Revise el código fuente de esta página. Implementar páginas de error personalizadas. Consiste implementar un mecanismo para proporcionar un identificador/referencia de error único al cliente (navegador) mientras registra los detalles en el lado del servicio y no los expone al usuario.
SESSION ID IN URL DISCLOSURE	
DESCRIPCIÓN	SOLUCIÓN
La reescritura de URL se utiliza para rastrear el ID de sesión del usuario. El identificador de sesión se puede divulgar a través de encabezados de referenciado de sitios cruzados. Además, el identificador de sesión puede almacenarse en el historial del explorador o en los registros del servidor.	Para contenido seguro, ponga ID de sesión en una cookie. Para ser aún más seguro, utilice una combinación de cookies y reescritura de URL.
X-FRAME-OPTIONS HEADER NOT SET	
DESCRIPCIÓN	SOLUCIÓN
El encabezado X-Frame-Options no está incluido en la respuesta HTTP para proteger contra ataques ´ClickJacking´.	La mayoría de los navegadores web modernos admiten los encabezados HTTP Opciones de X-Frame. Asegúrese de que

	está configurado en todas las páginas web devueltas por su sitio (si espera que la página se enmarque solo por las páginas de sus servidor (por ejemplo, es parte de un FRAMESET), entonces usted querrá utilizar SAMEORIGIN, de lo contrario si nunca esperas que la página ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web soportados).
COOKIE SET WITHOUT HTTPONLY FLAG	
DESCRIPCIÓN	SOLUCIÓN
Se ha establecido 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, la cookie estará accesible y se puede transmitir a otro sitio. Si se trata de una cookie de sesión, entonces el secuestro de sesión puede ser posible.	Asegúrese de que el indicador HttpOnly está establecido para todas las cookies.
REFERER EXPOSES SESIÓN ID	
DESCRIPCIÓN	SOLUCIÓN
Se encontró un hipervínculo que apunta al nombre de host anther. A medida que se utiliza la reescritura de la URL de la ID de sesión, se puede divulgar en el encabezado referencia a los hosts externos.	Esto es un riesgo si el identificador de sesión es sensible y el hipervínculo se refieren a un host externo o de terceros. Para contenido seguro, ponga ID de sesión en una cookie de sesión segura.
WEB BROWSER XSS PROTECTION NOT ENABLED	
DESCRIPCIÓN	SOLUCIÓN
La protección XSS del explorador web no está habilitada o esta deshabilitada por la	Asegúrese de que el filtro XSS del navegador web está habilitado,

configuración del encabezado de respuesta HTTP´X-XSS-Protection´ en el servidor web	estableciendo el encabezado de respuesta HTTP X-XSS-Protection en ´1´.
X-CONTENT-TYPE-OPTIONS HEADER MISSING	
DESCRIPCIÓN	SOLUCIÓN
El encabezado Anti-MINME-Sniffing X-Content-Type-Options no se estableció en 'nosniff'. Esto permite que versiones anteriores de Internet Explorer y Chrome realicen MIME--Sniffing en el cuerpo de la respuesta, haciendo que el cuerpo de la respuesta sea interpretado y mostrado como un tipo de contenido distinto al tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas a Firefox utilizaran el tipo de contenido declarado (si se ha establecido), en lugar de realizar el Sniffing MIME.	Asegúrese de que el servidor de aplicaciones/web establezca la cabecera Content-Type apropiadamente y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese de que usuario final utilice un navegador web compatible con los estándares y moderno que no realice MIME-Sniffing en absoluto o que pueda ser dirigido por la aplicación web/ servidor web para que no realice MIME-Sniffing.

Tabla 2. *Descripciones y soluciones de cada notificación del riesgo medio*