# Evaluación de herramientas de detección de vulnerabilidades XSS

***Resumen*—En todo sitio web se debe realizar un estudio o análisis de su operación que permita tener información para establecer un plan de mitigación de riesgos, ya que si un cliente se ve afectado a nivel de entrega de datos u operación del sitio puede provocar el daño de su imagen y credibilidad. Se realizó los pasos o las tareas que recomiendan las metodologías permitiendo tener un marco referencial y la secuencia lógica o guía para conseguir información de vulnerabilidades en ataques de tipo XSS[1]. Para la revisión del sitio se definió un cronograma de trabajo a la gerencia de TIC´S de una organización dedicada a dar servicios de salud, se les informó sobre el alcance del trabajo y las herramientas a utilizar. Para un reconocimiento inicial se organizaron entrevistas con el personal encargado de manejar el sitio, se preguntó sobre la manera en que se encuentra estructurada la infraestructura de red lo que permitió entender y definir como se realizaría el análisis. Posterior a esta etapa de reconocimiento se buscó las herramientas que permita realizar un escaneo[2] del sitio como lo hace OSINT[3], seleccionando a "Maltego" que permitió transformar las direcciones de dominio e ir explotando las características e información de contactos de las personas encargadas del sitio. Para realizar el análisis de vulnerabilidades desde un sitio alterno se necesitó de las herramientas y servicios de conexión de internet, un access point, Kali Linux 2.0 instalado sobre Virtual Box. En la etapa de acceso las herramienta que se emplerarón fueron Dirbuster, Zarproxy, Paros, ProxiStrike, Uniscan, Vega y W3af las que presentaron resultados en diversos formatos que permitieron emitir el informe a la gerencia de TIC´S de la institución de salud.**

## I. INTRODUCCION

En la actualidad con la expansión de las aplicaciones sobre el Internet ha hecho que las organizaciones tiendan a mantener un contacto directo con sus clientes mediante este medio ya sea por el gran espectro de clientes que puede manejar así como la aparición de dispositivos en los que se puede incorporar esta tecnología y por su costo. En la actualidad se puede definir algunos tipos de ataques en la web según estadísticas[4] que permiten tener en cuenta como los sitios web son el blanco de ataques perpetrados para obtener información o afectar su disponibilidad, lo que conlleva al daño de la imagen de muchas corporaciones puesto que sus usuarios pueden dejar de confiar en la utilización de estos medios. Los pricipales ataques que Imperva[4]que se dan son principalmente ataques de inclusión local de archivos(LFI) que se dan cuando una los links de las URL reciben como parámetros alguna página que se encuentre alojada en el servidor y puede ser llamada por elementos de la misma página como JavaScript, inclusión remota de archivos(RFI) que permite realizar un ataque similar que se aprobecha de la inclusión dinámica de archivos desde sitios remotos, ataques de SQL injection que pueden vulnerar o inclusive dañar una base de datos mediante el envio de instrucciones que se añaden a los SQL de las páginas permitiendo tener acceso o corromper bases de datos, Ataques de tipo Directory Traversal que permiten ejecutar comandos de sistema operativo fuera de el directorio que contiene sus páginas, Ataques web XSS que permiten a aplicaciones perpetrar ataques aprobechándose de vulnerabilidades de los parámetros que se tranfieren del usuario al sitio, Ataques de extracción de direcciones de correo que permite obtener información de correo electrónico de las personas, Ataques del tipo de spamming a través de comentarios que se infiltran de manera similar a un spam y finalmente Ataques de violación del protocolo HTTP que consiste en el envio de petiociones http mal formados.

[1]Cross Site Scripting

[2]Definir las direcciones IP que conforman el sitio

[3]Open Source intelligence, OSINT que es la información pública de recursos que esta disponible en Internet.

Se revisó que para que un ataque sea efectivo se deben efectuarlos en periodos largos de tiempo(más de 40 días) lo que permitiría obtener la mayor cantidad de vulnerabilidades, ajustando las herramientas de ataque para poder encontrar vulnerabilidades y poder lograr el cometido del ataque, en el caso de un análisis de vulnerabilidades se pueden clasificar en ataques http y los de tipo injection que para una revisón leve y de reconocimiento se lo puede realizar en periodos de 15 minutos. En el caso de un análisis de vulnerabilidades se utilizaron algunas herramientas que verificaron las vulnerabilidades con la intención de determinar cual de ellas es la que reporta reportes completos de ataques de tipo XSS y en el ataque perpetrado para determinar vulnerabilidades de un sitio real se lo puede considerar como Gray Hat attack ya que se mantuno conocimiento de la información básica de la infraestructura, permitiendo de algún modo avanzar con el mismo sin tener que conocer la infraestructura global. En este caso se necesita determinar cuales son los principales mecanismos de mitigar un ataque XSS que se pudieran generar en cualquier sitio y determinar si la utilización de un WAF[4] mediante herramientas open source disminuyen el riesgo en este tipo de ataques y que tipo de aplicaciones tienen mayor vulnerabilidad, en este caso se va a atacar a un portal de servicios que tiene a GlassFish como servidor de aplicaciones y al sitio web de la misma organización que tiene a Apache como servidor web y mediante herramientas de como Vega y OWASP ver cual presenta mejores niveles de reporte en ataques XSS. Finalmente se quiere verificar como afecta en la red estos tipos de ataque con herramientas como sar y kSar.

## II. MARCO TEÓRICO

## III. CONFIGURACIÓN DEL EXPERIMENTO

Después de las autorizaciones que la entidad de salud proporcionó para que se pueda revisar su sitio web se inició con la configuración del experimento, tras coordinaciones previas al ensamblado del sitio desde donde se realizó el análisis, se definió las herramientas de software, así como el equipamiento informático y de comunicaciones, entre estos se estableció la utilización de tres computadoras portátiles, un punto de acceso y un canal con salida a Internet. El sistema operativo que se utilizó en las máquinas anfitrionas[5] fie Windows 8 en los tres casos. En el caso de la definición de las características base de las máquinas virtuales a instalar se definió a Kali Linux 2.0 como sistema operativo huesped[6] y se fijaron algunos parámetros para que se pueda cumplir con carácterística mínimas necesarias para que arranque la máuina virtual ya que en muchas de las pruebas que se realizaron no permitió una instalación completa si no se cumplía con ciertos parámetros como en el caso de memoria RAM que necesitó que se configuren 2GB y de espacio de almacenamiento con 12GB, a más de ello un procesador que pueda ocupar el 60 % de utilización del CPU del equipo anfitrión. Se definierón tambien tres adpatadores de red para que cualquiera pueda servir como adaptador auxiliar en caso de que alguno falle y cada adaptador de la red se lo configuró en modo promiscuo. Las imágenes de Kali Linux se las encontraron en un mirror alojado en una de las Instituciones de educación superior en esta caso la “Escuela Politécnica Nacional” [7] que cuenta con imágenes ISO[8] de los sistemas operativos utilizados, una vez descargado se lo ubica en un sitio desde el cual la máquina virtual tenga acceso, Se arranca en este punto el manejador de máquinas virtuales el cual en su paso siguiente pide la ubicación en la que se encuentra la imagen y la instalción se la realizó fijando algunas caraterísticas como idioma, teclado a emplear, direcciones de las tarjetas de red y usuarios que va a contener la máquina virtual. Una vez concluida la instalación de la máquina virtual se debe detenerla o almacenar su estado actual con la finalidad de exportar el servicio virtualizado que fue útil ya que en muchas de las modificaciones de la configuración la máquina

[4]Web Application Firewall.

[5]Equipo sobre el cual se instaló el sistema operativo para realizar el análisis.

[6]El sistema que se instala sobre la máquina virtual

[7]http://mirror.epn.edu.ec/

[8]El estándar ISO 9660 define un sistema de archivos para CD-ROM. Su propósito es que tales medios sean legibles por diferentes sistemas operativos

virtual dejó de funcionar y lo que se realizaba era importar el servicio virtualizado y continuar desde la instalación base.

El router[9] utilizado fue un TP-Link Modelo No. TL-WR841N / TL-WR841ND, al cual se lo configuró de modo que no tenga problemas ni obstáculos en su camino para llegar a sitio a ser examinado. Primero se registraron en una bitácora sus direcciones MAC[10] y se fijó una dirección IP fija[11] que corresponde a la entrada LAN de una de sus interfaces y que tenga conexión con un modem ADSL[12], al punto de acceso se fija para lo que corresponde a la red interna un SSID[13], fijando además el nivel de seguridad se lo desactiva, se habilita los controles de TCP, UDP e ICMP flood para que no se sature el router. Con la red ya configurada se inicia nuevamente la máquina virtual como usuario administrador(root) y como se definió previamente tres interfaces se porcede a levantarlas y se realizó pruebas de conectividad con el sitio destinado para revizar sus vulnerabilidades, se usó el comando ping y traceroute y cuando se obtiene el acceso se pudo iniciar con la revisión de las herramientas que posee Kali Linux 2.0 para realizar ataques o revisar vulnerabilidades. Como la etapa de reconocimiento se realizó en las instalaciones de la institución de salud y con el ambiente listo para que funcione se buscó cual de las herramientas cumplia con los requisitos de proporcionar la sufiente información del sitio y un entorno gráfico que permita tener una visión global del sitio. Se revisó inicialmente algunas herramientas que se conocen en el mercado como nmap, zenmap, netdiscover y maltego. la primera(nmap) fue muy útil pero no bridó mayor ayuda a nivel intuitivo, netdiscover y al igual que nmap no tenia una interfaz amigable al igual que netdiscover, zenmap posee interfaz amigable al usuario y se recopilo algunos tipos de análisis, en esta todo lo que se definió de manera gráfica se transormó a comandos nmap que se almacenaron automáticamente, un punto importante fue que esta herramienta posee la definición de profiles que permiten hacer una agrupación de parámetros de nmap y almacenarlos para su reutilización.

En el caso de maltego que se encuentra en el menú de opciones más utilizadas en Kali Linux se la revisó para su utilización y la diferencia principal que se encontró fue que necesitava cada usuario registrar sus datos en un sitio externo[14] creando una cuenta para que se pueda realizar la revisión de dominio y sus diferentes tipos de escaneos. Cuando se completo la tarea anterior se pudó ingresar ya a la interfaz gráfica presentada por la herramienta(maltego) y se registro la información de correo de las personas encargadas de realizar el escaneo y revisa en su base de datos que la cuenta se encuentre registrada y lista para su utilización. Esta herramienta permite en la versión instalada que es comunitaria[15]conectarse a un servidor externo que contiene información de servidores de nombre a nivel mundial y esta es la opción que se utilizó para iniciar la revisión del dominio. Cuando se ingresa el dominio automáticamente se transforma en un entorno gráfico que permite ir transformando o explotando sus nodos y en ese caso obtener direcciones IP, servidores de nombre y las cuentas de correo de los administradores del sitio.

En este caso la herramienta(maltego) proporcionó una interfaz de usuario amigable e información que con las otras herramientas no se pudo obtener.

[9]Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

[10]En las redes de computadoras, la dirección MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

[11]Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red que utilice el protocolo IP, que corresponde al nivel de red del Modelo OSI.

[12]Módem ADSL: modula las señales enviadas desde la LAN para que puedan transmitirse por la línea ADSL y demodula las señales recibidas.

[13]El SSID (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.

[14]www.paterva.com/web6/community/maltego

[15]En el caso de maltego community permite hacer un número limitado de revisiones a los dominios ingresados.

Figura 1. Herramienta empleada para escaneo de dominio

Cuando se obtuvo la dirección IP del sitio se revisó documentación de las herramientas de XSS y se encontró un listado de las que se utiliza en este tipo de ataques y se encontró a Metasploit que es un framework que permite realizar el ciclo completo del hacker y viene instalado con Kali Linux pero se encontró que no viene con alguna herramienta que permita realizar este tipo de ataques, pero que mediante la utilización de ciertos módulos se puee integrar componentes como beef que es otro framewor que permite realizar este tipo de ataques, motivo por el que se descartó a mencionada herramienta.

Cuando se cumple ya la fase previa el paso siguiente es iniciar con la revisión de las herramientas y la primera en revisarse fue zaproxy al cual se lo puede arrancar ingresando por el menú contextual y en la opción de análisis de aplicaciones web aparece su ícono. Cuando se accede a este componente aparece una ventana en la que permite ingresar el URL para ello se debe revisar la opción de política de la herramienta en la que se definió el nivel de ataque en este caso se definió un ataque de alto nivel y que genere un log de las mismas características, posee esta herramienta la posibilidad de habilitar plugins[16] que permite revisar desde un navegador en específico la revisión de sus vulnerabilidades, posee también un componente que permite generar payloads[17]de manera autática, así como los reportes de las páginas más vulnerables.

[16]Componente que se puede añadir a un programa para aumentar sus capacidades.

[17]Script de generación de código generalmente javascript que se puede utilizar en ataques XSS.

## IV. EVALUACIÓN DE RESULTADOS Y DISCUSIÓN

## V. TRABAJOS RELACIONADOS

## VI. CONCLUSIONES Y TRABAJO FUTURO

## REFERENCIAS


[1] Robert W. Beggs. *Mastering Kali Linux for Advanced Penetration Testing*, volume 4 of *10*. Published by Packt Publishing Ltd., 2014.

[2] Juan Ramón Bermejo Higuera. Metodología de evaluación de herramientas de análisis automático de seguridad de aplicaciones web para su adaptación en el ciclo de vida de desarrollo= assessment methodology of web applications automatic security analysis tools for adaptation in the development life cycle. 2014.

[3] Jorge López. Virtualización sencilla con virtualbox. *Todo linux: la revista mensual para entusiastas de GNU/LINUX*, (88):21–24, 2008.

[4] Mario Andrés Torres Samaniego. *Desarrollo e implementación de un sistema de administración de aprendizaje (LMS: Learning Management System) disponible para Universidades.* PhD thesis, 2013.