MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito

Aplicaciones Web y Apps Móviles

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Marzo 2019

Sobre MILE-SEC

MILE-SEC
Capacitación y Consultoría en
Hacking Ético & Forense Digital

MILESEC E.I.R.L, es una empresa de capitales Peruanos fundada en el año 2017, netamente dedicada a brindar servicios de capacitación a empresas, instituciones, organizaciones y profesionales, en las áreas de seguridad de la información y tecnologías de la información (T.I.), tales como; Pruebas de Penetracion, Hacking Ético, Evaluación de Vulnerabilidades, Forense de Computadoras y Forense Digital. Así mismo brinda servicios de consultorías especializadas en todas las áreas antes mencionadas.

Durante estos años ha realizado capacitaciones presenciales y consultorías tanto públicas cuanto privadas para Ecuador y Perú, en las ciudades de Lima, Cusco y Trujillo. Así mismo ha realizado capacitaciones online o virtuales.


http://www.mile-sec.com/

informes@mile-sec.com / mileseceirl@gmail.com

https://www.facebook.com/mileseceirl/

https://twitter.com/mileseceirl

https://www.linkedin.com/in/milesec/

Temario

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- Seleccionar las herramientas para pruebas de seguridad web
- Buscar vulnerabilidades web
- Recorrido de directorio
- Medidas correctivas contra recorrido de directorio
- Ataques para filtrado de entradas
- Medidas correctivas contra ataques de entradas
- Ataques de scripts por defecto
- Medidas correctivas contra ataques de scripts por defecto
- Mecanismos de login sin asegurar
- Medidas correctivas contra el login sin asegurar
- Realizar escaneos generales de seguridad para vulnerabilidades en aplicaciones web
- Minimizar los riesgos de seguridad web
- Practicar seguridad por obscuridad
- Poner firewalls
- Analizar código fuente
- Descubrir fallas en Apps móviles

Introducción

Los sitios web y aplicaciones web son objetivos comunes para ataques, porque están en todos lados, y frecuentemente están abiertos para cualquiera acceda. Básicamente, los sitios web se utilizan para marketing, información de contacto, descarga de documentos, y similares, de tal manera es fácil para los atacantes maliciosos atacarlos. Las plataformas web comúnmente utilizadas como WordPress y sistemas relacionados para la gestión de contenido, son especialmente vulnerables para ser atacados, debido a su presencia, además de ausencia de pruebas y parches.

Para los atacantes maliciosos los sitios web proporcionan una delantera hacia aplicaciones web complejas y bases de datos, para almacenar información valiosa, como tarjetas de crédito, y otra información sensible, los cuales son muy atractivos. Aquí es donde el dinero está, ya sea literalmente y figurativamente.

Seleccionar las herramientas para pruebas de seguridad web

Las buenas herramientas para pruebas de seguridad, pueden ayudar a garantizar se obtenga el máximo provecho del trabajo. Como muchas cosas en la vida, se obtendrá aquello por lo cual se paga, cuando se trata de probar por agujeros en seguridad. Esta es la razón por la cual se utilizan herramientas comerciales cuando se evalúan sitios web y aplicaciones web por vulnerabilidades.

- Acunetix Web Vulnerability Scanner
- AppSpider
- Web Developer
- Netsparker

* https://www.acunetix.com/
* https://www.rapid7.com/products/appspider/
* https://chrispederick.com/work/web-developer/
* https://www.netsparker.com/

Buscar vulnerabilidades web

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los ataques contra los sitios web y aplicaciones vulnerables mediante HTTP, constituyen la mayoría de ataques relacionados en Internet. Muchos de estos ataques pueden ser realizados incluso si el tráfico HTTP está encriptado (mediante HTTPS), también conocido como HTTP sobre SSL/TLS, porque el medio de comunicación no tiene relación con estos ataques. Las vulnerabilidades de seguridad actualmente se encuentran en los sitios web, y las aplicaciones por si misma, o en el servidor web y el software del navegador ejecutándose en los sistemas, y con los cuales se comunican.

Muchos ataques contra los sitios web y aplicaciones son solo pequeñas molestias, y podrían no afectar información confidencial o la disponibilidad del sistema. Sin embargo, algunos ataques pueden causar estragos en los sistemas, poniendo en riesgo información sensible e incluso haciendo la organización no cumpla con las leyes y regulaciones estatales, federales e internacionales de privacidad, y seguridad de la información.

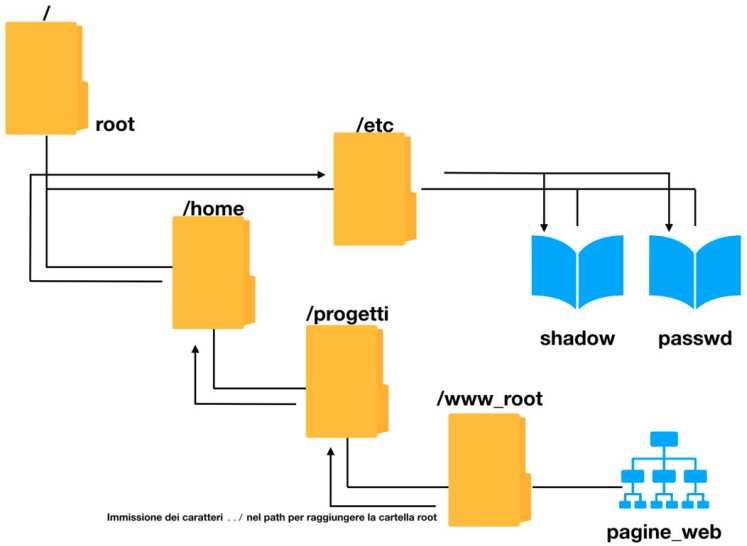
Recorrido de directorio

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

El recorrido de directorio es realmente una debilidad muy básica, pero puede tornarse interesante, pues algunas veces expone información sensible sobre los sistemas web. Este ataque involucra navegar un sitio y buscar por huellas sobre la estructura de directorios del servidor, y archivos sensibles podrían ser cargados intencionalmente o no.

- Crawlers
- Google

- site
- filetype:
- allintitle:
- inurl:
- related:
- link:



* https://www.httrack.com/
* https://www.google.com
* https://www.exploit-db.com/google-hacking-database

Medidas correctivas contra recorrido de directorio

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se pueden emplear tres medidas correctivas principales para evitar se comprometan archivos a través del recorrido de directorio:

- No almacenar, archivos antiguos, no públicos, o sensibles en el servidor web.
- Configurar el archivo “robots.txt” para prevenir motores de búsqueda, como Google, hagan crawling hacia área más sensibles del sitio.
- Asegurarse del servidor web está adecuadamente configurado para permitir acceso público hacia únicamente aquellos directorios necesarios para el funcionamiento del sitio.

Las más recientes versiones de los servidores web, tienen buena seguridad en los directorios. Asegurarse de ejecutar las más recientes versiones.

* http://httpd.apache.org/docs/current/configuring.html
* http://ghh.sourceforge.net/

Ataques para filtrado de entradas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los sitios web y aplicaciones están implementados para tomar prácticamente cualquier tipo de entrada, asumiendo erróneamente son válidos, y posteriormente procesarlo. No validar las entradas es uno de los más grandes errores hecho por los desarrolladores web.

Muchos ataques pueden insertar datos malformados, frecuentemente, muchos a la vez, los cuales pueden ser ejecutados contra un sitio web o aplicación, lo cual puede confundir al sistema para hacerlo divulgar mucha información hacia el atacante. Los ataques de entrada pueden también facilitar el atacante malicioso obtengan información desde el navegador web de los usuarios confiados.

- Desbordamientos de buffer
- Manipulación de la URL
- Manipulación de un campo oculto
- Inyección de código e inyección SQL
- Cross-site scripting

Medidas correctivas contra ataques de entradas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los sitios web y aplicaciones deben filtrar datos entrantes. Lo sitios y aplicaciones deben verificar y asegurarse los datos ingresados encajan dentro de los parámetros esperados por la aplicación web. Si los datos no coinciden, la aplicación debe generar un mensaje de error o devolver hacia la página previa.

Prácticas seguras de codificar software pueden eliminar todos estos problemas, si se hace una parte crítica del proceso de desarrollo. Los desarrolladores deben conocer e implementar estas mejores prácticas:

- Nunca presentar valores estáticos no necesarios de ser visualizados por el usuario y el navegador web.
- Filtrar los etiquetas <script> desde los canpos de entrada
- Deshabilitar mensajes de error detallados del servidor web y bases de datos, si es posible.

Ataques de scripts por defecto

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Programas web pobremente escritos, como scripts PHP y ASP, pueden permitir a los atacantes maliciosos visualizar y manipular archivos sobre el servidor web, y otra cosas para las cuales no está autorizado. Estas fallas son también comunes en los CMSs, los cuales son utilizados por los desarrolladores, equipos de TI, y profesionales de marketing para mantener el contenido de un sitio web.

Los ataques de scripts por defecto son comunes porque código muy pobremente escrito es accedible públicamente en sitios web. Los atacantes maliciosos también pueden aprovecharse de varios scripts de ejemplo instalados en los servidores web, especialmente versiones antiguas del servidor IIS de Microsoft.

Muchos desarrolladores y webmasters utilizan estos scripts sin entender como realmente funcionan, o sin probarlos, lo cual puede introducir serias vulnerabilidades de seguridad.

Medidas correctivas contra ataques de scripts por defecto

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se puede ayudar a prevenir ataques contra scripts web por defecto de la siguiente manera:

- Conocer como los scripts funcionan antes de desplegarlos dentro del entorno web.
- Asegurarse los scripts por defecto o de ejemplo son eliminados del servidor web antes de utilizarlos.
- Mantener cualquier CMS actualizado. No utilizar scripts públicamente accedibles los cuales contengan información confidencial.
- Definir permisos en los archivos sobre áreas sensibles de la aplicación o sitio, para prevenir acceso público.

Mecanismos de login sin asegurar

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Muchos sitios web requieren al usuario “loguearse” antes de poder hacer cualquier cosa dentro de la aplicación. Estos mecanismo de login frecuentemente no manejan correctamente los IDs de usuarios y contraseñas. Frecuentemente divulgan mucha información, lo cual puede ser utilizada por un atacante malicioso para obtener IDs válidos de usuario y contraseñas.

Para probar mecanismos de login inseguro, se debe navegar la aplicación y hacer “login”

- Utilizar un ID de usuario no válido con una contraseña no válida
- Utilizar un ID de usuario válido con una contraseña no válida
- Utilizar un ID de usuario no válido y una contraseña no válida

Una herramienta para tratar de “averiguar contraseñas” en Hydra.

* https://github.com/vanhauser-thc/thc-hydra
* ftp://ftp.cerias.purdue.edu/pub/dict
* https://packetstormsecurity.com/Crackers/wordlists

Medidas correctivas contra el login sin asegurar

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se pueden implementar la siguientes medidas correctivas para prevenir personas ataquen los sistemas débiles de login, en las aplicaciones web.

- Cualquier error de login devuelto hacia el usuario final debería ser tan genérico como sea posible.
- La aplicación nunca deberá devolver códigos de error en la URL para diferencias usuarios y contraseñas válidas y no.
- Utilizar CAPTCHA o (reCAPTCHA), o formulario de login web para prevenir intentos de romper contraseñas.
- Emplear un mecanismo para bloqueo de intrusos en el servidor web, o dentro de la aplicación web.
- Verificar por y cambiar cualquier contraseña por defecto del proveedor, a algo fácil de recordar, pero difícil de romper.

Escaneos de seguridad para vulnerabilidades aplicaciones web

Es necesario reiterar la necesidad de las pruebas manuales y automáticas contra los sistemas web. Pues no se tendrá una imagen global confiando únicamente en alguna de estos métodos. Es altamente recomendable utilizar escáneres de vulnerabilidades contra aplicaciones web, todo en uno, como por ejemplo Acunetix o AppSpider, para ayudar a descubrir vulnerabilidades a un precio razonable, sino será muy difícil encontrarlos de otra manera.

Combinar los resultados de un escáner con una mentalidad maliciosos y las técnicas de hacking, se tendrá la capacidad de encontrar muchas fallas de seguridad web.

Minimizar los riesgos de seguridad web

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Mantener las aplicaciones web seguras requieres vigilancia constante, además de procedimientos de hacking ético, con una buena dosis de apoyo por parte de los desarrolladores web y proveedores. Manteniéndose actualizado en las últimas técnicas de ataque, herramientas para evaluación y técnicas, además de permitir a los desarrolladores y proveedores conocer cuan prioritaria es la seguridad para la organización.

Se puede ganar experiencia directa en las pruebas y técnicas de hacking contra aplicaciones web, utilizando diversos recursos, como OWASP Testing Guide.

* https://www.owasp.org/index.php/OWASP_Testing_Project

Practicar seguridad por obscuridad

Ocultar algo de una vista obvia utilizando método triviales; puede ayudar a prevenir ataques automáticos como gusanos, o scripts, los cuales atacan tipos de scripts específicos o puertos HTTP por defecto.

- Para proteger las aplicaciones web y bases de datos, usar diferentes máquinas para ejecutar cada servidor web, aplicación y base de datos.
- Utilizar un servidor web con funcionalidades de seguridad incorporadas, para maneja los controles de acceso y realizar procesos aisladamente. Esto ayuda a asegurar si una aplicación es atacada, no necesariamente se pondrán otras aplicaciones en riesgo sobre el mismo servidor
- Utilizar una herramienta para obscurecer la identidad del servidor web.
- Si se está ejecutando un servidor Linux, utilizar un programa para cambiar la huella del sistema operativo.
- Cambiar el servidor web para ejecutarse en un puerto no estándar.

Poner firewalls

Considerar los siguientes controles adicionales para proteger los sistemas web, incluyendo lo siguiente:

- Un firewall basado en red o IPS, el cual pueda detectar y bloquear ataques contra las aplicaciones web.
- Un IPS basado en host para aplicaciones web.

Estos programas pueden detectar ataques contra bases de datos y aplicaciones web en tiempo real, además de cortarlos antes de tener la posibilidad de dañar algo.

* https://www.watchguard.com/
* https://www.paloaltonetworks.com/
* https://www.port80software.com/products/serverdefender
* https://www.barracuda.com/products/webapplicationfirewall
* https://www.fortinet.com/products/web-application-firewall/fortiweb.html

Analizar código fuente

El desarrollo de software es donde muchos agujeros de seguridad empiezan y deben finalizar, pero raramente es así. Si se siente confianza en los esfuerzos de las pruebas de seguridad en este punto, se debe profundizar más para encontrar fallas de seguridad en el código fuente, pues hay cosas las cuales podrían nunca ser descubiertas por los escáneres tradicionales, y técnicas de hacking, pero sin embargo son serios problemas.

Esto es más simple de lo cual se puede percibir, pues no es necesario ir línea por línea en el código y ver si sucede algo. No es incluso necesaria experiencia en desarrollo (aunque se sugiere).

Para este propósito existen diversas herramientas disponibles.

* https://www.roguewave.com/products-services/klocwork
* https://www.checkmarx.com/

Descubrir fallas en Apps móviles

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Adicionalmente a ejecutar herramientas automáticas para verificar por vulnerabilidades en Apps móviles, existen otras cosas por las cuales se debe buscar, incluyendo:

- Bases de datos de claves criptográficas, las cuales están fijas en la aplicación
- Mejorar el manejo de información sensible; como información identificable personalmente (PII, localmente donde el usuario y otras apps puedan accederlo.
- Debilidades de Login, como ser capaz de evadir formularios de login
- Permitir contraseñas en blanco o débiles.

No todas estas verificaciones son descubiertas mediante un análisis manual, y podrían requerir herramientas adicionales.

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito

Aplicaciones Web y Apps Móviles

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Marzo 2019