Pruebas de Seguridad en aplicaciones web segun OWASP

Donde estamos... Hacia donde vamos?

Edgar D. Salazar T

OWASP Venezuela Chapter Leader
edgar.salazar@owasp.org
@3ddavid

Realidad o Ficción

3ddavid Edgar D Salazar T
Lulzsec ataca la web de una agencia de seguridad del Gobierno británico bit.ly/jiyT6L
20 jun

InForenses Informatica Forense
Hackearon página web de la Asamblea Nacional VIA http://bit.ly/mIkQKa @Globovisión
13 jun

seguinfo Segu-Info
Anonymous lanzó ciberataque contra web del Senado argentino y SADAIC: El ataque a los sitios webs de el Senado a...
http://bit.ly/kgYKZK
29 jun

InForenses Informatica Forense
Hackers bloquean por horas página electrónica de Cancillería de ... - El Nacional.com tiny.ly/Hbbr
11 jun

seguinfo Segu-Info
Cae el website de MasterCard, probablemente por un nuevo ataque relacionado con WikiLeaks: El website principal ...
http://bit.ly/ki296X
1 jul


Expectativas
Controles
Contexto
Un sistema es seguro si cumple las expectativas en un contexto dado

La Seguridad total no existe.

El riesgo no puede eliminarse completamente, pero puede **reducirse**.

OWASP ¿Por que? Y ¿Para quien?

Desarrolladores de Software

Testers de Software

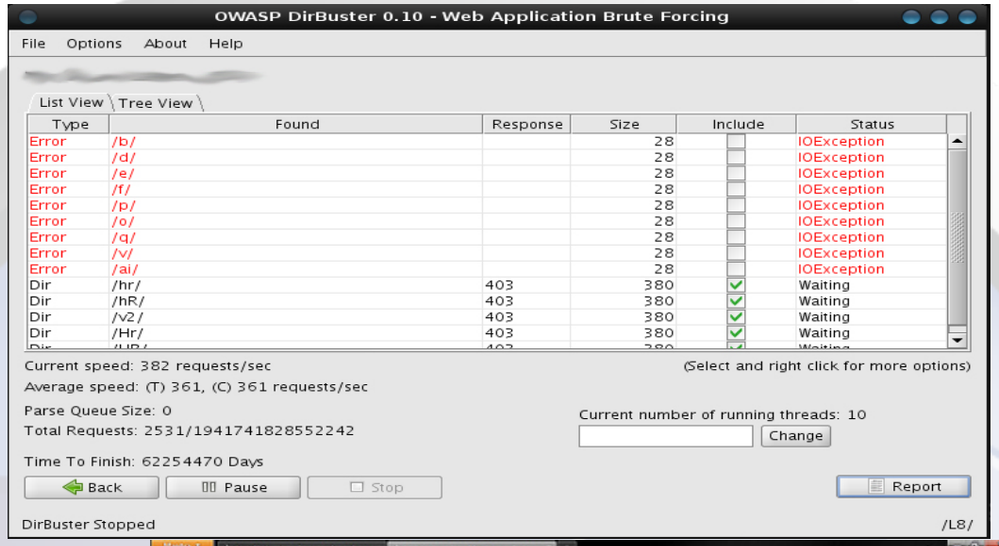
Especialistas de Seguridad

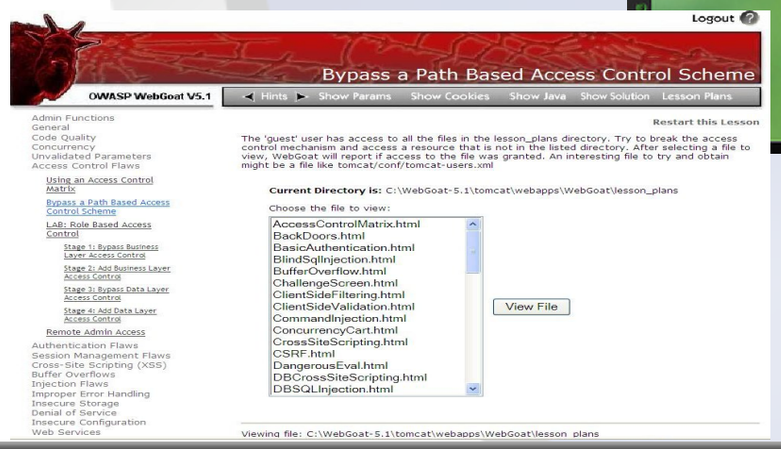
Proyectos Documentales de OWASP

- ✔ Preguntas Frecuentes sobre Seguridad en Aplicaciones web (OWASP FAQ)
- ✔ Guía de Desarrollo Seguro (OWASP Development)
- ✔ Guía de Pruebas (OWASP Testing Guide)
- ✔ Guia de Revision de Codigo (OWASP Code Review)
- ✔ OWASP TOP-10 (Los 10 riesgos mas importantes en aplicaciones web)
- ✔ OWASP Seguridad Movil (OWASP mobile Security)
- ✔ Como detectar y responder en tiempo real los ataques a aplicaciones
- ✔ Estándar de Verificación de Seguridad en Aplicaciones
- ✔ Entre muchos mas...

Proyectos Software de OWASP

- ✔ WebScarab --> ZAP (The Zed Attack Proxy)
- ✔ Dirbuster
- ✔ DotNet
- ✔ ESAPI
- ✔ WebGoat
- ✔ Mantra Framework
- ✔ OWASP Live CD
- ✔ OWASP AntiSamy Java Project
- ✔ OWASP WAF
- ✔ Entre muchos mas...





Pruebas de Seguridad según OWASP

El conjunto de prueba de OWASP se divide en 10 sub categorías las cuales se mencionan a continuación:

- Recopilación de Información
- Pruebas de gestión de la configuración
- Pruebas de la lógica de negocio
- Pruebas de Autenticación
- Pruebas de Autorización
- Pruebas de gestión de sesiones
- Pruebas de validación de datos
- Pruebas de denegación de Servicio
- Pruebas de Servicios Web
- Pruebas de AJAX

Pruebas de Seguridad según OWASP

Recopilación de Información

La primera fase en la evaluación de seguridad se centra en recoger tanta información como sea posible sobre una aplicación objetivo. La recopilación de información es un paso necesario en una prueba de intrusión. Esta tarea se puede llevar a cabo de muchas formas.

- Spiders, Robots, y Crawlers
- Reconocimiento mediante motores de Búsqueda
- Identificación de puntos de entrada de la aplicación
- Pruebas para encontrar firmas de Aplicaciones Web
- Descubrimiento de aplicaciones
- Análisis de códigos de error

Pruebas de Seguridad según OWASP

Pruebas de Gestión de la Configuración

A menudo los análisis sobre la infraestructura o la topología de la arquitectura pueden revelar datos importantes sobre una aplicación Web. Se pueden obtener datos como por ejemplo el código fuente, los métodos HTTP permitidos, funcionalidades administrativas, métodos de autenticación y configuraciones de la infraestructura.

- Pruebas de SSL/TLS
- Pruebas del receptor de escucha de la BD
- Pruebas de gestión de configuración de la infraestructura
- Pruebas de gestión de configuración de la aplicación
- Gestión de extensiones de archivo
- Archivos antiguos, copias de seguridad y sin referencias
- Interfaces de administración de la infraestructura y de la aplicación
- Métodos HTTP y XST

Pruebas de Seguridad según OWASP

Comprobación del Sistema de Autenticación

Autenticar un objeto puede significar confirmar su procedencia, mientras que autenticar a una persona consiste a menudo en verificar su identidad. La autenticación depende de uno o más factores de autenticación. En seguridad informática, autenticación es el proceso de intentar verificar la identidad digital del remitente de una comunicación.

- Transmisión de credenciales a través de un canal cifrado
- Enumeración de usuarios
- Pruebas de diccionario sobre cuentas de Usuario o cuentas predeterminadas
- Pruebas de Fuerza Bruta
- Saltarse el sistema de autenticación
- Comprobar Sistemas de recordatorio/restauración de contraseñas vulnerables
- Comprobar Sistemas de recordatorio/restauración de contraseñas vulnerables
- Pruebas de gestión del Caché de Navegación y de salida de sesión
- Pruebas de CAPTCHA
- Múltiples factores de autenticación
- Probar por situaciones adverzas

Pruebas de Seguridad según OWASP

Gestión de Sesiones

La gestión de sesiones cubre ampliamente todos los controles que se realizan sobre el usuario, desde la autenticación hasta la salida de la aplicación. HTTP es un protocolo sin estados, lo que significa que los servidores web responden a las peticiones de clientes sin enlazarlas entre sí.

Es importante que la seguridad de la aplicación sea considerada en el contexto de los requisitos y expectativas del proveedor.

Pruebas de Seguridad según OWASP

Pruebas de Autorización

Autorización es el concepto de permitir el acceso a recursos únicamente a aquellos que tienen permiso para ello. Las pruebas de Autorización significan entender como funciona el proceso de autorización, y usar esa información para saltarse el mecanismo de autorización.

Pruebas de Seguridad según OWASP

Pruebas de Logica de Negocio

Comprobar por fallas en la logica de negocio en una aplicación web multifuncional requiere pensar en modos no convencionales. Si el mecanismo de autenticación de una aplicación es desarrollado con la intención de seguir pasos 1,2,3 para poder autenticarse, que pasa si uno salta del paso 1 directo al 3? En este ejemplo, la aplicación o bien provee acceso fallando el mecanismo de autenticación, muestra un mensaje de error de acceso negado, o solo un mensaje de error 500?

Pruebas de Seguridad según OWASP

Pruebas de Validación de Datos

La debilidad más común en la seguridad de aplicaciones web, es la falta de una validación adecuada de las entradas procedentes del cliente o del entorno de la aplicación. Esta debilidad conduce a casi todas las principales vulnerabilidades en aplicaciones, como inyecciones sobre el intérprete, ataques locale/Unicode, sobre el sistema de archivos y desbordamientos de búfer.

Pruebas de Seguridad según OWASP

Pruebas de Denegación de Servicio

El tipo más común de ataque de Denegación de Servicio (Dos) es del tipo empleado en una red para hacer inalcanzable a la comunicación a un servidor por parte de otros usuarios válidos. El concepto fundamental de un ataque DoS de red es un usuario malicioso inundando con suficiente tráfico una máquina objetivo para conseguir hacerla incapaz de sostener el volumen de peticiones que recibe. Cuando el usuario malicioso emplea un gran número de máquinas para inundar de tráfico una sola máquina objetivo, se conoce generalmente como ataque denegación de servicio distribuidos (DDoS).

Pruebas de Seguridad según OWASP

Pruebas de Servicios WEB

Los servicios web y SOA (Arquitectura Orientada a Servicios) son aplicaciones en expansión que están permitiendo que los negocios interoperen y crezcan a un ritmo sin precedentes. Los clientes de servicios web generalmente no son frontales web, sino otros servidores. Los servicios web están expuestos a la red como cualquier otro servicio, pero pueden ser utilizados en HTTP, FTP, SMTP o acompañados de cualquier otro protocolo de transporte.

Las vulnerabilidades en servicios web son similares a otras vulnerabilidades como la inyección SQL, revelación de información, etc, pero también tienen vulnerabilidades de XML.

Pruebas de Seguridad según OWASP

Pruebas de AJAX

El uso de las técnicas AJAX puede conseguir enormes beneficios en la experiencia de uso por parte de los usuarios de las aplicaciones web. Sin embargo, desde el punto de vista de la seguridad, las aplicaciones AJAX tienen una superficie de ataque mayor que las aplicaciones web convencionales, a veces son desarrolladas centrándose más en qué se puede hacer que en qué se debería hacer. Además, las aplicaciones AJAX son más complicadas porque el procesamiento se realiza tanto en el lado del cliente como en el lado del servidor.

“La seguridad de un sistema informático es inversamente proporcional a la estupidez del administrador”

@owasp

http://www.owasp.org

@owasp_ven
http://www.owasp.org/index.php/venezuela

Edgar D Salazar T

@3ddavid
edgar.salazar@owasp.org

Dudas o Preguntas?