Vulnerabilidades en Aplicaciones Web

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 5 de Noviembre del 2015

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Digital Forensics.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS www.facebook.com/alonsoreydes

pe.linkedin.com/in/alonsocaballeroquezada/

Vulnerabilidad más comunes en Aplicaciones Web

¿Qué es lo que típicamente buscan los atacantes cuando evalúan una aplicación web?. Los problemas son usualmente copiosos, pero pueden agruparse en pocas categorías.

“Open Web Application Security Project” - OWASP ha realizado un gran trabajo en documentar con un consenso general las vulnerabilidades de seguridad en aplicaciones web más críticas.

Es muy interesante su “Top Ten Project”, el cual proporciona una lista regularmente actualizada de los temas de seguridad en aplicaciones web.

Los ejemplos expuestos a continuación detallan algunas de estas categorías de OWASP.

1. Cross-Site Scripting (XSS)
2. Injection Flaws (SQLi)
3. Cross-Site Request Forgery (CSRF)

* OWASP - http://www.owasp.org

Cross-Site Scripting

Los ataques Cross-Site Scripting recaen en la deficiencias de validación de entrada / salida en aplicaciones web. Sin embargo, a diferencia de otros tipos de ataque, el objetivo de XSS no es la aplicación en si misma, sino los otros usuarios de la aplicación vulnerable.

Por ejemplo, un usuario malicioso puede publicar un mensaje en una aplicación web “Libro de visitantes” con un contenido ejecutable. Cuando otro usuario visualice este mensaje, el navegador interpretará el código y lo ejecutará, dando control al atacante sobre el sistema del segundo usuario. Por lo tanto la carga de un ataque XSS afecta típicamente la aplicación del usuario final.

Un XSS adecuadamente ejecutado puede ser devastador de una aplicación web , como también en la reputación de la organización. Un XSS puede generar el secuestro de cuentas y sesiones o robo de cookies.

OWASP describe con buen detalle técnico los ataques XSS.

* XSS OWASP - https://www.owasp.org/index.php/XSS

SQL Injection

Las aplicaciones web modernas confían en contenidos dinámicos. Esto se logra recuperando datos actualizados desde una Base de Datos o un servicio externo. En respuesta a una petición para una página web, la aplicación generará una consulta, algunas veces incorporando porciones de la petición dentro de la consulta.

Si la aplicación no es cuidadosa en la forma como construye la consulta, un atacante puede alterar la consulta, modificando como esta es procesada por el servicio externo.

Estas fallas de inyección pueden ser devastadoras, pues el servicio algunas veces confía completamente en la aplicación web, y casi siempre escondido “a salvo” detrás de algunos firewalls.

Una de las plataformas más populares para almacenar datos web es SQL, y muchas aplicaciones web están basadas completamente en scripts front-end los cuales simplemente consultan una base de datos SQL, ya sea en el mismo servidor web o en un sistema back-end separado.

SQL Injection (Cont.)

Una de las mecanismos más eficientes para realizar esto es la técnica denominada SQL Injection. Mientras las fallas de inyección afectan cualquier tipo de dispositivos externos, SQL Injection es de lejos la más prevalente y popular de las fallas.

Una SQL Injection se relaciona al ingreso en bruto de consultas SQL dentro de una aplicación para realizar un acción inesperada. Algunas veces, las consultas existentes son simplemente editadas para lograr los mismos resultados – SQL es fácilmente manipulable por la ubicación de incluso un solo carácter en un lugar seleccionado con acierto, causando comportamiento bastante malicioso consulta. Algunos de los caracteres utilizados comúnmente para estos ataques de validación de ingreso incluyen la comilla simple ('), doble guión (--), y el punto y coma (;). Todos estos con un especial significado en SQL.

OWASP describe con buen detalle técnico los ataques SQL Injection.

* SQL Injection OWASP - https://www.owasp.org/index.php/SQL_Injection

Cross Site Request Forgery

Las vulnerabilidades CSRF se conocen desde hace una década, pero recientemente se han reconocido como un tema bastante serio.

El concepto de un CSRF es sencillo: una aplicación web proporciona a los usuarios una autenticación de sesión persistente, de esta manera no hay necesidad de autenticarse nuevamente cada vez se solicita una página. Pero si un atacante puede convencer al navegador web del usuario a enviar una petición hacia un sitio web, puede aprovecharse de la sesión persistente para realizar acciones en lugar de la víctima. El resultado es una variedad de situaciones: cambio de contraseña de una cuenta, transferencia de dinero, compra de mercancía, y más.

Un CSRF es fácil de explotar. Un atacante inserta una etiqueta “image” dentro de una página web, cuando la víctima carga la pagina, su navegador enviará la petición GET para cargar en enlace insertado en esta etiqueta.

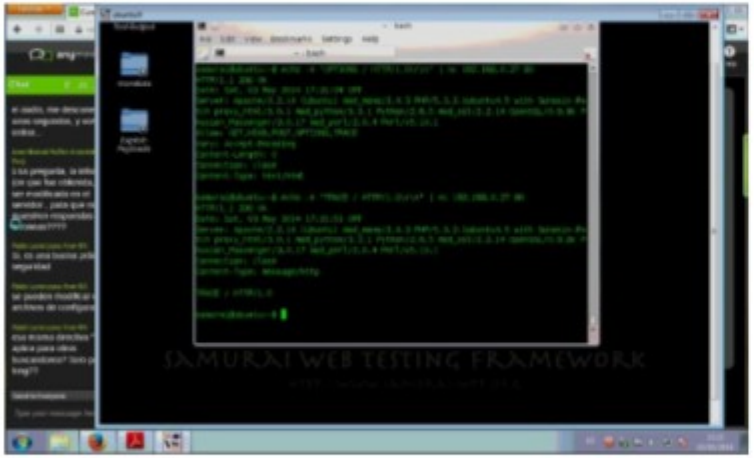
OWASP describe con buen detalle técnico los ataques CSRF.

* CSRF OWASP - https://www.owasp.org/index.php/CSRF

Curso Virtual de Hacking Aplicaciones Web

Curso Virtual de Hacking Aplicaciones Web

2015



Último Curso del año 2015

Grupo Sábado:

7, 14, 21 y 28 de Noviembre del 2015
De 9:00am a 12:45pm (UTC -05:00)

Grupo Domingo:

8, 15, 22 y 29 de Noviembre del 2015
De 9:00am a 12:45pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Más Información: http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web
E-mail: **caballero.alonso@gmail.com** / Sitio Web: http://www.reydes.com

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

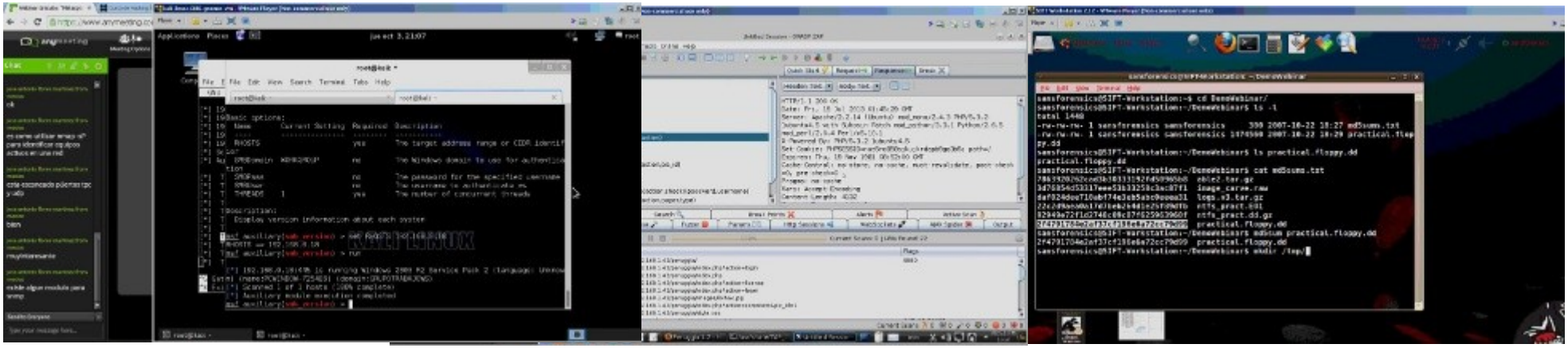
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

http://www.reydes.com/d/?q=Curso_de_Informatica_Forense



Más Contenidos

Videos de 30 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Diapositivas utilizadas en los Webinars Gratuitos.

http://www.reydes.com/d/?q=node/3

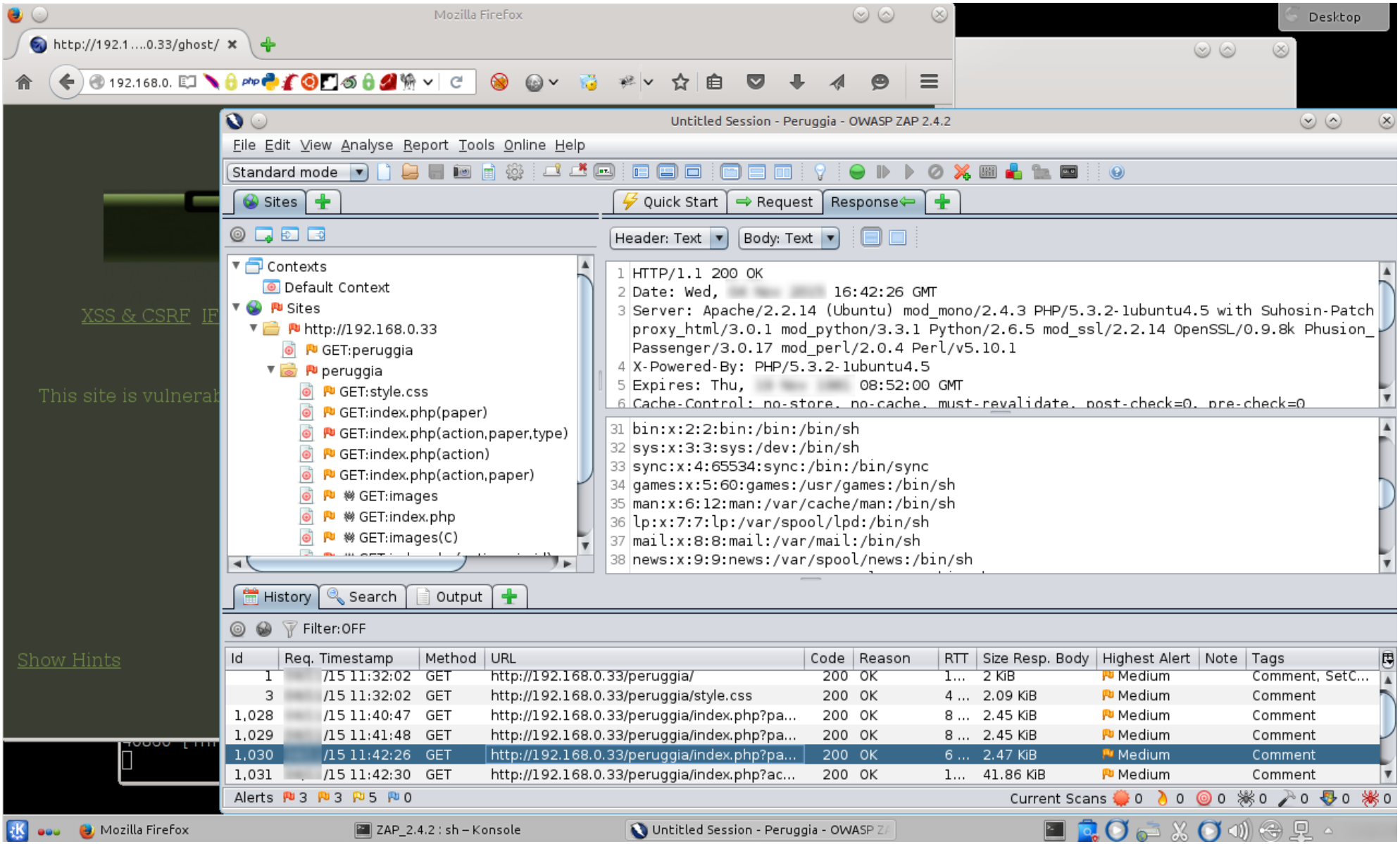
Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1

Demostraciones



Vulnerabilidades en Aplicaciones Web

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 5 de Noviembre del 2015