Webinar Gratuito
Vulnerabilidades en Aplicaciones Web

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Cómputo Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 4 de Julio del 2013

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Cómputo Forense y GNU/Linux.

- Ex Integrante de RareGaZz y actual integrante de PeruSEC.

- Ex Redactor en la Revista Linux+ DVD (ES).

- Creador del II Reto Forense Digital Sudamericano - Chavin de Huantar 2012.

- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.

- Más de 10 años de experiencia en el área.

- Twitter: @Alonso_ReYDeS

- LinkedIn: pe.linkedin.com/in/alonsocaballeroquezada/

Vulnerabilidades más comunes en App Web

¿Qué es lo que típicamente buscan los atacantes cuando evalúan una aplicación web?. Los problemas son usualmente copiosos, pero pueden reunirse en algunas 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 que se expondrán a continuación detallan algunas de estas categorías de OWASP.

1. Cross-Site Scripting (XSS)
2. Injection Flaws (i)
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 del 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 se 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, ya que 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 que 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 que 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 que toda la consulta se comporte de manera bastante maliciosa. Algunos de estos 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 significa 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 detrás 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 que se solicita una página. Pero si un atacante puede convencer al navegador web del usuario a enviar una petición a un sitio web, puede tomar ventaja 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.

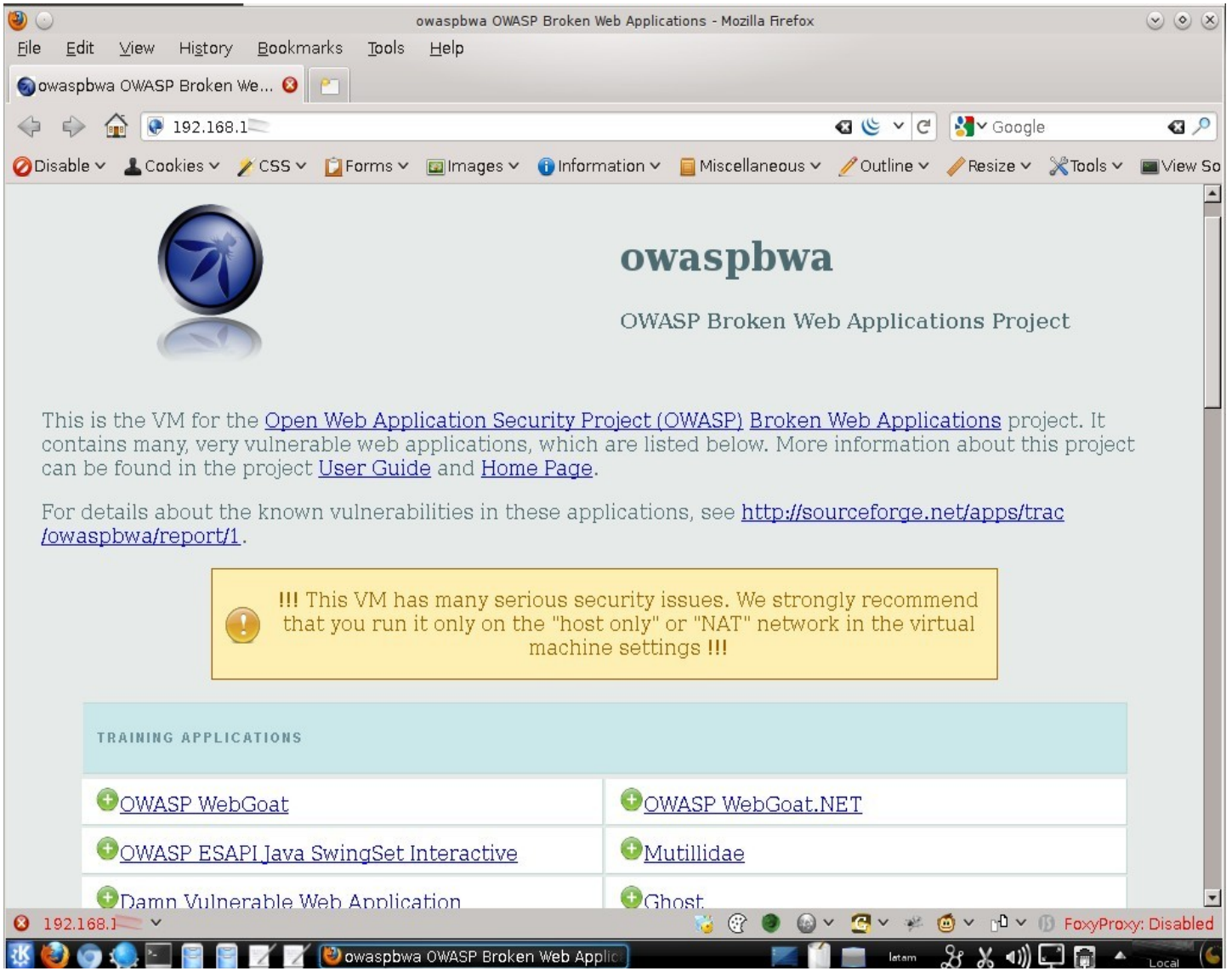
Un CSRF es fácil de explotar. Un atacante inserta una etiqueta “image” dentro de una página web, cuando la víctima carga la pagina, su navegador enviará la petición GET para cargar en enlace insertado en esta etiqueta.

OWASP describe con buen detalle técnico los ataques CSRF.

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

Demos

Es momento de las demostraciones



Curso Online de Hacking Aplicaciones Web

Días:

Sábados 6, 13, 20 Julio y 3, 10 de Agosto del 2013.

Horario:

De 9:00am a 12:00 (UTC -05:00)

Más Información:

http://www.slideshare.net/reydes/curso-hacking-aplicacionesweb

Correo electrónico: caballero.alonso@gmail.com
Twitter: https://twitter.com/Alonso_ReYDeS
LinkedIn: http://pe.linkedin.com/in/alonsocaballeroquezada/
Skype: ReYDeS
Sitio Web: http://www.reydes.com

Webinar Gratuito
¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Cómputo Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 4 de Julio del 2013