# Explotación a CMSs 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 Febrero del 2015

# Presentación

Alonso Eduardo Caballero Quezada es 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 Miembro de Open Web Application Security Project (OWASP).

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 e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, presentándose también constantemente en exposiciones enfocadas a, Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS

pe.linkedin.com/in/alonsocaballeroquezada/

# CMS - Content Managment System (Web)

UN CMS Web es un sistema de software el cual proporciona herramientas de autoria ,colaboración, y herramientas para sitios web diseñadas para permitir a los usuarios con bajos conocimientos en lenguajes de programación y lenguajes de marcas crear y gestionar contenidos en un sitio web con relativa facilidad. Un CMS robusto proporciona lo fundamental para la colaboración, ofreciendo a los usuarios la habilidad de gestionar documentos y resultados para la edición y participación de diversos autores.

La mayoría de sistemas utilizan un repositorio de contenido o base de datos para almacenar contenido de páginas, metadatos, y otros activos de información los cuales podrían ser necesarios para el sistema.

La capa de presentación muestra el contenido a los visitantes del sitio web basado en un conjunto de plantillas.

La administración también es típicamente realizar a través de interfaces basadas en un navegador.

* http://en.wikipedia.org/wiki/Content_management_system

# Ventajas y Desventajas de los CMS

## Ventajas

Bajo Costo
Fácil Personalización
Facilidad de Uso
Gestión del flujo de trabajo
Bueno para SEO (Search Engine Optimization)

## Desventajas

Costos de Implementación
Costo de Mantenimiento
Temas de Latencia
Combinación de Herramientas
Seguridad

* http://en.wikipedia.org/wiki/Web_content_management_system

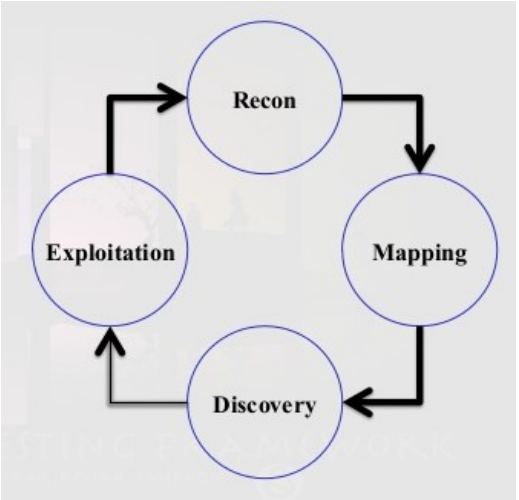
# Fase de Explotación

En este paso final el atacante toma toda la información capturada hasta este punto y la utiliza para explotar la aplicación. Esto puede implicar realizar un volcado de la base de datos, o hacer un “pivoting” para atacar el resto de la red.

La explotación es donde se lanzan los ataques. Muchos profesionales se enfocan en esta etapa en detrimento de las pruebas, pues la explotación se construye sobre toda la información recolectada y las tareas completadas hasta este punto. Sin los primeros tres pasos de la metodología descrita la explotación generalmente falla.

**Es un Ataque Cíclico**

Cuando se explota satisfactoriamente una vulnerabilidad usualmente se abren nuevos caminos, por lo tanto se inicia el proceso nuevamente, aprovechándose del nuevo acceso o información. A diferencia del atacante malicioso, el trabajo de un profesional es encontrar todas las vulnerabilidades posibles, no solamente una.



# WordPress

WordPress es un software web el cual puede ser utilizado para crear bellos sitios web o blog. El corazón del software es construido por una comunidad de cientos de voluntarios. Incluye miles de plugins y temas disponibles para transformar el sitio web en cualquier cosa imaginable.

La seguridad en Wordpress es tomada muy seriamente, pero como cualquier otro sistema existen potenciales temas de seguridad los cuales pueden surgir si no se toman las precauciones básicas de seguridad.

Como muchos paquetes modernos de software, WordPress se actualiza regularmente para solucionar nuevos temas de seguridad. Mejorar la seguridad del software es siempre una preocupación constante, y al final se debe siempre mantenerse actualizado con la versión más reciente de Wordpress. Las antiguas versiones de WordPress no son mantenidas con actualizaciones de Seguridad.

* https://wordpress.org/
* http://codex.wordpress.org/Hardening_WordPress
* https://wordpress.org/news/category/security/

# Drupal

Drupal es una plataforma open source para gestión de contenido, la cual brinda poder a millones de sitios webs y aplicación. Es construido, utilizado y apoyado por una activa y diversa comunidad de personas alrededor del mundo. Miles de módulos add-on y diseños permiten construir cualquier sitio imaginable.

Drupal proporciona consejos sobre la configuración de seguridad para los administradores del sitio e incluye las cosas a hacer y las cosas a no hacer. Se intenta exponer la información en prioridad de la configuración basado en la probabilidad de su utilidad y probable beneficio/daño de la configuración.

Se sugiere también estar subscrito a la lista de correo de seguridad de Drupal. Y las personas interesadas deben unirse también al grupo de mejores prácticas en seguridad.

* https://www.drupal.org/
* https://www.drupal.org/security
* https://www.drupal.org/security/secure-configuration
* http://groups.drupal.org/best-practices-drupal-security

# Joomla

Joomla es un sistema gestor de contenido galardonado, el cual permite construir sitios web y aplicaciones web en línea muy poderosas. Muchos aspectos, incluyendo facilidad de uso y ampliación, hacen a Joomla el software disponible para sitios web más popular. Lo mejor de todo, Joomla es una solución open source libremente disponible a cualquiera.

Joomla contiene páginas con información relevante para asegurarlo. Se debe tener en consideración lo siguiente:

Debido a la variedad y complejidad de los servidores web, los temas de seguridad no puede ser resueltos con soluciones simples o iguales.

Para asegurar un sitio web se debe ganar experiencia real, u obtener ayuda experimentada de otros.

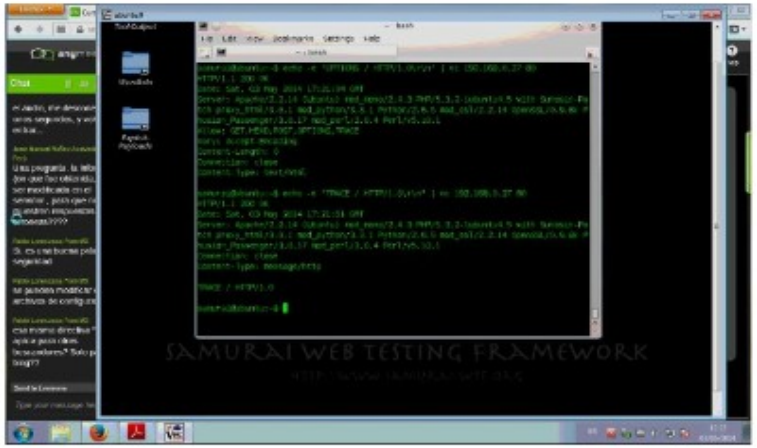
Se sugiere estar familiarizado con GNU/Linux, Apache, MySQL, PHP, HTTP y Joomla

* http://www.joomla.org/
* http://developer.joomla.org/security-centre.html
* https://docs.joomla.org/Security_Checklist

# Curso Virtual de Hacking Aplicaciones Web

## Curso Virtual de Hacking Aplicaciones Web

## 2015




**Grupo Sábado:**
7, 14, 21 y 28 de Febrero del 2015
De 3:30pm a 7:15pm (UTC -05:00)

**Grupo Domingo:**
8, 15, 22 de Febrero y 1 de Marzo 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

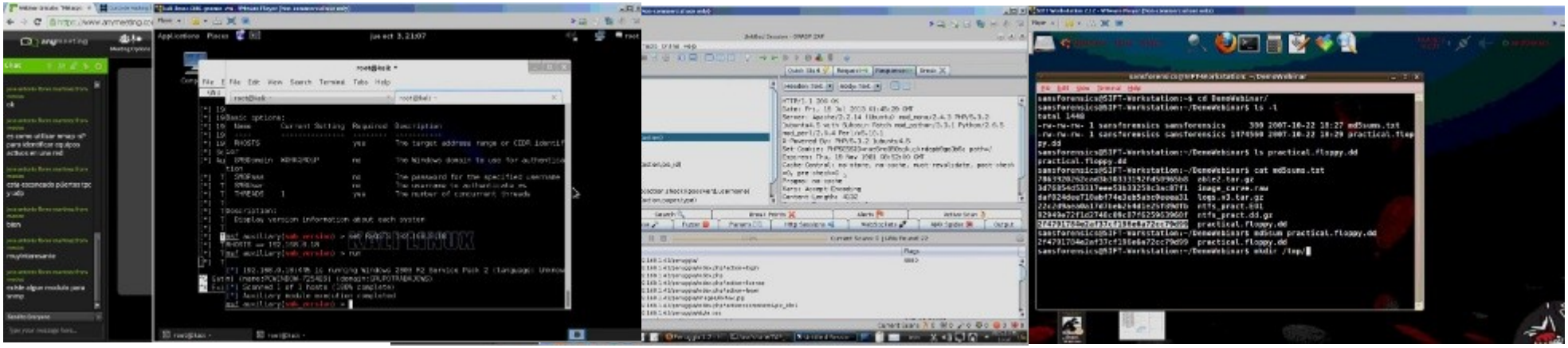
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

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 22 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

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

Diapositivas utilizadas en los Webinars Gratuitos.

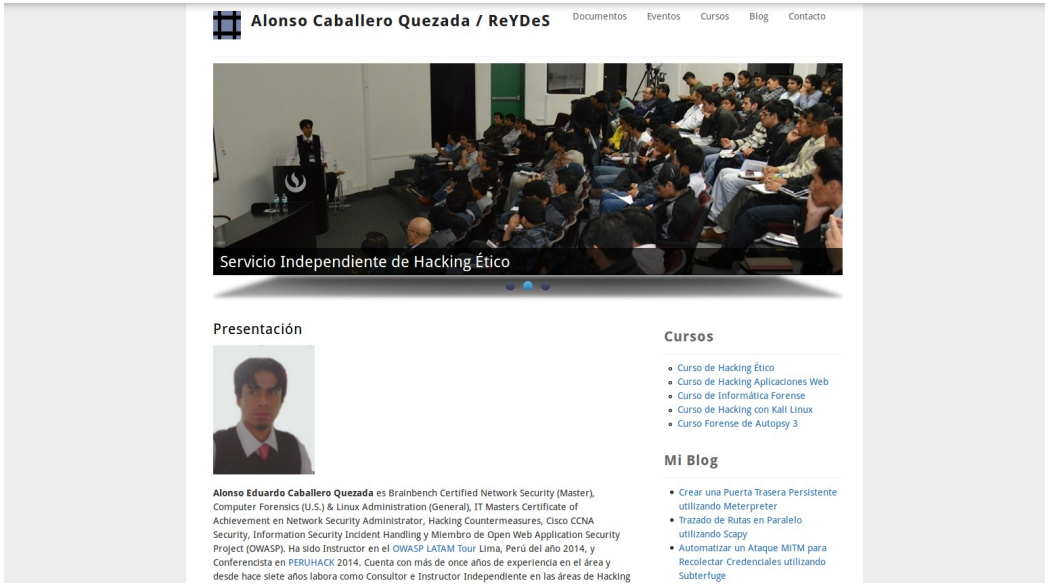
http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

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

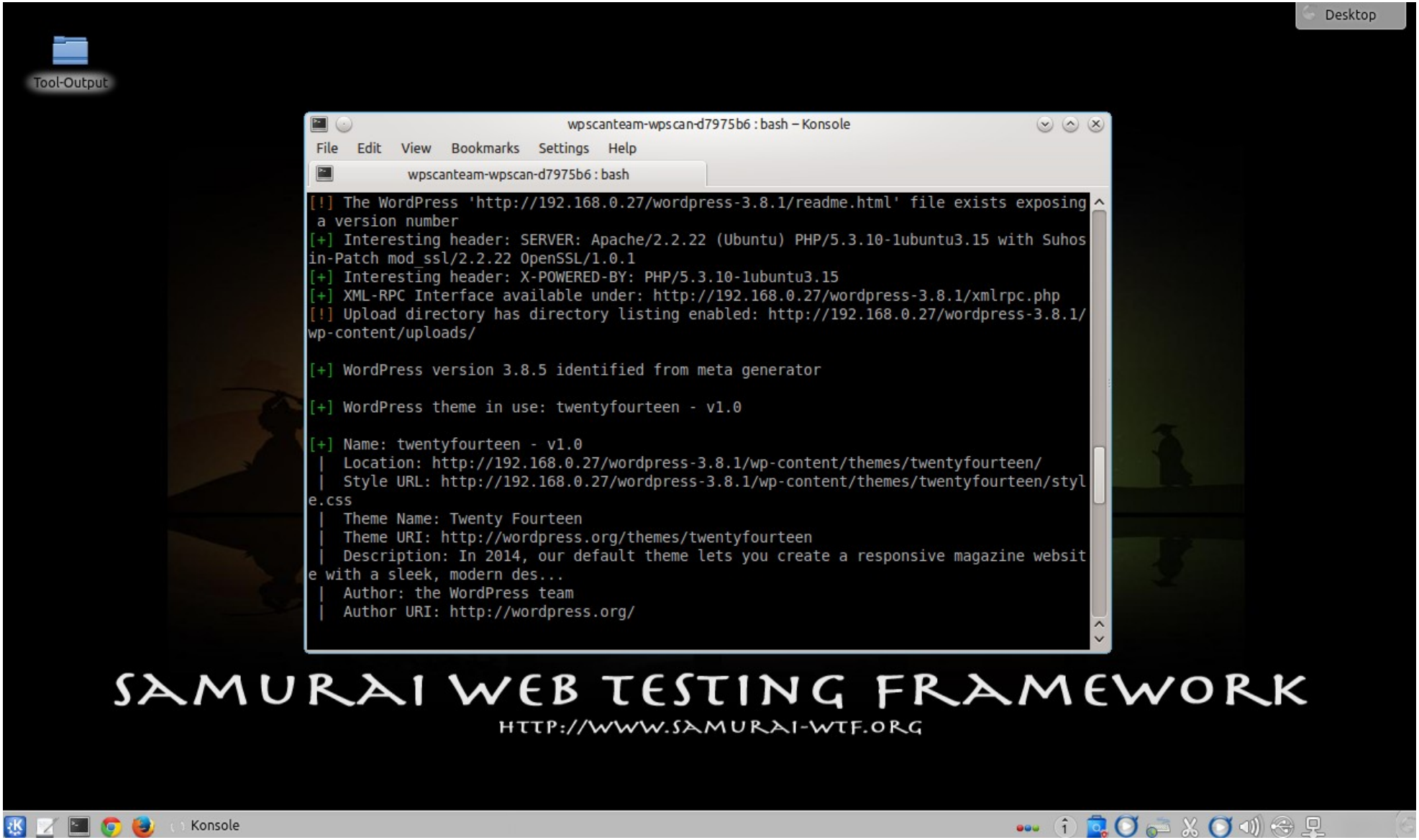
Mi Blog sobre temas de mi interés.

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



# Demostraciones

.



# Explotación a CMSs Web

## ¡Muchas Gracias!

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 Febrero del 2015