WEB PENETRATION TESTER

12 HORAS - CURSO PRESENCIAL

TPX MX SA DE CV.
Curso Presencial.
Edición 2, Año 2018.

https://tpx.mx/cursos/web-penetration-tester
cursos@tpx.mx
tpx.mx @tpx_mx tpx.mx

Actualmente las aplicaciones Web son uno de los vectores de ataque mayormente utilizados por los usuarios mal intencionados para comprometer los activos de información de las organizaciones. Desde hace algunos años grandes fugas de información se han convertido en noticias diarias.

El curso tiene como propósito entrenar a recursos humanos **en la evaluación de los controles de seguridad implementados por los equipos de desarrollo,** a fin de poder **detectar vulnerabilidades que pongan en riesgo la información relacionada a dichas aplicaciones**.

Durante el curso, el alumno, será capaz de identificar las tecnologías utilizadas por la aplicación, la lógica de negocio implementada, ejecutar un análisis a conciencia sobre la estructura de la aplicación web y probar los dominios de seguridad en la aplicación.

Para ello se hará uso una metodología aceptada de forma internacional para la revisión de aplicaciones Web, así como se aprovechará la experiencia en tecnología de cada uno de los alumnos para enfocar los conocimientos hacia la evaluación de controles.

Datos del Curso.

Duración: 12 horas

Conocimientos previos del alumno: Conocimientos sobre servidores Web, Lógica de programación, Conocimientos básicos en shell a nivel usiario.

Requisitos del alumno: Laptop, con la distribución Kali Linux más estable, esta puede ser virtualizada en el sistema operativo nativo que utiliza, .

Día 01
+ TEORICO

1. Introducción y recopilación de información

- Vista general de la web desde la perspectiva de Web Pentester
- Explorando los diferentes servidores y clientes
- Discusión de los diferentes tipos de vulnerabilidades y su medición.
- Definición de un alcance y proceso de prueba de aplicación web
- Definición y metodologías de pruebas de penetración
- Definición del uso de proxy en un pentest
- Tipos de reportes

2. Recolección de información e identidad

- Descubriendo la infraestructura dentro de la aplicación
- Identificación de las máquinas y sistemas operativos
- Métodos de aprendizaje para identificar nodos
- Descubrimiento de configuración de software
- Explorando fuentes de información externas
- definición de un spider hacia web.
- Introducción a shell scripting enfocado a auditorias web.
- Creación de secuencias de comandos para automatizar las solicitudes web y spidering.

Día 02
+ PRACTICO

3. Inyección.

- Vulnerabilidades de aplicaciones web y técnicas de verificación manual
- Proxies de intercepción (Burp Suite)
- Fuga de información y exploración de directorios
- Recolección del Usuarios.
- Inyección de comando.
- path traversal
- Inclusión de archivos locales (LFI)
- Inclusión remota de archivos (RFI)
- inyección SQL
- Inyección SQL a ciegas
- Automatización en inyecciones sql
- JavaScript para el atacante

4. JavaScript y XSS

- Vectores de ataques en XSS
- Session flaws
- Session fixation
- Comparación de XML y JSON en vectores de ataque.
- Ataques de lógica
- Herramientas de automatización de aplicaciones web.

5. CSRF and Logic Flaws

- Metasploit para Web Pentesters
- Aprovechando los ataques para obtener acceso al sistema
- Cómo pivotar nuestros ataques a través de una aplicación web
- Comprender los métodos de interacción con un servidor mediante inyección SQL
- Explotar aplicaciones para robar cookies
- Ejecutando comandos a través de vulnerabilidades de aplicaciones web
- Caminando a través de un escenario de ataque completo.

6. Examen WPT.

El temario se encuentra en constante actualización, conforme a las nuevas metodologías de hacking y ciber seguridad, por lo que tiene cambios sin previo aviso con el fin de mejorar la calidad del diplomado.

Ultima actualización: Abril 2018

TPX MX SA DE CV

Aguascalientes México.

Una empresa dedicada a la ciberseguridad e investigación científica.