ETHICAL HACKING – SEGURIDAD EN APLICACIONES WEB

Duración: 24 hrs.

Código: WETCS

Curso:

Descripción del curso

El curso de Ethical Hacking muestra técnicas para vulnerar y proteger aplicaciones:

.-Técnicas básicas y avanzas de INYECCIONES sobre aplicaciones web.
.-Gestión y ruptura de sesiones (Session Management).
.-Ataques del tipo Cross Site Scripting (XSS).
.-Malas configuraciones del servidor.

Objetivos:

El Participante al finalizar el curso será capaz de:

Aplicar los conocimientos y técnicas de seguridad informática para vulnerar y proteger aplicaciones web. Las técnicas se encuentran relacionadas a la metodología OTP (OWASP Testing Project).

Dirigido a:

- Publico en General.

REQUISITOS MÍNIMOS

Conocimiento básico del sistema Operativo Microsoft Windows.
Conocimiento básico de algoritmos y estructura de datos.

CONTENIDO

Sesión 1

- Introducción al desarrollo seguro de aplicaciones web.
- Introducción a OTP (OWASP Testing Project).
- Inyecciones de código SQL.
  - Concepto de inyecciones y malas prácticas de desarrollo.
  - Tipos de inyecciones.
    - .- Inyecciones basadas en UNIONES.
    - .- Inyecciones a ciegas (BLIND).
      - ° Inyecciones Booleanas.
      - ° Inyecciones basadas en Tiempo.
  - Técnicas avanzadas de explotación.
    - .- Upload de SHELLCODE y PAYLOAD.
    - .- Extracción de Memoria RAM.
    - .- Elevación de privilegios.
- CTF 01: Desarrollo de ejercicio práctico.

Sesión 2

- Gestión y ruptura de autenticación.
  - Definición del proceso de sesiones.
  - Conceptos de COOKIEs y TOKENs.
  - Secuestro de Sesiones (Session Hijacking).
  - Identificación de Sesiones mal cerradas.
  - Ataques sobre formularios de acceso.
    - .- Ataques del tipo SNIPPER.
    - .- Ataques del tipo BATTERING RAM.
    - .- CLUSTER BOMB.
  - Identificación de inadecuada gestión de privilegios.
- Herramienta: BURPSUITE.
- Cross Site Scripting (XSS).
- Definición de los ataques del lado del cliente.
- Introducción al JAVASCRIPT.
- Tipos de Cross Site Scripting.
  - XSS Reflejado.
  - XSS Persistente.
  - XSS DOM.

CONTENIDO

Sesión 3

- Cross Site Scripting (XSS).
  - -Técnicas avanzadas de explotación.
    - .-Mapeo de computadores con JAVASCRIPT.
    - .-Robo de sesiones con JAVASCRIPT.
    - .-Ejecutables para obtener sesión remota con Metasploit.
  - -CTF 02: Desarrollo de ejercicio práctico.
- Manejo inadecuado de Carga de archivos.
  - -Concepto de la carga de archivos a través de formularios web.
  - -Manipulación de la extensión del archivo.
  - -Manipulación del tipo de archivo.
  - -Creación de imágenes con BACKDOORS y PAYLOADs.

Sesión 4

- Remote/Local File Inclusion.
  - - Concepto de la ejecución de código a través de RFI y LFI.
  - - Identificación de la vulnerabilidad.
  - - Obtención y lectura de archivos del sistema operativo.
  - - Ejecución de código REMOTO.
- CTF 03: Desarrollo de ejercicio práctico.
- Examen FINAL.

EVALUACIÓN

La evaluación de cursos será totalmente práctica. Se realizarán entre 4 y 5 prácticas de las cuales se eliminará la nota más baja y se obtendrá un promedio (PP). Durante la última sesión se realizará un examen final (EF), el cual se promediará con la nota de prácticas y de esta manera se tendrá la calificación final.

PROMEDIO DE PRACTICAS

$$PP=\frac{(PR1 + Pr2 + Pr3 + PR4) - Menor\ (PR)}{3}$$

Nota Final:

$$NF = (PP + EF) / 2$$