CURSO

WEB HACKING

Plan de estudio

educación IT

Nuestro propósito

Transformar positivamente la vida de las personas.

Queremos que seas protagonista en la transformación que estamos viviendo. Por eso, nos comprometemos a capacitarte para que estés al día con las necesidades digitales actuales.

Te invitamos a trabajar en conjunto para que descubras tu mejor versión y la potencies. Anímate, toma las riendas de tu futuro.

Code your future!

Contenido del curso

Aprende las técnicas más utilizadas por los hackers para vulnerar aplicaciones web. Entiende cómo analizar la seguridad en empresas realizando ataques.

Prácticas en clase

Durante el curso trabajarás con múltiples laboratorios y CTFs (Capture The Flag) orientados a vulnerabilidades reales en aplicaciones web.

- Explorarás distintas superficies de ataque mediante el análisis y manipulación de peticiones HTTP/HTTPS con herramientas como Burp Suite Community Edition, Gobuster, SQLMap y Wfuzz.
- Enumerarás recursos ocultos, detectarás tecnologías con WhatWeb y analizarás configuraciones inseguras en aplicaciones modernas.
- Simularás ataques clásicos como XSS, SQLi, CSRF, LFI y RCE, mediante payloads personalizados, fuzzing manual, automatización con Nuclei y explotación avanzada con Metasploit.
- Atacarás entornos WordPress con WPScan, descubrirás vulnerabilidades en plugins y realizarás pruebas de fuerza bruta con Hydra.
- Pondrás a prueba tus habilidades en entornos controlados que replican fallos reales del OWASP Top 10 (2021), aplicando técnicas de evasión, manipulación de sesiones, robo de cookies, y uso de frameworks como BeEF.
- Generarás reportes técnicos de los hallazgos y recomendarás medidas defensivas.

¿Qué aprenderás?

- Uso experto de Burp Suite.
- Manipulación de peticiones HTTP/HTTPS.
- Detección de tecnologías web con WhatWeb.
- Explotación de sitios WordPress con WPScan.
- Utilización de Gobuster y Wfuzz.
- Explotación de vulnerabilidades críticas.
- Scripting con bash y python.
- Control de navegadores web con BeEF.
- Automatización de pruebas con Nuclei.
- Escaneo con Nikto y Nmap.
- Fuerza bruta y cracking de contraseñas.
- Explotación avanzada: Metasploit Framework.

Plan de estudios

1 Fundamentos de seguridad web

- Conceptos Clave: HTTP, HTTPS y Cifrado TLS.
- Cabeceras HTTP y políticas de seguridad.
- Identificación de tecnologías web.
- Uso de WhatWeb y Wappalyzer.
- Análisis de frameworks, servidores y CMS.
- Reconocimiento activo y pasivo.
- Enumeración: directorios y archivos ocultos.
- Utilización de Gobuster y Wfuzz.
- Dirsearch para enumerar archivos ocultos
- Detección de tecnologías y configuraciones.
- Uso de WhatWeb y Nmap.
- Descubrimiento de rutas ocultas.
- Enumeración de rutas sensibles.
- Descubrimiento de vulnerabilidades.
- Introducción a OWASP Top 10 (2023).
- Escaneo básico con Nikto y Nmap..
- Detección de servicios y puertos con Nmap.
- Uso de scripts NSE.

2 Ataques clásicos en aplicaciones web

- Cross-site scripting (xss).
- Reflejado, Persistente y Basado en DOM.
- Bypassing de filtros y payloads avanzados.
- Control de navegadores web con BeEF.

- SQL Injection (SQLi).
- Inyecciones básicas y avanzadas.
- Blind SQLi.
- Automatización de SQLi con SQLMap.
- Command Injection.
- Explotación de comandos del sistema.
- File Inclusion (LFI y RFI).
- Manipulación de rutas.
- Exploración de archivos.
- Archivos maliciosos: inclusión remota/local.
- Cross-Site Request Forgery (CSRF).
- Comprender y explotar CSRF.
- Métodos modernos de mitigación.

3 Burp Suite (Manual Exploitation)

- Introducción a Burp Suite.
- Instalación de Burp Suite Community Edition.
- Configuración de Community Edition.
- Proxy y Certificado SSL para HTTPS.
- Interfaz de usuario y configuración.
- Tabs principales.
- Proxy, Target, Repeater,
- Intruder, Decoder, Comparer.
- Intercepción de peticiones.
- Manipulación de peticiones HTTP/HTTPS.
- Modificación: headers, métodos y parámetros.
- Análisis manual de vulnerabilidades.
- Repetición de peticiones con Repeater.

- Fuzzing Manual de parámetros con Intruder.
- Técnicas avanzadas con Burp Suite Community.
- Gestión de cookies para robo de sesiones.
- Modificación de Parámetros GET y POST.
- Uso de extensiones (BApp Store).
- Instalación manual de extensiones.
- Active Scan, Logger++, Autorize.

4 Análisis y explotación de apps web modernas

- Detección de vulnerabilidades avanzadas.
- Enumeración de subdominios con Subfinder.
- Verificación de hosts con httpx.
- Server-Side Request Forgery (SSRF).
- Deserialización insegura.
- Path Traversal y Directory Listing.
- Ataques a plataformas específicas.
- Manipulación de tokens JWT.
- Escaneo y Explotación: WordPress con WPScan.
- Detección de plugins y temas vulnerables con WPScan.
- Escaneo con Nuclei.
- Explotación automatizada con Metasploit.
- Scripting de reconocimiento y ataque.
- Scripting con bash o Python.
- IA para Automatización
- Desarrollo de Payloads personalizados.
- Construcción de Payloads XSS, SQLi, y RCE.

5 Protección de aplicaciones web

- Configuración segura de servidores web.
- Implementación de HTTP Security Headers.
- ModSecurity y WAFs Modernos.
- ModSecurity en Apache y Nginx.
- Protección de aplicaciones WordPress.
- Configuración segura de WordPress.
- Hardening de WordPress con WPScan.
- Protección de cookies y sesiones.
- Atributos Secure, HttpOnly y SameSite.
- Validaciones servidor y cliente.
- Aplicación de OWASP Top 10 (2021).
- Creación de reportes técnicos y ejecutivos.
- OSWA-WEB-200: Web Attacks with Kali Linux.
- Web Application Penetration Tester.
- Extreme Web Application Penetration Tester.
- Burp Suite Certified Practitioner.
- HTB Certified Web Exploitation Specialist.

Modalidad del Curso

Duración
4 semanas / 15 h

Frecuencia semanal
2 encuentros de 2 h

Modalidad
Online en vivo

Grupos reducidos
Promedio 15 personas

Nivel: Intermedio

- [ ] Principiante
- [x] Intermedio
- [ ] Avanzado
- [ ] Experto

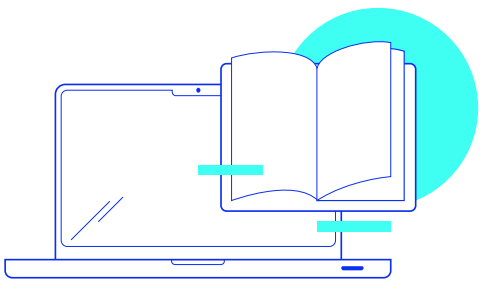
Requisitos

Es recomendable tener una base sobre:

- **Introducción a la Ciberseguridad**
- **Introducción a Bases de Datos y SQL**

Dedicación fuera de clase

Además de las horas de clase, recomendamos que inviertas 4 h semanales extras para realizar los desafíos complementarios, estudiar el material de lectura y completar los exámenes del Alumni.



¿Cómo será tu experiencia?

Aprender haciendo

Ejercita y pon en práctica lo estudiado.

Trabajo en equipo

Une esfuerzos y potencia los resultados.

Clases grabadas

Consúltalas las veces que quieras.

Profesores expertos

Aprende de gigantes de la industria.

Asistente académico

Recibe soporte dentro y fuera de clase.

Plataforma Alumni

Encuentra recursos, materiales y clases.

¿Por qué Educación IT?

IT Créditos

Gana puntos al aprobar los exámenes de los cursos. Luego, podrás canjearlos por nuevos cursos sin costo alguno. Los IT Créditos que acumules no vencen ni se devalúan.

Garantía de aprendizaje

Si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, ¡vuelve a tomar el curso sin ningún costo! Puede ser de forma total o parcial.

Comunidad en Discord

Mantente en contacto con la comunidad de EducaciónIT a través de nuestro servidor de Discord. Podrás hablar con tus compañeros, profesores, asistentes académicos y soporte.

Preguntas frecuentes

Si me pierdo una o más clases, ¿puedo recuperarlas?

Todas las clases quedan grabadas de por vida en tu plataforma Alumni. ¡Siempre podrás volver a verlas cada vez que lo necesites!

¿Cómo voy a aprender?

Te enfrentarás a situaciones de trabajo reales, en donde tendrás que aplicar lo aprendido de forma individual y en equipo. Por medio de la prueba y el error, irás superando desafíos y obteniendo nuevas habilidades que luego podrás aplicar en el ámbito laboral.

¿Cómo son las clases online en vivo?

Las clases duran entre 2 y 3 horas de lunes a viernes (sábados 3 o 4 hs) y se desarrollan de forma online en vivo en aulas virtuales, donde vas a poder interactuar con el instructor y tus compañeros. Manejamos cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.

educación IT

Plan de estudio

Code your future

www.educacionit.com

@educacionit