CURSO

SEGURIDAD WEB: SQL INJECTION & XSS

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 las clases realizaremos ataques sobre sitios web de práctica, que nos permitirán entrar en contacto directo con las técnicas, herramientas y comportamientos de las aplicaciones web existentes. Realizaremos ataques para saltar procesos de autenticación, inyectar información dentro de bases de datos, capturar datos de usuarios y más.

¿Qué aprenderás?

- Fundamentos HTTP y ZAP Proxy
- Detectar qué tecnologías utiliza una aplicación Web
- Modificar las peticiones y respuestas HTTP
- Cross Site Scripting
- Utilización de Cookies para la seguridad de una App
- Detectar vulnerabilidades con XSS, CSRF y SQL Injection
- SQL/Command Injections
- Utilizar Zed Attack Proxy y Vega
- Inclusiones, Shells, Sesiones y Validaciones Client-Side
- Control de un navegador web a través de BeEF
- Crear archivos remotos en servidores vulnerables
- Protecciones con Apache + ModSecurity

Plan de estudios

1 HTTP y ZAP Proxy

- HTTP
- Instalación de DVWA sobre Kali Linux
- Acceso desde Ncat
- Análisis de las Cabeceras HTTP
- Obtener métodos con el verbo OPTIONS
- ZAP - Peticiones y Respuestas
- Zap - Configuración del Proxy
- Zap - Configuración del Scope
- Zap - Análisis de Peticiones y Respuestas
- Zap - Modificar Peticiones al Vuelo
- ZAP - Escaneo Pasivo
- Zap - Configuración de Escaneo Pasivo
- Zap - Spidering
- Zap - Descubrir Directorios Ocultos
- Zap - Fuzzing de Peticiones Web
- ZAP - Plugins y Escaneo Activo
- Zap - Reenviar peticiones
- Zap - Instalación de Plugins
- Zap - Configuración de Escaneo Activo
- Zap - Lanzamiento de Escaneos Activos

2 Cross Site Scripting

- XSS - Introducción
- XSS Reflejado

- Análisis de código
- Nivel Medio
- Nivel Alto
- Nivel Imposible
- XSS - Otras variantes
- XSS Persistente
- XSS Basado en DOM
- Detección a través de Fuzzing
- VLab
- XSS Payloads
- XSS DoS
- Robo de Cookies
- Keylogger
- VLab - Redirección
- BeEF - Browser Exploitation Framework
- BeEF enganche
- BeEF - GetCookie y GetFormValues
- BeEF - Redirect Browser
- BeEF - Detect Virtual Machine
- XSS Payloads
- XSS Persistente
- XSS Persistente
- XSS DoS
- XSS Con Redirect
- Via HTTP Headers
- Robo de Cookies
- XSS Alert con Cookies
- Robo de Cookies a través de json request
- Atributo httponly para evitar el robo

- Robo de Cookies via img o algún otro request

3 SQL/Command Injections

- SQLi Básico
- Análisis de código nivel Low
- Generación de Errores
- SQLi Payloads
- Mostrar nombre de base de datos, versión y usuario
- Mostrar todas las tablas de la base
- Mostrar todas las columnas
- Mostrar todos los datos de las columnas
- SQLi
- Command Injection
- Inyección básica de comandos
- Crear archivos en el sistema
- Crear una conexión shell con NetCat
- Identificar la password de la base de datos

4 Inclusiones, Shells, Sesiones y Validaciones Client-Side

- File Inclusions
- Local File Inclusion
- Remote File Inclusion
- Shells PHP
- Creación de una shell en PHP
- Subir a través de File Upload
- Remote Hell - Análisis de Código
- Utilización de Remote Hell
- Cookies de Sesión

- El atributo secure
- El atributo httponly
- Cambio de contenido
- Enumerar los usuarios del sistema
- Validaciones Client-Side
- Saltar Restricciones de Longitud en Formularios
- Saltar validaciones JavaScript
- Enviar un XSS con el nivel de seguridad

5 Protecciones con Apache + ModSecurity

- Configuración Segura de Apache
- X-Frame Options
- X-Content-Type-Options
- Content Security Policy
- Cookies
- HTTPS Strict Transport Security
- Public-Key-Pins
- Mod Security - Instalación
- Instalación de ModSecurity y el CRS
- Habilitar ModSecurity en Modo Detection Only
- Navegar la aplicación y mirar los logs de ModSecurity
- Lab: Habilitar en On y probar
- Mod Security - Configuración
- XSS vs ModSecurity
- SQLi vs ModSecurity
- PHPInfo vs ModSecurity
- Lab: LFI vs ModSecurity
- Mod Security - Reglas Personalizadas

- Found User-Agent associated with security scanner
- Content-Length HTTP header is not numeric.
- Directory Listing
- Describir el comportamiento de una regla

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

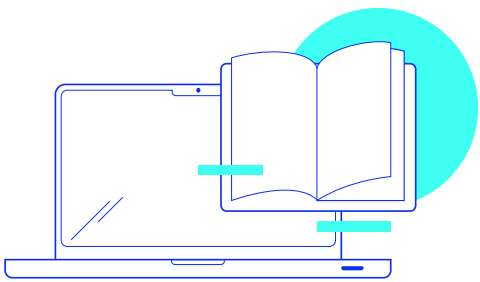
Te aconsejamos tener un dominio sobre:

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.

Career Advisor

Ingresa al mundo laboral junto a nuestros asesores de carrera: crea un CV que impacte, arma y comparte tu portfolio en LinkedIn y Behance y ten simulacros de entrevistas.

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