CYBERIUM ARENA

Descripción

Sumérgete en la arquitectura fundamental de las aplicaciones web, las mejores prácticas de seguridad y protocolos web avanzados. Avanza en las complejidades de los lenguajes web, enfatizando los aspectos de seguridad de JavaScript, creación de bases de datos y técnicas de inyección SQL. Mejora tu experiencia en identificar vulnerabilidades, dominando herramientas como Burpsuite y explorando técnicas avanzadas de XSS. Concluye con pruebas de penetración prácticas, desde la escalada de privilegios hasta la seguridad de aplicaciones de WordPress.

ZX311 - SEGURIDAD DE APLICACIONES WEB

Módulo 1: Introducción a la Aplicación Web

Sumérgete en el núcleo de la seguridad de las aplicaciones web, comenzando con conceptos y arquitectura fundamentales de WebApp. Domina las complejidades de las interacciones cliente-servidor, mejora la seguridad mediante técnicas de fingerprinting y fortalece las interfaces de administración. Profundiza en las mejores prácticas de desarrollo web, desde características de seguridad de HTML5 hasta directrices de PHP, y comprende las sutilezas de los códigos de respuesta HTTP avanzados.

Conceptos de WebApp

Arquitectura de Aplicaciones Web
Cliente, Servidor y Base de Datos
Técnicas de Fingerprinting y Reconocimiento
Seguridad de la Interfaz de Administración
Fortalecimiento de la Interfaz de Administración
Manipulación de Parámetros
Implementación y Auditoría de la Encriptación HTTPS

Fundamentos de WebApp

Características y Seguridad de HTML5
Mejores Prácticas de Seguridad de PHP
Códigos de Respuesta HTTP/2 & HTTP/3

Módulo 2: Lenguajes Web

Domina los aspectos de seguridad del desarrollo web, enfocándote en el papel de JavaScript para profesionales. Entiende la manipulación dinámica de HTML, el secuestro de formularios y las amenazas modernas de ingeniería social, técnicas de análisis de datos a través de HTML, JSON y XML, y profundiza en bases de datos SQL, desde su creación hasta técnicas avanzadas de explotación de inyección.

JavaScript para Profesionales de Seguridad

Manipulación Dinámica de HTML
Secuestro de Formularios
Ingeniería Social: Amenazas Modernas y Defensas
Técnicas de Análisis de HTML, JSON y XML
Creación de Bases de Datos SQL
Entendiendo la Inyección SQL
Explotando la Inyección SQL
Explotando la Inyección SQL Ciega

Módulo 3: Vulnerabilidades Web

Profundiza tu experiencia en seguridad web con herramientas como Burpsuite, avanzando hasta dominar su versión Pro y extensiones. Aprende defensas contra ataques de fuerza bruta, mitigación de inyección de comandos y métodos sofisticados de enumeración de usuarios. Sumérgete en técnicas de inclusión de archivos, tanto locales como remotas, y mejora tus habilidades en XSS, explorando sus estrategias avanzadas de explotación.

Trabajando con Burpsuite

Dominando Burpsuite Pro y Extensiones
Técnicas y Defensas de Fuerza Bruta
Explotación de Inyección de Comandos
Enumeración Avanzada de Usuarios
Inclusión de Archivos Locales y Remotos
Trabajando con XSS
Técnicas Avanzadas de XSS

Módulo 4: Penetración de WebApp

Emprende una exploración comprensiva de ataques a aplicaciones web. Profundiza en técnicas de escalada de privilegios, explotación de traversal de directorios y las complejidades de Inclusión de Archivos Local y Remota (LFI & RFI). Domina técnicas avanzadas desde inclusión de archivos hasta tácticas de shell reverso, estrategias manuales de inyección SQL y vulnerabilidades de cadena de formato. Concluye con pruebas de seguridad prácticas de aplicaciones WordPress.

Ataques en Profundidad

Técnicas de Escalada de Privilegios
Explotación de Traversal de Directorios
Inmersión Profunda en LFI & RFI
Mecanismos de Carga y Evasión
Inclusión de Archivos a Shell Reverso
Técnicas Manuales de Inyección SQL
Vulnerabilidades de Cadena de Formato
Pruebas de Aplicaciones

ZX Ofensiva | NIVEL: 6 | DURACIÓN: 40h