CYBERIUM ARENA

Description

Dive into foundational WebApp architecture, security best practices, and advanced web protocols. Progress into the intricacies of web languages, emphasizing the security aspects of JavaScript, database creation, and SQL injection techniques. Enhance your expertise in identifying vulnerabilities, mastering tools like Burpsuite, and exploring advanced XSS techniques. Conclude with hands-on penetration testing, from privilege escalation to WordPress application security.

WEBAPP SECURITY

Module 1: Introduction to Web App

Dive into the core of web application security, starting with foundational WebApp concepts and architecture. Master the intricacies of client-server interactions, enhance security through fingerprinting techniques, and fortify admin interfaces. Delve deeper into web development best practices, from HTML5 security features to PHP guidelines, and understand the nuances of advanced HTTP response codes.

WebApp Concepts
Web Application Architecture
Client, Server, and Database
Fingerprinting & Reconnaissance Techniques
Securing the Admin Interface
Hardening the Admin Interface
Parameter Tampering
Implementing & Auditing HTTPS Encryption

WebApp Basics
HTML5 Features & Security
PHP Security Best Practices
HTTP/2 & HTTP/3 Response Codes

Module 2: Web Languages

Master the security aspects of web development, focusing on JavaScript's role for professionals. Understand dynamic HTML manipulation, form hijacking, and modern social engineering threats, data parsing techniques across HTML, JSON, and XML, and delve deep into SQL databases, from creation to advanced injection exploitation techniques.

JavaScript for Security Professionals
Dynamic HTML Manipulation
Form Hijacking
Social Engineering: Modern Threats & Defenses
HTML, JSON, and XML Parsing Techniques
Creating SQL Databases
Understanding SQL Injection
Exploiting SQL Injection
Exploiting Blind SQL Injection

Module 3: Web Vulnerabilities

Deepen your expertise in web security with tools like Burpsuite, advancing to mastery with its Pro version and extensions. Grasp brute force defenses, command injection mitigation, and sophisticated user enumeration methods. Dive into file inclusion techniques, both local and remote, and enhance your skills in XSS, exploring its advanced exploitation strategies.

Working with Burpsuite
Mastering Burpsuite Pro & Extensions
Brute Force Techniques & Defenses
Command Injection Exploitation
Advanced User Enumeration
Local & Remote File Inclusion
Working with XSS
Advanced XSS Techniques

Module 4: WebApp Penetration

Embark on a comprehensive exploration of web application attacks. Delve deep into privilege escalation, directory traversal exploitation, and the intricacies of Local and Remote File Inclusion (LFI & RFI). Master advanced techniques from file inclusion to reverse shell tactics, manual SQL injection strategies, and format string vulnerabilities. Conclude with hands-on WordPress application security testing.

Attacks In-Depth
Privilege Escalation Techniques
Exploiting Directory Traversal
Deep Dive into LFI & RFI
Upload Mechanisms & Bypass
File Inclusion to Reverse Shell
Manual SQL Injection Techniques
Format String Vulnerabilities
WordPress Application Testing

ZX Offense | LEVEL: 6 | DURATION: 40h