OffSec

WEB-200 OSWA

Web Attacks with Kali Linux

The WEB-200 course provides a comprehensive overview of web application vulnerabilities and their exploitation using tools available in Kali Linux. The purpose of this course is to explore the fundamental concepts needed to begin a much longer journey within Information Security, Penetration Testing, or Application Security. Web applications often represent the largest attack surface for an organization - anyone with a browser and internet access can discover and interact with a public-facing web application. By mastering the skills and techniques within this course, you will be prepared to identify and exploit vulnerabilities in web applications.

Tools for the Web Assessor	Gain hands-on experience with industry-standard tools used by web application penetration testers
Cross-Site Scripting (XSS) Introduction, Discovery, Exploitation and Case Study	Learn how attackers inject malicious code into web pages to hijack user sessions, steal sensitive data, or deface websites
Cross-Site Request Forgery (CSRF)	Discover how attackers trick authenticated users in web applications and learn how you can identify and exploit CSRF vulnerabilities
Exploiting CORS Misconfigurations	Understand how to identify and fix CORS misconfigurations to keep your web applications safe
Database Enumeration	Discover the techniques that attackers use to steal sensitive information related to a web application's database structure and how to stop them
SQL Injection (SQLi)	Exploit vulnerabilities in web applications through SQL injections and learn techniques to prevent and mitigate SQL injection attacks
Directory Traversal	Learn how to identify and exploit directory traversal vulnerabilities and how you can prevent attackers from accessing restricted areas in your web servers
XML External Entities	Learn how attackers user manipulate XML processors to exploit input vulnerabilities, how to secure your XML parsers, and to prevent XXE vulnerabilities in your web applications
Sever-Side Template Injections (SSTI)	Learn how to identify and exploit SSTI vulnerabilities and how you can protect your web applications from server-side template injections
Server-Side Request Forgery (SSRF)	Understand different SSRF attack vectors and how to implement countermeasures against them

Command Injection	Learn how attackers take advantage of command injection vulnerabilities and the potential impact on your system's integrity. Practice identifying, exploiting, and mitigating command injection vulnerabilities
Insecure Direct Object Referencing	Learn how to handle object references in a secure manner to prevent attackers from accessing private data or performing unauthorized actions
Assembling the Pieces: Web Application Assessment Breakdown	Combine and expand different web application attack and assessment techniques you've learned throughout the course