Training: OffSec
OffSec WEB-200 Web Attacks with Kali Linux

OffSec Learning Partner

TRAINING GOALS:



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.

WEB-200 has topics and examples covering a large number of web application skills, including:

- Leveraging various types of Cross-Site Scripting (XSS) vulnerabilities using our Kali Linux environment
- Performing web application reconnaissance, enumerating web applications, and sourcing or generating wordlists
- Using fuzzing tools for SQL Injection vulnerabilities and sqlmap for automated site crawls, but also when a manual approach is preferred
- Mastering Burp Suite tools: Repeater, Comparer, Intruder, and Decoder, to be effective web assessors
- Understanding the impact of Server-side Request Forgery (SSRF) including how the vulnerability occurs, and how it interacts with the vulnerable server through a case study with two SSRF vulnerabilities found in a real-world application.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

WEB-200 is organized into 16 modules, each with detailed explanations, specific case studies, and hands-on activities to emphasize the discovery, testing, and exploitation of these vulnerabilities to enhance offensive security skills. After the completion of the modules, learners will be able to test their knowledge on any one of 9 Challenge labs. Once prepared, the learner can sit for the OffSec Web Assessor (OSWA) certification, earning the right to share this accomplishment with employers.

Each participant in an authorized OffSec WEB-200 training held at Compendium CE receives a Learn One" license, which includes, among other benefits, a free OSWA exam voucher.

WEB-200 is designed for learners who want to build foundational skills in professional web application assessments. The course material will help clarify the attacks and techniques used by malicious actors against web applications. Note that basic Linux, networking, and scripting skills will help significantly with this course.

Objectives

After completing this course, learners will be able to:

- Understand and discover various types of Cross-Site Scripting (XSS) vulnerabilities
- Exploit XSS vulnerabilities by injecting and executing malicious scripts
- Comprehend and identify SQL Injection points and exploit them to manipulate database queries
- Utilize fuzzing tools to discover SQL Injection vulnerabilities
- Learn the Same-Origin Policy and how it interacts with cross-origin requests
- Test and exploit Cross-Origin Resource Sharing (CORS) vulnerabilities
- Identify and exploit Cross-Site Request Forgery (CSRF) vulnerabilities
- Use tools like Burp Suite, Nmap, and Gobuster for web application testing
- Perform file, directory, and parameter discovery using tools like Wfuzz and Hakrawler
- Apply offensive JavaScript techniques for web application exploitation

Who is this course for?

- Job roles like: Web Penetration Testers, Pentesters, Web Application Developers, Application Security Analysts, Application Security Architects, and SOC Analysts and other blue team members
- Anyone interested in expanding their understanding of Web Application Attacks, and/or Infra Pentesters looking to broaden their skill sets and Web App expertise

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CONSPECT:

- 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
- Server-Side Template Injection (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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Assembling the Pieces: Web Application Assessment Breakdown
  - Combine and expand different web application attack and assessment techniques you've learned throughout the course

REQUIREMENTS:

All learners are required to have completed or have the equivalent knowledge corresponding to OffSec SEC-100 CyberCore - Security Essentials course.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

The WEB-200 course and online lab prepares you for the OSWA OffSec Web Assessor certification. Learn more about the OSWA exam https://help.offsec.com/hc/en-us/articles/7281947451284-OSWA-Exam-FAQ

Each participant in an authorized OffSec WEB-200 training held at Compendium CE receives a Learn One" license, which includes, among other benefits, a free OSWA exam voucher.

TRAINER:

Authorized OffSec Trainer

ADDITIONAL INFORMATION:

The course includes a license "Learn One"

The license includes:

- One 200 or 300-level course
- 365 days of access
- 2 exam attempts
- Bonus KLCP and OSWP courses + exams
- 200+ Proving Grounds Practice labs

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007