RANGEFORCE

OWASP
The Open Web Application Security Project

RANGEFORCE TRAINING MODULE COVERAGE FOR OWASP'S TOP 10 List

The Open Web Application Security Project (OWASP) provides an ongoing list of the Top 10 security flaws that have enabled many successful cyberattacks over the past few years. The list is a great starting place for setting your cybersecurity training agenda in 2020, not only for your security team, but also for your web application developers and DevOps teams. Here is the current OWASP top 10 list.

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

To help you create that training plan, we have mapped our RangeForce Training Modules to OWAP's Top Ten List. As you would expect, of the three RangeForce training tracks, Web Application Security (WASE), Security Operations (SOC), and DevOps, the majority of training falls under web application security, with a few falling under security operations. We offer coverage to 90% of OWASP's 2019 Top 10 List. Here is our coverage:

Injection

- Wase - Blind Command Injection: Find & Exploit (NodeJS)
- Wase - Blind Command Injection: Fix (NodeJS)
- Wase - Blind NoSQL Injection: Find & Exploit (Meteor)
- Wase - Blind SQL Injection: Find & Exploit (PHP)
- Wase - Command Injection: Find & Exploit (PHP)
- Wase - Command Injection: Fix (PHP)
- Wase - NoSQL Injection 1: Exploit
- Wase - NoSQL Injection 1: Find
- Wase - NoSQL Injection 1: Fix
- Wase - NoSQL Injection 2: Exploit
- Wase - NoSQL Injection 2: Fix
- Wase - SQL Injection: Authentication Bypass
- Wase - SQL Injection: Prelude
- Wase - SQL Injection: Union Select

XML External Entities

- Wase - XML External Entity (Java)

Security Misconfiguration

- Currently no direct coverage

Broken Authentication

- Wase - Cookie Security: HttpOnly: Find & Exploit (NodeJS)
- Wase - Cookie Security: HttpOnly: Find & Exploit (PHP)
- Wase - Cookie Security: HttpOnly: Fix (NodeJS)
- Wase - Cookie Security: HttpOnly: Fix (PHP)
- Wase - Cookie Security: Secure: Find & Exploit (NodeJS)
- Wase - Cookie Security: Secure: Find & Exploit (PHP)
- Wase - Cookie Security: Secure: Fix (NodeJS)
- Wase - Cookie Security: Secure: Fix (PHP)

Sensitive Data Exposure

- Wase - Unrestricted File Upload: Find & Exploit (NodeJS)
- Wase - Unrestricted File Upload: Fix (NodeJS)
- Wase - Cookie Security: Secure: Find & Exploit (NodeJS)
- Wase - Cookie Security: Secure: Find & Exploit (PHP)
- Wase - Cookie Security: Secure: Fix (NodeJS)
- Wase - Cookie Security: Secure: Fix (PHP)

RANGEFORCE TRAINING MODULE COVERAGE FOR OWASP'S TOP 10 List

RangeForce constantly adds new modules and we will update this mapping every quarter. Please check with your RangeForce account representative to make sure you have the most up-to-date mapping. If you need support in developing your training plan, or want to test drive a few of these modules just reach out and ask.

Cross-site Scripting

- WASE - DOM-based XSS: Fix (JavaScript)
- WASE - XSS Filter Evasion: Find & Exploit (PHP)
- WASE - XSS Filter Evasion: Fix (PHP)
- WASE - XSS: Reflected
- WASE - XSS: Stored
- WASE - XSS: Stored-based Phishing

Insecure Deserialization

- WASE - Insecure Deserialization (Java)

Using Components with Known Vulnerabilities

- SOC - Docker RunC Container Escape
- SOC - Privilege Escalation: Kernel Exploit (Dirty Cow)
- SOC Challenge - Uncontained
- SOC Challenge - Webmin

Insufficient Logging and Monitoring

- Wase - XSS Filter Evasion: Find & Exploit (PHP)
- Wase - XSS Filter Evasion: Fix (PHP)
- Security Tools - Brute-force Defense
- SOC - IDS/IPS: Suricata Basics
- SOC - IDS/IPS: Suricata IDS Rules
- SOC - IDS/IPS: Suricata Rule Management

Broken Access Control

- Wase - Insecure Direct Object Reference 2: Exploit
- Wase - Insecure Direct Object Reference 2: Fix
- Wase - Insecure Direct Object Reference: Find & Exploit (NodeJS)
- Wase - Insecure Direct Object Reference: Find & Exploit (PHP)
- Wase - Insecure Direct Object Reference: Fix (NodeJS)
- Wase - Insecure Direct Object Reference: Fix (PHP)
- Wase - Path Traversal: Find & Exploit (NodeJS)
- Wase   Path Traversal: Find & Exploit (PHP)
- Wase - Path Traversal: Fix (NodeJS)
- Wase - Path Traversal: Fix (PHP)
- Wase - JSON Web Token Security
- Wase Challenge - JWT 1
- Wase Challenge - JWT 2
- Wase Challenge - JWT 3
- Wase - API Security: Exposed Tokens
- Wase - Cookie Security: HttpOnly: Find & Exploit (NodeJS)
- Wase - Cookie Security: HttpOnly: Find & Exploit (PHP)
- Wase - Cookie Security: HttpOnly: Fix (NodeJS)
- Wase - Cookie Security: HttpOnly: Fix (PHP)
- Wase - Cookie Security: Secure: Find & Exploit (NodeJS)
- Wase - Cookie Security: Secure: Find & Exploit (PHP)
- Wase - Cookie Security: Secure: Fix (NodeJS)
- Wase - Cookie Security: Secure: Fix (PHP)

Detailed information about the OWASP TOP TEN

About OWASP

OWASP is a worldwide nonprofit organization that focuses on improving software security. The main mission of OWASP is to ensure that software security is visible, and to provide insights and tools to help improve application security globally. Open Web Application Security Project, OWASP, Global AppSec, AppSec Days, AppSec California, SnowFROC, LASCON, and the OWASP logo are trademarks of the OWASP Foundation. Copyright 2020, OWASP Foundation, Inc.