COMTECH™
Fluent in the Future

PEN300 OWASP Top 10 Exploitation Bootcamp

Course Overview

Hackers routinely exploit web applications, especially as more services move to the cloud, despite the fact companies can easily fix most vulnerabilities within web applications before releasing their code to the wild. The "Web Application Exploitation" course teaches students about the most common web vulnerabilities (OWASP Top 10) in modern web applications, why they often exist, and several methods to test for their existence.

Each module has video lecture content introducing exploitation concepts to explain why the vulnerabilities exist, and how hackers exploit them. Each module also includes an immersive hands-on lab component, in which the student has the chance to exploit each vulnerability, using the vulnerable Mutillidae framework. Finally, the course encourages students to engage in a dynamic "capstone lab" designed to test the students' ability to exploit a novel web application leveraging vulnerabilities identified in the OWASP Top 10.

Upon completion of this course, the student will understand how to identify and exploit common vulnerabilities present in modern web applications, and they will gain valuable real-world skills and abilities through a series of challenging hands-on web application exploitation exercises and scenarios.

They will understand the underlying issues enabling these vulnerabilities to exist, and the general principles for fixing them in a web application.

Objectives

- Define the top ten vulnerabilities that are common to web applications
- Analyze a simple web application to search for the presence of the top ten web vulnerabilities
- Identify techniques to mitigate the presence of the top ten web vulnerabilities

Prerequisite Knowledge

Before taking this course, students should be familiar with:

- Networking applications and protocol analysis
- SQL statements
- Knowledge of Linux command line interface

Estimated Course Length: 9 hours

comtech.com | cyberstronger.com
275 West Street, Annapolis, MD 21401

Module	Lecture	Labs	Estimated Completion Time (minutes)
0	Introduction		5
1	A1: Injection	Introduction To OWASP Top Ten: A1 - Injection	60
2	A2: Broken Authentication	Introduction To OWASP Top Ten: A2 - Broken Authentication	30
3	A3: Sensitive Data Exposure	Introduction To OWASP Top Ten: A3 - Sensitive Data Exposure	45
4	A4: XML External Entities	Introduction To OWASP Top Ten: A4 - XML External Entities	40
5	A5: Broken Access Control	Introduction To OWASP Top Ten: A5 - Broken Access Control	30
6	A6: Security Misconfiguration	Introduction To OWASP Top Ten: A6 - Security Misconfiguration	30
7	A7: Cross Site Scripting	Introduction To OWASP Top Ten: A7 - Cross Site Scripting	75
8	A8: Insecure Deserialization	Introduction To OWASP Top Ten: A8 - Insecure Deserialization	30
9	A9: Using Components With Known Vulnerabilities	Introduction To OWASP Top Ten: A9 - Using Components With Known Vulnerabilities	45
10	A10: Insufficient Logging and Monitoring	Introduction To OWASP Top Ten: A10 - Insufficient Logging and Monitoring	30
11	Capstone	Introduction To OWASP Top Ten: Capstone	90
			Total: 8.5 hours

About Comtech

Comtech provides cybersecurity solutions and services tailored to training and workforce development. The CyberStronger product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech CyberStronger offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.