COMTECH™
Fluent in the Future

PEN600 Advanced Web Application Exploitation

Course Overview

Web applications are the source of many security vulnerabilities. Because of this, many web developers try to lock down the security of their web applications. However, not all of them do it correctly or completely, leaving certain avenues of attack still open. The Advanced Web Exploitation course explores how to search for, find, and exploit these hard to find vulnerabilities.

Each module will have video lecture content, explaining how to evade common incomplete mitigation strategies and how to find and exploit difficult vulnerabilities. Each module will also have a hands-on lab component, in which the students will have the chance to experiment with advanced techniques, seeing why they work and how they can be modified in whatever unique situation is encountered. Students will then complete a capstone lab that will allow the student to explore a novel web application and perform a multistep attack to exploit it completely.

At the end of this course, students will understand the shortcomings of incomplete fixes to these vulnerabilities. They will also understand how these vulnerabilities might manifest themselves and how to modify their attack strategy to compensate.

Objectives

- Evade common incomplete filters to achieve the basic attacks
- String multiple attacks together to achieve a more difficult objective

Prerequisite Knowledge

Before taking this course, students should be familiar with:

- Identify basic examples of the OWASP Top Ten vulnerabilities
- Exploit the basic manifestations of these vulnerabilities

Estimated Course Length: 24 hours

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

Module	Lecture	Labs	Estimated Completion Time (minutes)
0	Introduction		5
1	Basic Recon Tools	Lab 1: Recon Tools	60
2	Advanced SQL Injection	Lab 2.1: Detecting and Exploiting Hard to Find SQL Injection Vulnerabilities Lab 2.2: Advanced SQLmap Lab 2.3: Manual Blind SQL Injection Lab 2.4: NOSQL Injection	300
3	XSS Filter Evasion	Lab 3.1: XSS Filter Evasion Lab 3.2: Exploiting Misconfigured CORS	120
4	OS Command Injection Filter Evasion	Lab 4: OS Command Injection Filter Evasion	90
5	Local File Inclusion	Lab 5: Advanced Local File Inclusion	90
6	Cross Site Request Forgery	Lab 6: Advanced Cross Site Request Forgery	90
7	XML External Entities	Lab 7.1: XXE to Obtain Arbitrary Files Lab 7.2: Out Of Band XXE	120
8	Server Side Request Forgery	Lab 8: SSRF for Internal Port Scanning and File Disclosure	90
9	Insecure Deserialization	Lab 9: Exploiting Insecure Deserialization in Java and Python	90
11	Capstone	Lab 10: Capstone: Multistage Attack on a Partially Hardened Web Application	480
			Total: 24 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.