Web Application Security: Beginner Edition Bootcamp

Objective

With the ubiquity of web applications, understanding their security and being able to audit them is a critical skill all security professionals should possess.

In this beginner bootcamp, we will take you through the basics of modern web applications, their architectures, essential components and common deployment scenarios on servers and in the cloud.

Our teaching methodology focuses on helping beginners learn essential concepts by trying every attack practically in our purpose built labs. This ensures that at the end of this bootcamp you will have job-ready skills to begin your journey as a junior web application pentester.

Prerequisites

- A basic knowledge of computers and networking
- Familiarity with the Linux operating system

Course Content

A non-exhaustive list of topics that will be covered includes:

Module I: Modern Web Applications and Protocol Basics

Objective: Learn the building blocks of web applications and how everything works behind the scenes including HTTP Methods, web design patterns, client and server-side components. Understand modern deployment architectures such as single-page applications, microservices and serverless architecture

1. Client-side Languages and Concepts

2. Server-side Concepts
3. Web Servers
4. Web Communication - HTTP verbs
    a. HTTP request methods
    b. HTTP response codes
    c. HTTP headers and security
    d. HTTP access control
    e. HTTP authentication
    f. HTTP cookies

5. HTTPS vs HTTP

6. Data Storage - Database Servers
    a. SQL
    b. NoSQL

7. Web Application Architecture
    a. Monolithic architecture
    b. Single page applications
    c. Microservices
    d. Serverless architecture

Module II: Reconnaissance Basics

Objective: Learn how to perform reconnaissance on a network, identify live hosts, and fingerprint the services running on machines.

1. Domain Reconnaissance
    a. Whois lookup
    b. DNS reconnaissance
2. Network Scanning and Live Host Identification
3. Open Ports and Running Services
4. Identifying Architectures, Operating Systems and Frameworks
5. Spidering/Crawling Websites
6. Performing Directory Enumeration
7. Discovering Protected Resources

Module III: Tools of the Trade

Objective: Learn how to use popular open source tools for reconnaissance, observing, mangling data, and automation of attacks.

1. Enumerating Common/Framework-specific Directories
    - DIRB
    - DirBuster
    - Burp Suite
    - OpenDoor
2. Crawling Web Pages
    - ZAP
    - HTTrack
    - Burp Suite
3. Identifying Web Application Vulnerabilities with Scanners
    - Nikto
    - OpenVAS
    - Wapiti
    - Vega
    - OWASP OWTF
4. XSS Scanner
    - XSSer
5. Attacking Database Servers
    - sqlmap
    - jSQL
    - BBQSQL

Module IV: OWASP Top 10

Objective: Familiarize yourself with the OWASP Top 10 which are the most common vulnerabilities attackers are exploiting today. Learn everything with practical hands-on labs using both manual methods and tool based automation where applicable.

- A1 Injection Attacks
    - SQL Injection

  - NoSQL Injection
  - OS Command Injection
  - Code Injection

- A2 Broken Authentication
  - Weak Credentials
  - Default Credentials
  - SQL Injection
  - Cookie Manipulation
  - Parameter Tampering

- A3 Sensitive Data Exposure
  - Plain Text Transmission (HTTP/FTP/SMTP)
  - Presence of .git Directory
  - Presence of Debugging Utilities
  - Installation Files/README
  - Backup Directory/Log Directories
  - Lack of Custom Error Pages

- A4 XML External Entity
  - Classic XXE
  - Error Based XXE
  - Blind XXE

- A5 Broken Access Control
  - Path Traversal
  - Remote File Inclusion
  - Insecure Direct Object Reference
  - Client-Side Checks
  - Missing/Improper Functional Level Access Control
  - Missing HTTP Method-specific Access Control on Resources
  - CORS Misconfiguration

- A6 Security Misconfigurations
  - Management Applications with Weak/Default Credentials
  - Directory Listing Enabled
  - Disabled Security Features
  - Poor Error Handling

- A7 Cross-Site Scripting

    - Reflected Cross-Site Scripting
    - Stored Cross-Site Scripting
    - DOM Based Cross-Site Scripting

- A8 Insecure Deserialization
    - Remote Code Execution
    - Denial of Service

- A9 Using Components with Known Vulnerabilities
- A10 Insufficient Logging & Monitoring

Module V: Real World Attacks

Objective: Perform case study on popular real-world attacks, understand the root cause of the vulnerability, and how the attackers exploited it.

- Case Study
    - Laravel Unserialize RCE (CVE-2018-15133)
    - Rails DoubleTap RCE (CVE-2019-5418, CVE-2019-5420)
    - Jquery-File-Upload (CVE-2018-9206)
    - Drupalgeddon2 (CVE-2018-7600)