WEBAPP SECURITY BOOTCAMP

These video recordings are from our live online bootcamp

Session I

The following topics are covered in Session I

- Client-side Languages and Concepts
- Server-side Concepts
- Web Servers
- Web Communication - HTTP verbs
    - HTTP request methods
    - HTTP response codes
    - HTTP headers and security
    - HTTP access control
    - HTTP authentication
    - HTTP cookies
- HTTPS vs HTTP
- Attacking HTTP authentication
- Attacking HTTP login forms
- Web Application Architecture
    - Monolithic architecture
    - Single-page applications
    - Microservices
    - Serverless architecture
- AWS Lambda Overview

3:08:02

List of labs covered during the session (and homework):

- HTTP Protocol Basics (https://www.attackdefense.com/paredirect?cid=861)
- HTTP Method Enumeration (https://www.attackdefense.com/paredirect?cid=1802)

- Attacking HTTP Login Form with Burp Suite (https://attackdefense.com/challengedetails?cid=1896)
- Attacking HTTP Login Form with ZAProxy (https://attackdefense.com/challengedetails?cid=1897)

Session II

The following topics are covered in Session II

- Bypassing authentication by verb tampering
- Finding public S3 buckets
- Enumerating Common/framework-specific Directories
    - Dirb
    - Dirbuster
    - Gobuster
    - Burp Suite
    - OpenDoor
    - ZAProxy
- Passive and Active Crawling
- OWASP Top 10: A9 Using Components with Known Vulnerabilities
- OWASP Top 10: A1 Injection
    - Command Injection

3:23:35

List of labs covered during the session (and homework):

- Verb Tampering: API Gateway (https://www.attackdefense.com/challengedetails?cid=2276)
- Directory Enumeration with Dirb (https://attackdefense.com/challengedetails?cid=1881)
- Directory Enumeration with Dirbuster (https://attackdefense.com/challengedetails?cid=1883)
- Directory Enumeration with Gobuster (https://attackdefense.com/challengedetails?cid=1882)
- Directory Enumeration with Burp Suite (https://attackdefense.com/challengedetails?cid=1886)
- Directory Enumeration with Opendoor (https://attackdefense.com/challengedetails?cid=1884)
- Directory Enumeration with ZAProxy (https://attackdefense.com/challengedetails?cid=1885)
- Passive Crawling with Burp Suite (https://attackdefense.com/challengedetails?cid=1891)
- Active Crawling with ZAProxy (https://attackdefense.com/challengedetails?cid=1890)
- Vulnerable Xdebug Extension (https://attackdefense.com/challengedetails?cid=1909)
- Shellshock (https://attackdefense.com/challengedetails?cid=1911)
- Command Injection (https://attackdefense.com/challengedetails?cid=1899)
- Command Injection (https://attackdefense.com/challengedetails?cid=2282)

Session III

The following topics are covered in Session III

- OWASP Top 10: A1 Injection
    - SQL Injection
    - NoSQL Injection
- OWASP Top 10: A4 XML External Entity
- OWASP Top 10: A6 Security Misconfiguration

3:22:05

List of labs covered during the session (and homework):

- Command Injection II (https://attackdefense.com/challengedetails?cid=1906)
- Command Injection III (https://attackdefense.com/challengedetails?cid=1907)
- PHP Code Injection (https://attackdefense.com/challengedetails?cid=1900)
- SQL Basics (https://www.attackdefense.com/paredirect?cid=1801)
- Basic SQL Injection (https://attackdefense.com/challengedetails?cid=1901)
- OpenSupports (https://attackdefense.com/challengedetails?cid=437)
- DynamoDB : SQL Injection (https://attackdefense.com/challengedetails?cid=2292)
- DynamoDB : NoSQL Injection (https://attackdefense.com/challengedetails?cid=2293)
- XML External Entity (https://attackdefense.com/challengedetails?cid=2119)
- Apache Solr (https://attackdefense.com/challengedetails?cid=1530)
- Server Side Request Forgery (https://attackdefense.com/challengedetails?cid=2286)
- XML External Entity : Python Runtime (https://attackdefense.com/challengedetails?cid=2284)
- XML External Entity : PHP Runtime (https://attackdefense.com/challengedetails?cid=2285)
- RCE Via MySQL (https://attackdefense.com/challengedetails?cid=1910)
- Security Misconfigurations in Apache (https://attackdefense.com/challengedetails?cid=2149)

Session IV

The following topics are covered in Session IV

- OWASP Top 10: A8 Insecure Deserialization
- OWASP Top 10: A3 Sensitive Data Exposure
- OWASP Top 10: A2 Broken Authentication
- OWASP Top 10: A5 Broken Access Control
    - Insecure Direct Object Reference
    - Local File Inclusion
    - Directory and Path Traversal
- OWASP Top 10: A7 Cross-Site Scripting
    - Reflected XSS
    - Dom-based XSS
    - Stored XSS

3:42:26

List of labs covered during the session (and homework):

- Insecure Deserialization (https://attackdefense.com/challengedetails?cid=2283)
- Pickle Deserialization RCE II (https://www.attackdefense.com/challengedetails?cid=1915)
- Pickle Deserialization RCE I (https://www.attackdefense.com/challengedetails?cid=1912)
- Sensitive Data Exposure (https://attackdefense.com/challengedetails?cid=2299)
- Sensitive Directories in robots.txt (https://attackdefense.com/challengedetails?cid=1889)
- CVE-2018-12604 (https://attackdefense.com/challengedetails?cid=11)
- Session ID Analysis II (https://attackdefense.com/challengedetails?cid=813)
- Session ID Analysis III (https://attackdefense.com/challengedetails?cid=814)
- Online Airline Booking System (https://attackdefense.com/challengedetails?cid=438)
- Improper Session Management II (https://attackdefense.com/challengedetails?cid=1899)
- Session ID Analysis (https://attackdefense.com/challengedetails?cid=812)
- Insecure Direct Object Reference (https://attackdefense.com/challengedetails?cid=1907)
- Insecure Direct Object Reference II (https://attackdefense.com/challengedetails?cid=1899)
- BloofoxCMS (https://attackdefense.com/challengedetails?cid=279)
- Directory Traversal (https://attackdefense.com/challengedetails?cid=1899)
- DOM Based XSS (https://attackdefense.com/challengedetails?cid=1906)
- MyBB Downloads Plugin (https://attackdefense.com/challengedetails?cid=9)