WEB HACKING AND DEFENSE

COURSE WITH OWASP TOP 10 VULNERABILITIES

OWASP-YN

Duration: 2 days; Instructor-led | Virtual Instructor-led

COURSE OBJECTIVES

By the end of this course, participants will:

- Explain the OWASP Top 10 vulnerabilities and their impact on web applications.
- Identify the attack surface of web applications and common entry points for attackers.
- Perform SQL Injection attacks to extract sensitive data from databases.
- Execute Cross-Site Scripting (XSS) attacks to steal session cookies and manipulate user interactions.
- Exploit Cross-Site Request Forgery (CSRF) vulnerabilities to perform unauthorized actions.
- Conduct Broken Authentication attacks, including brute-forcing and session hijacking.
- Implement secure coding practices to prevent vulnerabilities like SQL Injection and XSS.
- Perform vulnerability assessments and penetration testing on web applications.
- Understand the importance of secure development practices and continuous security Testing.

METHODOLOGY

This program will be conducted with interactive lectures, PowerPoint presentations, discussions, and practical exercises.

COURSE CONTENTS

Day 1

Web Hacking Fundamentals

Module 1: Introduction to Web Security and OWASP Top 10

Topics Covered:

- Overview of web application security
- Introduction to OWASP Top 10 (2021 or 2023 edition).
- Explanation of the attack surface of web applications.

Activity 1: Animation

- How a web request flows between client, server, and database, and how attackers intercept or manipulate it?

Activity 2: Animation

- Discuss real-world breaches caused by OWASP Top 10 vulnerabilities (e.g., Equifax breach due to A03: Injection)

Module 2: Injection Attacks (A03: Injection)

Topics Covered:

- SQL Injection: Exploiting and extracting data from a vulnerable database.
- Command Injection: Executing system commands via web inputs.

Activity 3: Hands-on Labs & Exercise

- Lab 1: Use OWASP Juice Shop or DVWA (Damn Vulnerable Web Application).
  - Exploit SQL Injection to dump database contents.
  - Example: ' OR '1'='1 in a login form.

Activity 4: Animation

- Show how malicious SQL queries bypass authentication and retrieve sensitive data.

Module 3: Broken Authentication (A07: Identification and Authentication Failures)

Topics Covered:

- Exploiting weak passwords, session hijacking, and brute-force attacks
- Understanding multi-factor authentication (MFA) bypass techniques

Activity 5: Animation

- Demonstrate how session tokens are stolen and reused by attackers
  - Exercise: Implement a brute-force attack using Hydra or Burp Intruder.

GemRain Consulting Sdn Bhd.
69-2, Block D, Jaya One, Jalan Profesor Diraja Ungku Aziz, 46200 Petaling Jaya, Selangor, Malaysia
Contact: (+60)3 7931 3036 | (+60)12 613 3667 | Email: enquiry@gemrain.net | Website: www.gemrain.net

Module 4: Cross-Site Scripting (XSS) (A03: Injection)

Topics Covered:
- Reflected XSS, Stored XSS, and DOM-based XSS.
- Exploiting XSS to steal cookies and execute malicious scripts

Activity 6: Hands-on Labs & Exercise
- Use DVWA or OWASP Juice Shop to inject malicious scripts
- Animation: Show how a malicious script is injected into a web page and executed in a victim's browser.
- Exercise: Cookie session ID stealing.

Module 5: Cross-Site Request Forgery (CSRF) (A01: Broken Access Control)

Topics Covered:
- Exploiting CSRF to perform unauthorized actions on behalf of a user.

Activity 7: Hands-on Labs & Exercise
- Use DVWA to create a malicious HTML form that changes a user's password
- Animation: Show how a victim is tricked into submitting a malicious request.
- Exercise: Write a CSRF exploit using HTML and JavaScript.
- Recap with Q and A session

Day 2

Web Defence and Secure Coding

Module 6: Secure Coding Practices (1.5 Hour)

Topics Covered:
- Input validation and output encoding.
- Parameterized queries to prevent SQL Injection.
- Using secure libraries and frameworks

Activity 8: Hands-on Labs & Exercise
- Fix vulnerabilities in a sample web application (e.g., OWASP Juice Shop).
- Implement input validation and parameterized queries
- Animation: Show how input validation blocks malicious payloads.

Module 7: Web Application Firewalls (WAFs)

Topics Covered:
- Introduction to WAFs and their role in protecting web applications.
- Bypassing WAFs using obfuscation techniques.

Activity 9: Hands-on Labs & Exercise
- Use ModSecurity or a cloud-based WAF (e.g., AWS WAF).
- Test WAF rules and bypass them using encoded payloads.
- Animation: Show how a WAF detects and blocks malicious requests

Module 8: Secure Authentication and Session Management

Topics Covered:
- Implementing strong password policies and MFA.
- Secure session management techniques (e.g., secure cookies, session expiration).

Activity 10: Hands-on Labs & Exercise
- Configure secure cookies in a web application.
- Implement session timeout and regeneration.
- Animation: how secure session management prevents session hijacking.
- Exercise: Implement MFA

Module 9: Security Testing and Tools

Topics Covered:
- Introduction to security testing tools (e.g., Burp Suite, OWASP ZAP, Nmap).
- Performing vulnerability assessments and penetration testing.

Activity 11: Hands-on Labs & Exercise
- Use OWASP ZAP to scan a web application for vulnerabilities.
- Analyse the results and prioritize fixes.
- Animation: how a vulnerability scanner identifies and reports issues.
- Exercise: Perform a full penetration test on a sample application.

Module 10: Capture the Flag (CTF) Challenge

Topics Covered:
- Demo Hands-on CTF challenge covering selected topics.
- Participants work in teams to find and exploit vulnerabilities in a simulated environment.

Activity 12: Hands-on Labs & Exercise
- Use OWASP Juice Shop or Hack the Box for the CTF.
- Exercise: Participants document their findings and present their solutions.
- Recap with Q and A session