PHP Secure Development 2.4 hours of content | 60 hours of practice | Final Project

1.Introduction and Setup

- Introduction to the course and instructor
- Installing required tools and environments
- Setting up local labs using XAMPP
- Types of hackers

2. Introduction to OWASP Top 10

- Understanding secure development methodology
- Practical exercise on secure development flow
- Introduction to Burp Suite
- Burp Suite usage and features

3.OWASP Top 10 – In-Depth

- A10- SSRF vulnerability explained
  - SSRF attack demonstration (attacker perspective)
  - Understanding SSRF from client to server
  - Fixing SSRF vulnerabilities
- Introduction to regular expressions
- A9 - Using Components with Known Vulnerabilities
- A8 - Insecure Deserialization
  - Demonstration of Insecure Deserialization (black-box)
  - Demonstration of Insecure Deserialization (white-box)
  - Preventing Insecure Deserialization
- A7 - Cross-Site Request Forgery (CSRF) and Related Attacks
  - Introduction to A7
- Parameter tampering attacks
- Role of CAPTCHA in websites
- CAPTCHA best practices
- Session fixation explained
- Exploiting authentication flaws
- Summary of A7
- A6 - Security Misconfiguration
- A5 - Broken Access Control
- LFI/RFI vulnerabilities explained (attacker perspective)
  - Mitigation techniques for LFI/RFI
- Client-Side Security
  - Open Redirect vulnerability explained
  - Same-Origin Policy (SOP)
  - Security headers overview:
  - Content Security Policy (CSP)
  - X-Frame-Options
  - HSTS
  - HTTP Cookies
  - HttpOnly protection
  - Secure flag
- Cross-Site Request Forgery (CSRF)
  - Understanding CSRF
  - Preventing CSRF
  - Demonstrating CSRF protection with tokens
- XML and External Entities (XXE)
  - Understanding XXE
  - Fixing XXE vulnerabilities
- A4 - Insecure Design
- A3 - Injection
  - Cross-Site Scripting (XSS)
  - Introduction to XSS
  - Reflected XSS and mitigation
  - DOM-based XSS protection
  - Stored and DOM-based XSS protection strategies
- Remote Code Execution (RCE)
  - Introduction to RCE
  - File upload mechanisms and RCE
  - RCE using command injection
- Other Injection Attacks
- Server Side Template Injection (SSTI)
- SQL Injection
- Authentication and Session Management
- A2 - Broken Authentication
- A1 - Broken Access Control
  - JWT protection
- Course Summary
  - Final recap and summary of all topics covered