Web Penetration Testing 10 hours of content | 110 hours of practice | Final Project

1. Code Analysis and Security Flaw Identification

- Thinking Methods
- Case Study: Facebook Messenger
- Setting Up a Research Environment
- Basics of Chrome Developer Tools
- Advanced Chrome Developer Tools
- Basics of BurpSuite
- Advanced BurpSuite

2. Vulnerabilities and OWASP Top 10

- Case Study: Code Injection on eBay
- XSS (Reflected, Stored, DOM)
- CSS Injection
- Advanced XSS
- SOP, CORS, JSONP
- CSP (Content Security Policy)
- Case Study: Code Injection on AliExpress
- Open Redirect
- SSRF & CSRF
- Case Study: Account Takeover on Snapchat
- Storage Browser and Cookies
- Advanced CSS Injection
- Case Study: Takeover of LG SmartThinQ
- OAuth2
- Components with Known Vulnerabilities
- Case Study: Facebook Chat
- Security Misconfigurations
- Parameter Manipulation
- LFI/RFI/Path Traversal
- Case Study: ATO on WhatsApp & Telegram
- Broken Access Control
- JWT (JSON Web Tokens)
- Sensitive Data Exposure
- Broken Authentication
- Session Fixation
- Insufficient Anti-Automation
- Command Injection
- SQL Injection (Basic)
- SQL Injection (Advanced)

3. Testing Methodology and Report Writing

- Submitting Reports and Projects
- Writing a Penetration Testing Report
- Testing Methodology