QA Security 10 hours of content | 40 hours of practice | Final Project

1. Fundamentals of the Internet and Application Security

- Introduction to the HTTP protocol
- Structure of HTTP requests and responses
- Understanding HTTP status codes
- Cookies and client-side data storage
- Basic network protocols
- Introduction to HTML, CSS, and JavaScript
- Using popular libraries: Bootstrap, JQuery

2. Advanced Attacks and OWASP Top 10

- Hands-On Security Analysis with Burp Suite
  - Practical vulnerability testing using Burp Suite
- Identity and Authentication Management
  - Principles of modern identity management
  - Authentication and authorization mechanisms
  - Detecting Authentication & Identification Failures
  - Working with outdated or vulnerable system components
  - Security best practices for user access controls
- SSRF - Server-Side Request Forgery
  - Integrity Failures
- Insufficient Logging & Monitoring
- XSS (Cross-Site Scripting)
  - Understanding common XSS attack types:
  - Reflected XSS
  - Stored XSS
  - DOM-based XSS
  - Preventing XSS using encoding
- SQL Injection and Remote Code Execution (RCE)
  - Anatomy of SQL Injection attacks
- Introduction to Remote Code Execution vulnerabilities
- Advanced Security Mechanisms
  - Access control and authorization flaws (Broken Access Control)
  - Protection against CSRF (Cross-Site Request Forgery)
  - IDOR - Insecure Direct Object References
  - Secure cookie management practices
  - Using JWT - JSON Web Tokens for secure session handling

3. Penetration Testing Methodologies

- Penetration Testing Methodologies
- Practical application of the OWASP Top 10 in real scenarios
- Writing a professional penetration test report: documentation, prioritization, and conclusions