Web Security

24h

Expected results

- Practical knowledge of Vulnerability Assessment tools
- Practical knowledge of Web-based attacks
- Practical knowledge of code-based Vulnerability Detection

Requirements

- HTTP Protocol
  - Client-Server Model
  - HTTP Session Handling (Session Cookies)
  - HTTP Methods (GET, POST, ecc.)
- HTML
- Server-Side scripting
  - PHP
  - SQL
- Client-Side scripting
  - JavaScript (basic knowledge)

Topics

Technical

- Cross-Site Scripting (XSS)
  - Stored XSS
  - Reflected XSS
- Cross-Site Request Forgery
- SQL Injection
  - Stacked Queries
  - Error-based SQL Injections
  - Blind SQL Injections (Boolean-based e Time-based)
- Path Traversal
- Command Injection

Methodological

- White-box Testing
  - Code Review

- Black-box Testing
  - Vulnerability Scanners
- OWASP Testing Framework

Lab

- Implementation of Web-based attacks
- Security patch development on insecure code
- Vulnerability Assessment on sample code