orange Cyberdefense

Training Catalogue

Knowledge is power

HA 1.01 | Web Application Security

Overview

Hands-on training which covers a broad scope of vulnerabilities that can be found in Web applications. The objective is to provide participants with the methodology and tools required in order to assess a Web application. It is tailored for developers or junior security engineers who want to start their journey in attacking and compromising Web applications. It does not dive in-depth into specific vulnerabilities, but rather covers a broad spectrum of issues to provide the participants with a basic understanding of all the relevant topics.

Who should attend

- Developers
- Ethical hackers, incident responders
- IT system & network admins

Skills you'll learn

Basic understanding of Web technologies

Level 2

2 days

French or English

Course Modules

- **Introduction**
  - Overview of technologies in use
  - Encodings
  - Introduction to BurpSuite
- **Information gathering**
  - Generic information gathering
  - Specific information gathering
- **Entry point analysis**
  - Identifying entry points
  - Analysing entry points
  - Fuzzin entry points
- **Authentication & Authorisations**
  - Session issues
  - Authentication issues
  - Delegating authentication
  - SAML
  - Oauth2/OIDC
  - JWT
  - Access control
    - Function
    - Resource-based
- **Server-side attacks**
  - Injections
  - XML
  - Path traversal
  - Server-Side Request Forgery
  - Deserialization
  - Race conditions
- **Client-side attacks**
  - Same Origin Policy
  - Cross-Origin Resource Sharing
  - PostMessage API
  - JSONP
  - Cross-Site Scripting
  - Cross-Site Request Forgery
  - Websockets
- **Infrastructure attacks**
  - Attacking encryption mechanisms
  - Request smuggling
  - Cache poisoning