

kod szkolenia: BEZP\_WEB / ENG DL 2d

# Web Application Security





## Purpose of the training

The training is intended for IT practitioners – especially developers and QA engineers, but also system administrators and managers who want to know how web applications are attacked today and how to prevent it.



### Benefits of completing the training

Participant will gain comprehensive, practical knowledge about web application attacks and defense mechanisms, backed by multiple examples and exercises.



### **Expected Listener Preparation**

- Basic programming skills (any language)
- Basics knowledge about JavaScript and SQL syntax
- Basic knowledge about IT solutions architecture, web applications, OS and networks



#### Training Language

• Training: English



#### Czas trwania



#### 2 dni / 14 godzin

#### Training agenda

- 1. Introduction to web application security
  - Web application architecture
  - OWASP Top 10 2021
- 2. Network traffic security
  - TLS/SSL
  - HTTP security headers
  - Same-Origin Policy and Cross-Origin Resource Sharing (CORS)
- 3. Methodology
  - Network traffic analysis
  - HTTP request manipulation
  - Creating custom scripts
  - Vulnerability scanners
- 4. Vulnerability analysis (causes, fixes, exploitation)
  - Cross-site scripting (XSS)
  - Cross-Site Request Forgery (CSRF)
  - Directory Traversal
  - Unrestricted File Upload
  - Insecure Direct Object Reference (IDOR)
  - SQL/NoSQL injection
  - Server-Side Template Injection (SSTI)
  - Server-Side Request Forgery (SSRF)
  - Broken authentication and authorization
  - Denial of Service
- 5. API security
  - Authentication and authorization methods
  - OWASP API Security Top 10 2019
- 6. Blackbox web penetration test (CTF)