Corporate Readiness Certificate.

SYLLABUS

Web application penetration testing

Testy penetracyjne aplikacji internetowych

[Number of hours: 12 h]

DESCRIPTION OF THE COURSE

This course is designed for cybersecurity beginners who would like to start their journey with cybersecurity. The aim of the course is to understand the concepts related to web application security and to learn basics of the web application penetration testing.

REQUIREMENTS

- English language – at level allowing to get familiar with technical documentation

REQUIRED BACKGROUND

Basic knowledge of cybersecurity, understanding basic web technologies and protocols (e.g. HTTP, HTML, JavaScript).

PASSING CRITERIA

1. Passing course entrance test, with most of the questions being single choice. The test will verify basic knowledge of cybersecurity, understanding basic web technologies and protocols (e.g. HTTP, HTML, JavaScript)
2. Participating in lectures and workshops of the course.
3. Passing course final test, with multiple questions being open-ended. The test will verify knowledge and practice gained during the course.

ADDITIONAL INFORMATION ON COURSE

The course allows participants to get familiar with cybersecurity principles. The course focuses on the security of web applications, and how this security can be validated with penetration testing. Knowledge gained during the course will help participants understand key cybersecurity concepts, prepare for and perform basic web application penetration test, and report the findings. Finishing the course will help participants with starting professional cybersecurity career or participating in Bug Bounty programs.

CONTENT & LITERATURE

https://owasp.org/www-project-web-security-testing-guide/

https://github.com/OWASP/ASVS/

https://owasp.org/www-project-top-ten/

TECHNICAL REQUIREMENTS FOR UNIVERSITY

Course participants are required to have laptops/PCs (recommended usage of virtual machine with Kali Linux installed) with access to the Internet.

COURSE OVERVIEW

1. Introduction to course
2. Key knowledge basics:
    a) Infrastructure of web apps
    b) HTTP and HTTPS protocols
    c) TLS protocol
    d) HTML and JavaScript languages
    e) Local Proxy
3. Introduction to OWASP
    a) About OWASP organization
    b) OWASP testing documentation
    c) OWASP testing cheat sheets
    d) OWASP meetings
4. OWASP Top 10
    a) Top security risks
    b) Identifying OWASP Top 10 in practice
5. OWASP Testing Guide
    a) About OWASP Testing Guide
    b) Using OWASP Testing Guide
    c) General walkthrough of selected areas
6. OWASP ASVS
    a) About OWASP ASVS
    b) Using the ASVS
    c) General walkthrough of selected controls
7. Penetration testing project lifecycle
    a) Contractual requirements and obligations
    b) Planning of security testing
    c) Project management
8. Reporting
    a) How to write a report
    b) Severity/risk rating methodologies
9. Penetration testing in practice – workshops
    a) Introduction to workshop
    b) Individual work of student workshop

c) Group discussion workshop results
d) Workshop summary

10. Next steps
a) Ethical Hacking
b) Professional career
c) Bug Bounty