MODULE DESCRIPTION CARD – SYLLABUS

This module is a part of the Intensive International Education Programs in the field of the … organised at Poznan University of Technology as part of the „IMPACT – Innowacyjne Międzynarodowe Programy w AI, Cyberbezpieczeństwie i Teleinformatyce" project implemented SPINAKER Program of the National Agency for Academic Exchange, financed by the European Social Development Fund 2021–2027 (ESDF).

Module name:	Number of hours:	Lecturer:
Web Application Security	10	Piotr Kontowicz

Module Descriptions:

This module introduces participants to modern web application architectures and the most critical security threats affecting them. Through a combination of theory, demonstrations, and practical exercises, students learn how to analyze attack surfaces, identify vulnerabilities, and apply secure coding and configuration practices. The course emphasizes the OWASP Top 10 framework, covering both server-side and client-side threats, as well as modern defense mechanisms such as security headers, CSP, and secure authentication protocols.

Purpose of the support under Module:

The overall objective of the Innovative International Education Program in Artificial Intelligence is to enhance participants competencies in securing digital infrastructures and applications against modern cyber threats. The specific objective of this module is to equip students with practical skills for identifying, analyzing, and mitigating security vulnerabilities in web applications, fostering secure software development practices at every stage of the lifecycle.

Method of support under Module:

Support within the module is provided with the participation of the instructor and divided into the following elements:

- 6-week self-study program using teaching materials provided by the instructor on the e-learning platform;
- 6 weeks of support from the instructor in the form of online consultations using tools that enable meetings to be held;
- a test to verify the acquisition of competences.

Module-related learning outcomes:

Descriptions of the new competences:

Description of acquired competences

Knowledge:

1. Understands the architecture of modern web applications (frontend, backend, APIs, databases, cloud) and typical attack surfaces.
2. Identifies the most common categories of web vulnerabilities according to the OWASP Top 10, including injection, broken access control, and misconfigurations.

3. Recognizes mechanisms of authentication, session management, and security headers (CSP, HSTS, CORP) in mitigating attacks.

Skills:

1. Can identify and exploit common vulnerabilities in web applications in a controlled lab environment.
2. Can apply secure coding practices, implement input validation, and configure web frameworks to minimize security risks.
3. Can design and test API endpoints for secure authentication, authorization, and data exposure.

Social competences:

1. Is aware of the ethical and legal aspects of penetration testing and responsible disclosure of vulnerabilities.
2. Understands the importance of continuous learning and staying up to date with evolving cybersecurity threats and defensive measures.

Criteria for verifying learning outcomes

Area	Method of verification/validation
Theoretical knowledge	Online test and short case-study quiz
Practical skills	Laboratory exercises and challenge-based evaluation

Verification of learning outcomes is based on a combination of theoretical and practical assessments that comprehensively evaluate the students knowledge and applied skills in web application security. Each learning outcome category is verified through specific method.

Learning outcome category	Verification criteria	Assessment methods
Knowledge	Demonstrates understanding of modern web application architecture, OWASP Top 10 vulnerabilities, and key security mechanisms such as authentication, session management, and HTTP security headers (CSP, HSTS, CORP).	Online Moodle quizzes assessing theoretical comprehension and terminology.
Skills	Applies theoretical knowledge to practical tasks involving vulnerability identification, exploitation, and mitigation. Demonstrates the ability to use penetration testing tools and implement secure coding practices.	CTF-style challenges and hands-on labs simulating real-world attack and defense scenarios.

Method of verification/validation of learning outcomes

Verification and validation of learning outcomes are carried out through a structured combination of theoretical tests and practical performance evaluations. These methods ensure that students not only understand the principles of web application security but can also effectively apply them in realistic scenarios.

Assessment method	Description	Purpose and validation approach
Moodle quizzes	Periodic online quizzes covering theoretical aspects of web application security, including architecture, OWASP Top 10 vulnerabilities, authentication, session management, and HTTP security mechanisms.	Used to validate students' conceptual understanding and retention of theoretical material. Quizzes are automatically graded, ensuring objective evaluation. Repeated attempts provide formative feedback and reinforce learning.
CTF-style practical challenges	Scenario-based, hands-on exercises designed to simulate real-world security testing tasks such as identifying, exploiting, and mitigating vulnerabilities (e.g., SQLi, XSS, CSRF, SSRF).	Used to validate applied skills and the ability to translate theory into practice. Each task requires finding and documenting a “flag” or implementing a fix. Successful completion confirms competency in vulnerability analysis and secure coding.

Workload

25 h (including work with teaching materials provided by the lecturer, consultation, and the student's own work) – 1 ECTS point

Level of the European Qualifications Framework