COURSE DESCRIPTION CARD - SYLLABUS

Course name
Web Application Security [S2Inf1-GiTI>BAIN]

Course

Field of study
Computing

Year/Semester
2/3

Area of study (specialization)
Games and Internet Technologies

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
15

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl

Lecturers

Prerequisites

The student starting this course should have basic knowledge of web apps programming languages (a.o. web apps) and basic knowledge of database design. Student should have the ability to solve basic problems related to the process of designing IT systems and the ability to obtain information from different sources. The student should also understand the necessity to expand their competences / be ready to cooperate within the team. In addition, in terms of social competences, the student must present attitudes such as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people.

Course objective

- providing students with knowledge on designing secured web applications on the example of CMS / CRM / e-commerce systems. - developing students' skills in solving problems related to the design of web applications with the use of open-source solutions, frameworks and libraries supporting the construction of such solutions - shaping students' teamwork skills and independence in solving problems.

Course-related learning outcomes

Knowledge:

-has structured, theoretically founded knowledge in the field of security of web applications,
-has detailed knowledge related to selected issues in the field of computer science and knows the technologies used in the construction of secured web apps.
-has knowledge of the life cycle of web apps and the risks to which such applications are exposed,

Skills:
-student can formulating and solving engineering tasks, integrate knowledge from various areas of computer science (and, if necessary, knowledge from other scientific disciplines) as well as knowledge of the operation of web apps and apply a system approach, also taking into account non-technical aspects,
-can assess the usefulness and the possibility of using new technological achievements (methods, tools, libraries, frameworks, services),
-can be used to formulate and solve tasks and simple research problems regarding the specifics of web applications, analytical, simulation and experimental methods (such as: estimating the number of requests to the application, server load with SQL queries), is able to correctly design and implement efficient applications,
-can make a critical analysis of the existing technical solutions, including the assessment of the application's susceptibility to known threats,

Social competences:
-understands that in computer science knowledge and skills very quickly become obsolete, in particular internet technologies
-understands the need to use the latest technology achievements and knows examples and understands the causes of malfunctioning web applications that may lead to serious financial, image or social losses

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

- lecture - the knowledge acquired during the lectures is verified during the test, in writing. The test passing threshold is 50%. The correctness of the answers and the student's understanding of the problem are assessed.

- laboratories - based on the assessment of the current progress in the implementation of tasks.

Programme content

The module program includes an introduction to web application security with a focus on vulnerabilities from the OWASP Top 10 project.

Course topics

The lecture program includes discussion of the following topics, from the field of web application security: Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting XSS, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging and Monitoring.

Laboratory activities are carried out independently by students. Assignments include the following: review and analysis of selected open-source CMS/CRM/e-commerce web applications for vulnerabilities to known threats. Design and implementation of an in-house application and audit of its security.

Teaching methods

Lecture: multimedia presentation supplemented with examples and additional explanations on the blackboard. Lectures are conducted in accordance with the principles of a traditional lecture, in the form of a conversation lecture in justified cases.

Laboratories: multimedia presentation, presentation illustrated with examples.

Bibliography

Basic:
1. OWASP Top 10 Web Application Security Risks, [https://owasp.org/www-project-top-ten/]

Additional:
1. Web Application Security, Andrew Hoffman, O'Reilly 2020
2. Tworzenie bezpiecznych aplikacji internetowych, Lis M., Helion 2014
3. Web Application Security. Exploitation and Countermeasures for Modern Web Applications, O'Reilly 2019
4. Secure Web Application Development, Baker M., Apress 2022

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,00
Classes requiring direct contact with the teacher	30	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	20	0,50