COURSE DESCRIPTION CARD - SYLLABUS

Course name
Application Security

Course

Field of study
Computing

Year/semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
English

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
45

Other (e.g. online)
0

Tutorials
0

Projects/seminars
0

Number of credit points

5

Lecturers

Responsible for the course/lecturer:
dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl
tel: 61 665 3531
Faculty of Computing and Telecommunications

mgr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl
tel: 61 665 3992
Faculty of Computing and Telecommunications

mgr inż. Łukasz Matuszczak
lukasz.matuszczak@put.poznan.pl
tel: 61 665 3993
Faculty of Computing and Telecommunications

Prerequisites

The student starting this course should have basic knowledge of structured and object-oriented programming and basic knowledge of database design. He 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 safe web applications on the example of CMS / CRM / e-commerce systems and safe mobile applications.

- developing students' skills in solving problems related to the design of web and mobile 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 internet and mobile applications,

-has detailed knowledge related to selected issues in the field of computer science and knows the technologies used in the construction of secure web apps and mobile apps.

-has knowledge of the life cycle of web and mobile 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 / mobile 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 internet / mobile 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 and mobile technologies

-understands the need to use the latest technology achievements and knows examples and understands the causes of malfunctioning web/mobile 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 exam, in writing. The exam passing threshold is 50%. The correctness of the answers and the student's understanding of the problem are assessed.

-Laboratories / project - based on the assessment of the current progress in the implementation of tasks.

Programme content

The lecture program covers the following issues:

In 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

In the field of mobile application security: Improper Platform Usage, Insecure Data Storage, Insecure Communication, Insecure Authentication, Insufficient Cryptography, Insecure Authorization, Client Code Quality, Code Tampering, Reverse Engineering, Extraneous Functionality

Laboratories / project

Practical classes are conducted independently by students. The tasks include the following issues: review and analysis of selected open-source CMS / CRM / e-commerce web applications and a selected mobile application in terms of vulnerability to known threats.

Design and implementation of your own secure web and mobile application. Development of system design documentation containing: functional and non-functional requirements of the application, UML diagrams, OWASP security audit. Taking into account the latest technologies and trends in the design.

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 / project: multimedia presentation, presentation illustrated with examples.

Bibliography

Basic

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

2. *OWASP Mobile Top 10* [https://owasp.org/www-project-mobile-top-10/]

Additional

1. *Web Application Security*, Andrew Hoffman, O'Reilly 2020

2. *Tworzenie bezpiecznych aplikacji internetowych*, Lis M., Helion 2014

3. Learning iOS Security, Allister Banks , Charles S. Edge, Packt 2015

4. Learning Pentesting for Android Devices, Aditya Gupta, Packt 2014

Breakdown of average student's workload

	Hours	ECTS
Total workload	125	5,0
Classes requiring direct contact with the teacher	60	2,5
Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam, project preparation) [1]	65	2,5

[1] delete or add other activities as appropriate