Security

Faculty of Engineering, Design and Computing, Department of Information Technology

When

7 November 2022 - 31 January 2023
Class days: 3 to 4 days (1 day off)

General Information

Audience: Bachelor ICT 3rd year with experience in programming.
15 European Credits (20 weeks)
Where: Haarlem, the Netherlands

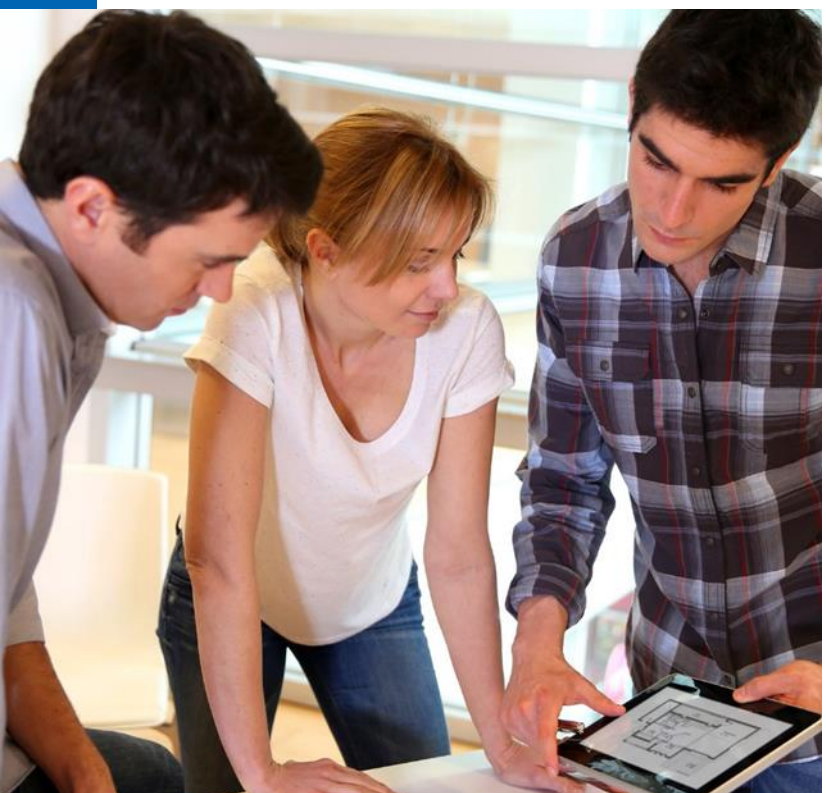
Teachers

Teachers of the Computer Science Haarlem study program and various guest lectures andworkshops by specialists from the field of ICT Security.

In this minor we work closely with the Eurofins company This company is specialized in IT Security.

Strategies and teaching activities

- Workshops by experts.
- Perform a security assessment with your project group.
- Do research with your project group.
- Lectures on theory combined with practical exercises.



About the course

Almost daily, news reaches us that the government or companies are dealing with cyber-attacks by hackers. Today's software engineering professionals must understand the basic discipline of building secure software.
Not because "it's a good idea", but because the nature of the internet mandates it.

This minor is highly practical and is divided into a number of courses.

The first course covers penetration testing. You will learn how the target system works, the weaknesses of this system and how to practically exploit these weaknesses and hack into it.

The second course is about secure programming. This course covers the OWASP top 10 flaws and how to fix them. Special attention is paid to securing an API

The third course is about networking security. This course provides an introduction to the core security concepts and skills needed for the installation, troubleshooting, and monitoring
of network devices to maintain the integrity, confidentiality, and availability of data and devices.

The last course covers the module Information Security Foundation and legal aspects of information security.

nholland
university of applied sciences

Competences

Analyse
- describe security aspects of computer systems that are linked to or via (public) networks.
- analysing the security flaws of an existing application.
- analysing infrastructure-related incidents, problems and security threats

Advise
- advising on the choice of software architecture or software frameworks in which quality characteristics such as availability, performance, security and scalability play a role.

Design
- design a network infrastructure that meets the security requirements

Implement
- set up a network infrastructure that meets the security requirements

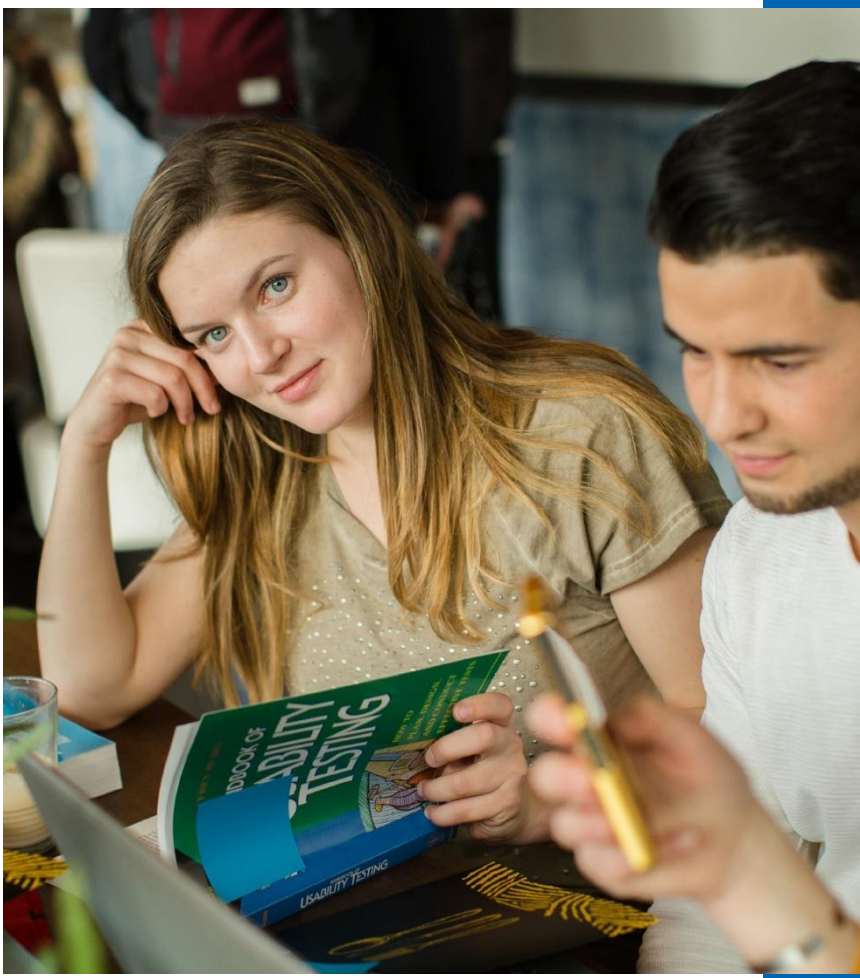
Goals

The student is able to:
- perform a security assessment on a web application
- write a recommendation providing solutions for the vulnerabilities found.
- research the technical functioning, impact and solution of a self-selected vulnerability and describe these in a report.
- make a web page in the language of choicewith 2 or more vulnerabilities and to make the same page with the correct fixes.
- design and create a secure API
- perform a security assessment on an API
- improve the security quality of the softwareto be developed.
- understand network security principles and the tools and configurations available.
- apply knowledge and skills to design, implement, and support network security.
- design and create a secure network
- understand the code information security (ISO 27001

Details of assessments

- Project assessment
- Code assessment
- Individual exams
- Security assessment

All assessments must be completed with a sufficient grade



Contact

Sign up (deadline 31-5-2022)

Petra Folkertsma, Haarlem
petra.folkertsma@inholland.nl

Questions

Willem Wenink, Haarlem
willem.wenink@inholland.nl