Course Title	Security
Semester	Spring (semester 2) – Term 4
Inholland Faculty	Faculty of Engineering, Design and Computing, Department of Information Technology
Language of instruction	English
Cycle	Bachelor level
Inholland Location	Haarlem

Code Subjects	Code	Subject Title	ECTS
	1922SEC02Z	Penetration Testing	4
	1920SEC03Z	Network Security	3
	1918SEC05Z	Secure Programming	3
	1922SEC06Z	Project Offensive Security	3
	1916SEC04Z	Information Security	1
	1916GE011Z	Professional Presenting	1

Number of ECTS	15
Content subjects	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.
Lecturer(s)	Teachers of the Computer Science Haarlem study program and various guest lectures and workshops 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.

Learning outcomes	Competences: Analyse • describe security aspects of computer systems that are linked to or via (public) networks. • analyzing the security flaws of an existing application. • analyzing 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 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 choice with 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 software to 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
Mode of delivery, planned activities and teaching methods	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.

Prerequisites and co-requisites (if applicable)	Audience: Bachelor ICT 3rd year with experience in programming.
Recommended or required reading and/or other learning resources/tools	
Assessment methods and criteria	Project assessment Code assessment Individual exams Security assessment
Contact	Petra Folkertsma, Haarlem petra.folkertsma@inholland.nl Willem Wenink, Haarlem willem.wenink@inholland.nl