Hanzehogeschool Groningen
University of Applied Sciences

Vak: Software Security — credits: 5

Vakcode	ITVP20SCY
Naam	Software Security
Studiejaar	2021-2022
ECTS credits	5
Taal	Nederlands
Coördinator	N. van der Spek
Werkvormen	Hoorcollege Practicum / Training
Toetsen	Opdrachten Engels - Overige toetsing Opdrachten Software Security - Overige toetsing

Leeruitkomsten

De student:

1. Detecteert veelvoorkomende beveiligingsproblemen in een desktopapplicatie met behulp van tools zoals American Fuzzy Lop.
2. Detecteert veelvoorkomende beveiligingsproblemen in een webapplicatie met behulp van tools zoals Burp Suite.
3. Bespreekt de voor- en nadelen -- evenals de geschiktheid -- van het toepassen van een bepaalde security tool binnen de ontwikkelcyclus van software.
4. Voert een architectural security risk assessement (d.w.z. design review) uit van een software-centric systeem met behulp van een threat modelling methode zoals Microsoft's DFD-gebaseerde STRIDE.
5. Voert een architectural privacy risk assessment (d.w.z. design review) uit van een software-centric systeem met behulp van een threat modelling methode zoals DistriNet's DFD-gebaseerde LINDDUN.
6. Pleit voor en tegen een claim die de verantwoordelijkheid van ontwikkelaars beschrijft voor het aanpakken van security problemen binnen een bepaald systeem.
7. De student kan zich mondeling en schriftelijk uitdrukken in het Engels (B2) in een professionele IT context;
8. De student past ethische standaarden toe en betrekt maatschappelijk ethische thema’s in de oordeelsvorming

Inhoud

Dit vak gaat over software security en heeft als thema "software quality in cyber-physical systems". Nu embedded systems steeds vaker aan het internet gehangen worden (ook wel het Internet of Things of IoT geheten), wordt het steeds belangrijker dat de firmware van deze apparaten van voldoende kwaliteit is. Binnen dit vak zullen we kijken naar hoe de kwaliteit van embedded software te verbeteren is, met de nadruk op security. Casussen zoals het op afstand hacken van een Jeep, het platleggen van cloud providers met een "bot army" van IP camera's, en het hacken van een casino via een "smart fish tank" geven aan hoe divers de threats zijn. De principes die in dit vak naar voren komen zijn zeer relevant voor software security en quality in de brede zin van het woord. De reden hiervoor is dat de problemen die we tegenwoordig in IoT apparatuur zien veel overeenkomsten hebben met de security problemen die we in de jaren 90 zagen in PCs. Ook toen werden basisprincipes van security niet toegepast bij het schrijven van software.

Opgenomen in opleiding(en)

HBO-ICT, Major Network & Security Engineering
HBO-ICT, Major Software Engineering

School(s)

Instituut voor Communicatie, Media & IT