Hanzehogeschool Groningen
University of Applied Sciences

Vak: Software Security — credits: 5

Vakcode	ITVP20SCY
Naam	Software Security
Studiejaar	2020-2021
ECTS credits	5
Taal	Nederlands
Coördinator	J.F. van der Lee

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. Kan Engels spreken en schrijven op CEFR B2 niveau.
8. Is in staat een root-cause analysis uit te voeren op een bestaand project en hierover een correct gestructureerd basis-rapport te schrijven.
9. Heeft zich toegelegd op het kritisch denken over filosofische theorieën betreffende de scheidingslijn tussen mens en machine (Turing test, Chinese room argument), de verantwoordelijkheden bij het toepassen van AI en IoT, en de implicaties van actor-network theory.

Inhoud

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. Kan Engels spreken en schrijven op CEFR B2 niveau.
8. Is in staat een root-cause analysis uit te voeren op een bestaand project en hierover een correct gestructureerd basis-rapport te schrijven.
9. Heeft zich toegelegd op het kritisch denken over filosofische theorieën betreffende de scheidingslijn tussen mens en machine (Turing test, Chinese room argument), de verantwoordelijkheden bij het toepassen van AI en IoT, en de implicaties van actor-network theory.

Opgenomen in opleiding(en)

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

School(s)

Instituut voor Communicatie, Media & IT