Threat Modeling

Project 3/4

Agenda

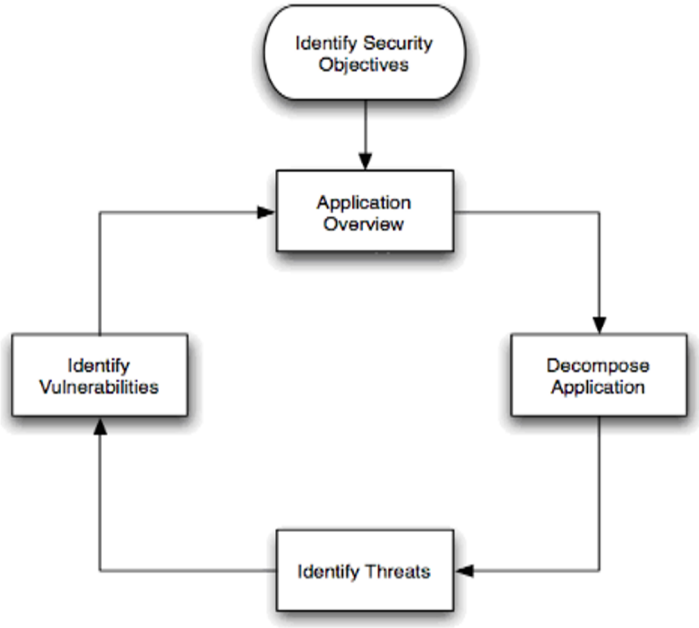
1. Intro
2. Oefening
3. Threat model
4. Threat analysis

Intro

Intro

- Securitydoelen
  - Confidentiality (Vertrouwelijkheid)
  - Integrity (Integriteit)
  - Availability (Beschikbaarheid)
  - Authentication (Authenticatie)
  - Authorization (Autorisatie)

- OWASP



Ontwerpen

Wie zijn de potentiële aanvallers? (Adversaries)

- Gebruikers
- Medewerkers
- System admins
- Hackers
- Dieven

Ontwerpen

Wat wil ik beschermen? (Assets)

- Klantgegevens
- Geld
- Producten
- Reputatie

Ontwerpen

Hoe kan ik het aanvallen?

- Man in the middle attack
- SQL injection op loginscherm
- …

Oefening

Oefening

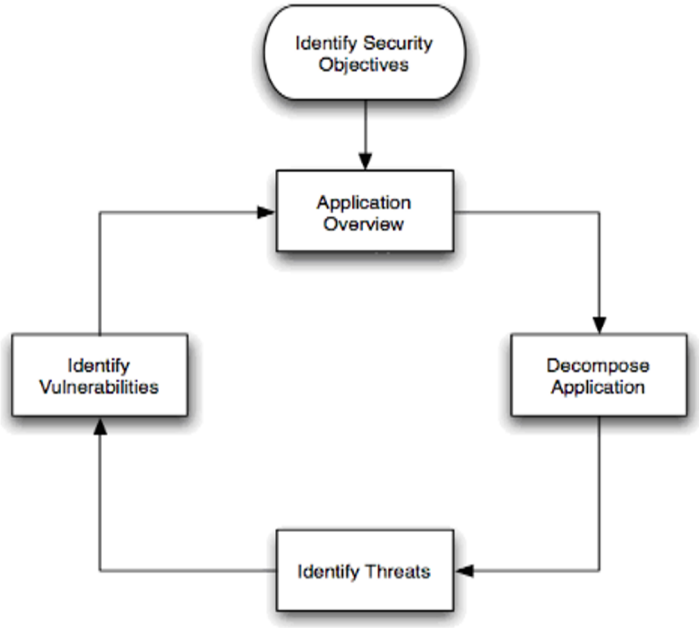
Zie de getekende plattegrond.

Tegen wie moet je je beschermen?
Wat valt er te halen?
Hoe kan iemand er bij komen?

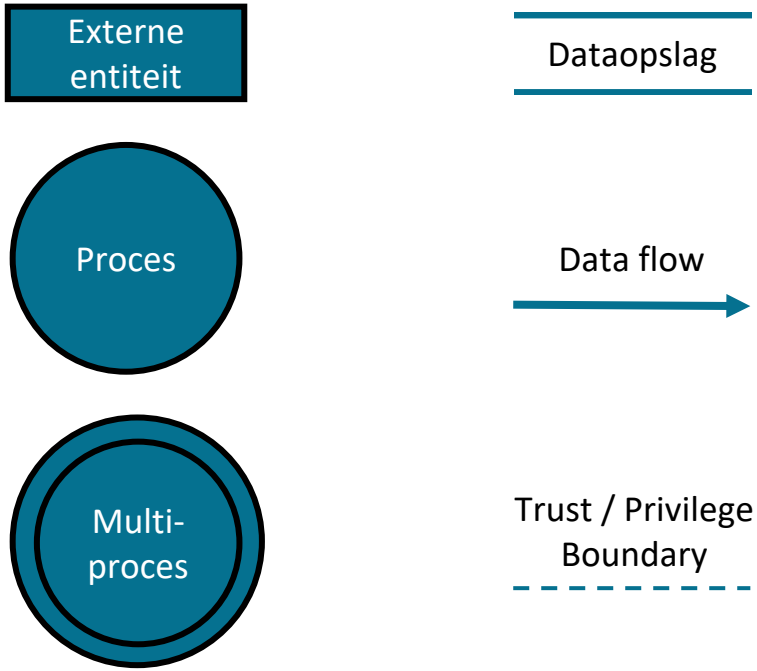
Threat model

De stappen

- De applicatie in kaart brengen
- Dreigingen identificeren
- Zwakheden identificeren
- Gevaren ranken

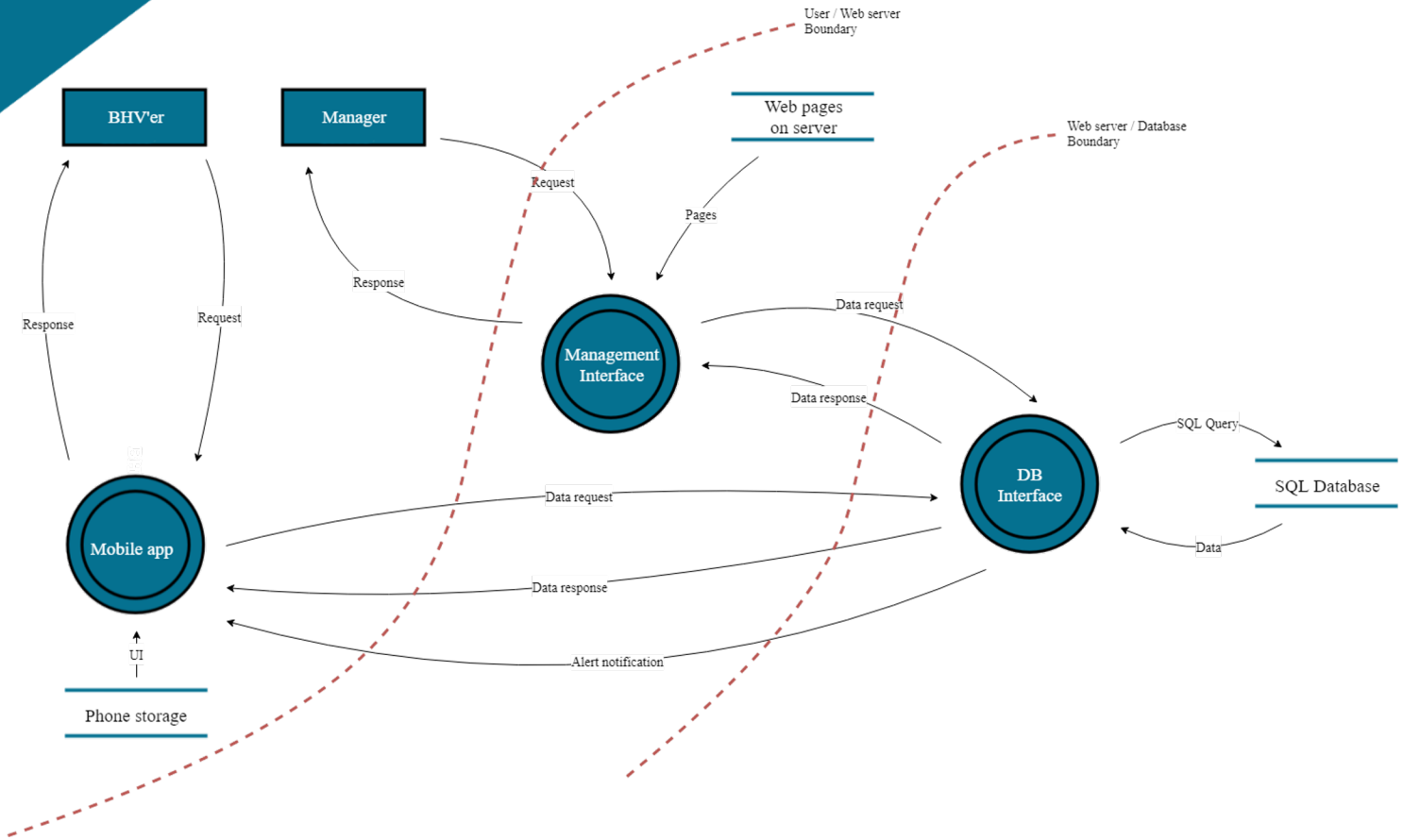


Threat model



Threat model

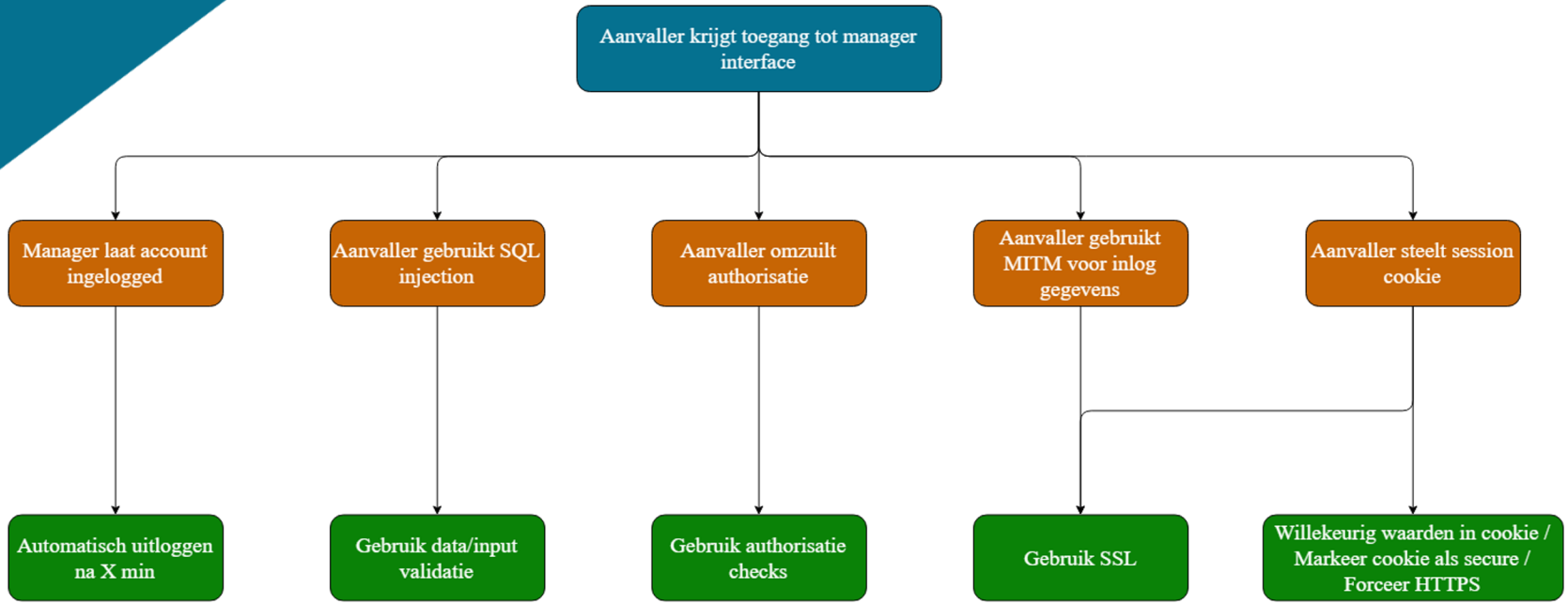
Data flow



Threat analysis

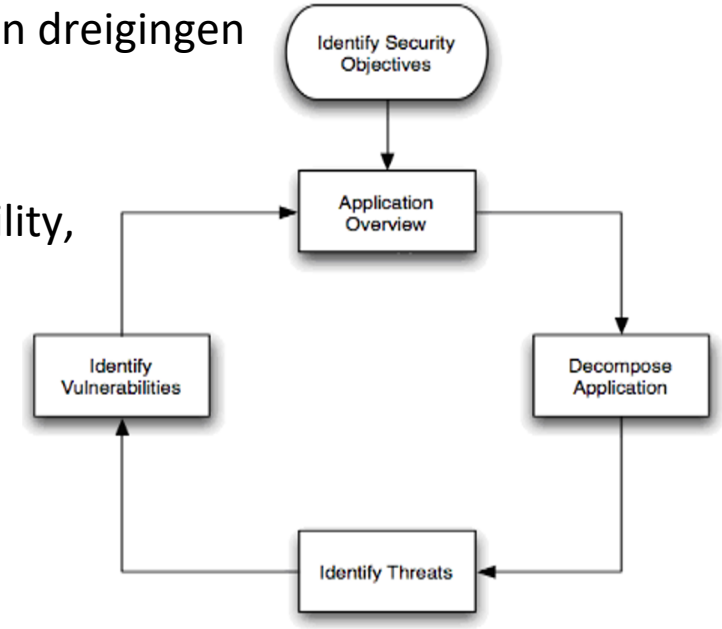
Threat analysis

Attack tree



The steps

- STRIDE
  - Spoofing, Tampering, Repudiation, Information Disclosure, DoS, Elevation of Privilege
  - Gebruikt voor categoriseren van dreigingen
- DREAD
  - Damage Potential, Reproducibility, Exploitability, Affected users, Discoverability
  - Ieder een cijfer geven 0-10
  - Gebruikt voor prioriteren van gevonden zwakheden



Nu jullie!

Breng je eigen bank in kaart!

Waar zitten de gevaren?

Zie de opdrachtomschrijving voor het beveiligingsplan op Praktijklink.

OWASP.org
OWASP Security Cheat Sheet (Git)
OWASP Security Cheat Sheet