Øvelse 3 - OWASP Top 10: Injection Sårbarheder

Formål

I denne øvelse vil du dykke ned i OWASP Top 10's kategori nummer 5, **Injection**. Målet er at forstå, hvad injection-sårbarheder er, hvordan de kan udnyttes, og hvilke sikkerhedsforanstaltninger der kan beskytte mod dem. Herudover er det en generel introduktion til begreber og termanologier.

Vi laver opsamling i klassen.

Instruktioner

1. **Forstå Injection-sårbarheder**
   Gå til OWASP Top 10 Injection og læs beskrivelsen af injection-sårbarheder.
   Opgave: Forklar med dine egne ord, hvad en injection-sårbarhed er, og hvordan den typisk kan udnyttes i webapplikationer. Giv eksempler på forskellige typer af injection-angreb, såsom SQL injection og command injection.
2. **Forståelse af Positive Server-Side Input Validation**
   Læs afsnittet *How to Prevent* på OWASP-siden om injection.
   Opgave: Forklar, hvad der menes med "positive server-side input validation" som en metode til at forhindre injection-angreb. Hvorfor er denne metode effektiv, og hvordan adskiller den sig fra "negative validation" (Blocklist)?
3. **CWE-20 - Improper Input Validation**
   Find afsnittet *List of Mapped CWEs* på OWASP injection-siden og læs om CWE-20.
   Opgave: Beskriv, hvad CWE-20 "Improper Input Validation" dækker over. Hvorfor er korrekt inputvalidering vigtig for applikationssikkerhed?

Links

- OWASP Top 10 Injection

Last update: 2026-09-07 05:23:23