Øvelse 51 – (Gruppeøvelse) Undersøgelse af CWE'er

Formål

Formålet med denne øvelse er at give jer en grundlæggende forståelse for, hvad **Common Weakness Enumeration (CWE)** er, og hvordan det bruges til at beskrive og klassificere typiske svagheder i IT-systemer. I skal som gruppe undersøge en række udvalgte CWE'er og formulere en kort konceptuel forklaring på, hvad hver enkelt dækker over.

Baggrund

CWE beskriver **svagheder** i softwaredesign, implementation og konfiguration, som kan føre til sårbarheder. I modsætning til CVE'er, som beskriver specifikke og konkrete sårbarheder i produkter, er CWE'er **generelle mønstre eller fejltyper**, som danner grundlag for mange CVE'er.

CWE bruges i bl.a. secure coding, sikkerhedstest og udvikling af værktøjer som SAST og DAST.

Instruktioner

I jeres gruppe skal I undersøge og forklare følgende CWE'er:

- CWE-20
- CWE-653
- CWE-287
- CWE-272
- CWE-1329
- CWE-306

For hver CWE skal I lave en **kort og præcis konceptuel forklaring** med fokus på:

- Hvad dækker svagheden over?
- Hvordan kan den føre til en sårbarhed?

- I hvilken kontekst opstår den typisk?

> Brug den officielle CWE-database til at finde beskrivelser og eksempler.

Nyttige links

- What is CWE?
- CWE-database (MITRE)

Refleksionsspørgsmål

- Hvordan adskiller CWE'er sig fra CVE'er?
- Hvilken rolle spiller CWE i udvikling og sikkerhedstest?
- Hvilke af de undersøgte svagheder vurderer I som mest kritiske – og hvorfor?
- Hvordan kan man anvende viden om CWE'er til at forebygge sikkerhedsproblemer?

2025-04-03 05:55:59