

Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utgave 2023

Universitetsforlaget



Oppgaver

Kapittel 11: Innebygd informasjonssikkerhet

Oppgave 1: Innebygd

- Hva menes med at informasjonssikkerhet og personvern skal være innebygd?
- Hvilke to veiledere/rammeverk fra Microsoft og Datatilsynet definerer en sammenfallende syvtrinns modell for innebygd informasjonssikkerhet (og personvern)?
- Nevn hva som bør gjøres generelt og hva en virksomhet bør gjøre for å sørge for god opplæring i informasjonssikkerhet (1. fase).

Oppgave 2: Sikker smidig systemutvikling

- På hvilken måte er smidig utvikling forskjellig fra systemutvikling med fossefallmetoden?
- Hvordan kan sikkerhet integreres i smidig systemutvikling?

Oppgave 3: Sikkerhet i skyen

- Nevn faktorer som kan bidra til bedre sikkerhet ved skyløsninger enn ved On-Prem.
- Nevn faktorer som kan bidra til dårligere sikkerhet ved skyløsninger enn ved On-Prem.
- Forklar meningen med venstreskift (Shift-Left) i DevSecOps.

Oppgave 4: Applikasjonssikkerhet og XSS

Du er medlem av en ny sosial plattform kalt FAGSNAKK utviklet av og for studenter ved universitetet hvor dere kan ha faglige diskusjoner, organisert med én side for hvert fag. En dag er FAGSNAKK-siden full av det samme kattebildet som (det ser ut som) har blitt postet av ulike brukere (inkludert deg), men alle nekter for å ha gjort det. En medelev mener at dette kan skyldes en XSS-sårbarhet i FAGSNAKK og at bildene er et resultat av et XSS-angrep.

- Hva et XSS-angrep?
- Hvordan kan XSS-angrepet beskrevet ovenfor vært gjennomført?
- Hvordan kunne angrepet på FAGSNAKK ha vært forhindre?