Forside

EKSAMEN

Emnekode: ITF25019

Emnenavn: Datasikkerhet i utvikling og drift

Dato: 24/05-2023

Eksamenstid: 09.00-13.00, 4 timer

Hjelpemidler: Ingen

Faglærer: Tom Heine Nätt

Verifiseringskode: A37FF

Om eksamensoppgaven:
Eksamenssettet inneholder **7** hovedoppgaver, der oppgavene igjen er delt i deloppgaver.
Hver hovedoppgave teller omtrentlig 1/7-del av totalen, med mulighet for noen mindre justeringer under sensuren basert på det eksakte omfanget til hver oppgave. **Karakter fastsettes imidlertid på basis av en helhetsvurdering av besvarelsen.**

Gjør dine egne forutsetninger dersom du mener noe er uklart. Husk å lese oppgavetekstene grundig, da det er informasjon som begrenser og forenkler oppgavene, samt informasjon om krav til besvarelsen. Besvar deloppgaver slik de er inndelt (dvs. ikke svar på a og b samlet).

Oppgavene kan svært gjerne besvares som punktlister (der hvert punkt er noen få setninger og hvert punkt er en vesentlig og selvstendig opplysning/prinsipp). Punktene kan være komprimerte, men ikke mer komprimerte enn at sensor forstår at du kan det som beskrives. Er det lettere å skrive en full tekst kan du også gjøre det, men pass da nøye på så det blir litt strukturert og ikke bare "masse tekst". Bruk av fet, kursive og understreking på vesentlige momenter vil lette lesingen både for deg selv og sensor.

Oppgavene vil bedømmes på hvilke hvilke momenter og prinsipper du trekker frem som viktige.

Det kan være fort gjort å bruke opp "for mye tid" på en oppgave, da enkelte oppgaver er ganske åpne. Sørg for å nøye fordele tiden din ut over de ulike oppgavene. Hver hovedoppgave bør ta omtrentlig 30 minutter å besvare.

Lykke til!

Sensurfrist: 14/06-2022

Karakterene er tilgjengelige for studenter på Studentweb.

1 Oppgave 1 - Software security

Du får nå i oppgave å lage en oppsummering av sikkerhetskonseptene *shift left* / *building security in* / *security by design*. **Konseptene er ikke helt overlappende, men like nok til at du i denne oppgaven kan håndtere de som noe felles.**

Du må som minimum forklare hva dette konkret innebærer, hvorfor det er (/kan være) en god ide, fordeler/gevinster og ulemper/utfordringer.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 15

2 Oppgave 2 - Logging

a) Beskriv hva hensikten og gevinstene med et *logg management system* er.

b) Hvilke hovedmetoder har man for å initiere logging i en applikasjon, og hvilke bruksområder har hver av de?

Med hovedmetoder i spørsmål b) menes ikke noe direkte teknisk i selve applikasjonen/loggingen/loggsystemer, men prinsipper/situasjoner/hendelser i applikasjonen som man kan initiere en logging med. I forelesning/forelesningsnotatene er dette omtalt som "triggere for logging".

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

3 Oppgave 3 - Content-Security-Policy

Oppgaven handler om content security policy - CSP (sikkerhetsstandard som ofte settes som en sikkerhetsheader).

a) Gi en oversikt over muligheter som CSP gir og hvorfor vi bør benytte dette (du kan unnlate sandbox-delen, som berøres i oppgave c).

b) I hvilken kontekst gir CSP beskyttelse (altså hvem beskytter det og i hvilke situasjoner).

c) Gi en spesifikk beskrivelse av funksjonaliteten *sandbox* i CSP. Berør også hvordan denne kan benyttes sammen med <iframe>-taggen.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

4 Oppgave 4 - Inputvalidering

a) Gi en oversikt over ulike former for inputvalidering. Både ned på konkrete metoder, men også overordnet i ulike prinsipper/inndelinger.

b) Drøft påstanden om at inputvalidering ikke bør være primærmetoden for å hindre angrep.

c) Skriv et regulært uttrykk for saksnummer på formen: Inntil 5 siffer (minimum 2), bindestrek to bokstaver (A-Z) og mulighet for punktum og èn bokstav (A-Z) til slutt. Altså er følgende gyldige saksnummer: 23-FD, 22322-AT, 654-DB.P og 55-KL.T

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

5 Oppgave 5 - Hardening

a) Beskriv kort hva som menes med prinsippet *hardening* (herding) og hvilke ulike tiltak (generelt beskrevet) det ofte innebærer.

b) Hvorfor er hardening nødvendig ut over slik tjenester og systemer leveres (default)?

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

6 Oppgave 6 - Skraping

a) Diskuter ulike måter skraping kan utgjøre en sikkerhetstrussel og hvorfor det ofte glemmes.

b) Gjør en oppsummering av mulige mottiltak mot skraping (både forhindre og redusere konsekvenser).

c) Diskuter kort hvordan og hvorfor mottiltakene i punkt b kan overlappe med beskyttelse mot DoS (du trenger ikke ta for deg hvert mottiltak, diskuter generelt)

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10

7 Oppgave 7 - Databaser

a) Hvorfor og hvordan ønsker man å benytte brukere og rettigheter i en database opp mot en applikasjon?
b) Hvilke muligheter ligger i de fleste databaser i forhold til rettigheter. Tenk gjerne også bredere enn selve rettighetssystemet, og angi hvordan man kan oppnå flere muligheter ved å kombinere rettighetssystemet og andre mekanismer i databasen.

Skriv ditt svar her

Format

Words: 0

Maks poeng: 10