Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 12: Applikasjonssikkerhet og GDPR

Spørsmål 1: Cyber Kill Chain

a. Hva er «Cyber Kill Chain»?
b. Forklar trinnene i Cyber Kill Chain.

Spørsmål 2: Spredning av nettverksormer

Forklar generelt hvordan nettverksormer sprer seg.

Spørsmål 3: Botnett-angrep

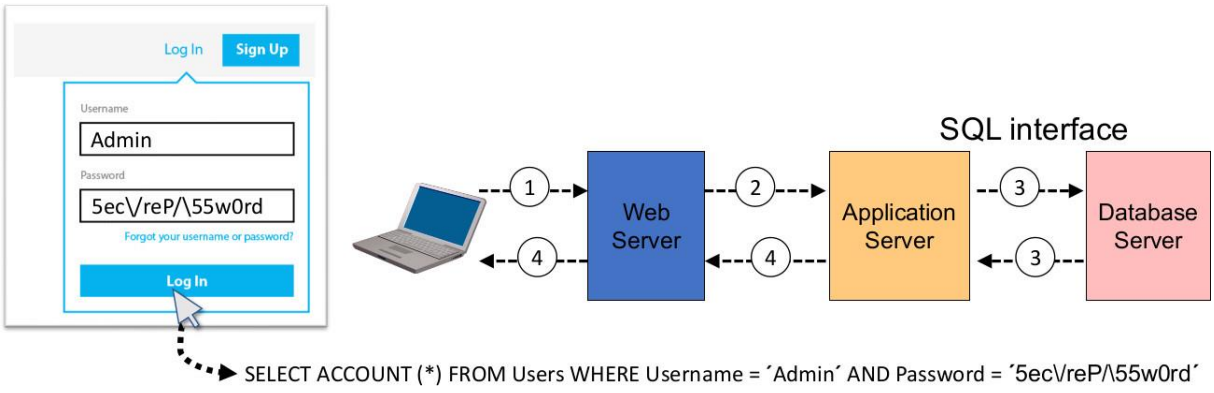
a. Hva er et botnett?
b. Hva er et DDoS, og hvordan kan et botnett brukes til å gjøre et DDoS-angrep?
c. Beskriver to andre angrep som kan utføres med botnett.

Spørsmål 4: SQL-Injeksjon

a. Hva er et SQL-injeksjonsangrep og hvordan kan det forhindres?
b. Hva er et XSS-angrep, og hvordan kan det forhindres?

Spørsmål 5: SQ-Injeksjon Eksempel

En web-applikasjon gjør brukerautentisering ved at inndata fra påloggingsskjermen brukes direkte uten filtrering for å danne SQL-kommandoer sendt til back-end SQL-database, som illustrert i figuren nedenfor. Logikken er at brukerautentiseringen er vellykket hvis det mottatte passordet er lik det lagrede passordet for den valgte brukeren.



En angriper ønsker å logge inn som Admin og skriver inn passordet: A´ OR ´X´ = ´X
a. Hva blir SQL-kommandoen som sendes til SQL-databaseserveren?
b. Hva er effekten av denne kommandoen?

Spørsamål 6: OWASP

a. Hva betyr forkortelsen OWASP ?
b. Hva er målsettingen til OWASP ?
c. Hva er "OWASP Top 10" ?
d. Hva er nr.1 i "OWASP Top 10" ?
e. Hvorfor har nr.1 vært på toppen av listen i så mange år ?
f. Hva er hensikten med OWASP ASVS ?

Spørsmål 7: Sikker Smidig

a. På hvilken måte er smidig forskjellig fra systemutvikling med fossefallmetoden ?
b. Hvordan kan sikkerhet integreres i smidig systemutvikling.

Spørsmål 8: Innebygd personvern og innebygd informasjonssikkerhet

GDPR (General Data Protection Regulation) ble satt ikraft som ny lov i EU den 25. mai 2018. GDPR oversatt til norsk kalles PVF (Personvernforordningen). Teksten i denne ble til den nye Personopplysningsloven som ble satt ikraft den 20. juli 2018.

a. Hva er hovedelementene for innebygd personvern i henhold til GDPR artikkel 5?
b. Hva er hovedelementene for utvikling og drift av IT-systemer i samsvar med innebygd personvern og innebygd informasjonssikkerhet ifølge Datatilsynets veileder?

https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/

Spørsmål 9: Personvern i skyen

Et IT-selskap som behandler persondata bestemmer seg for å overføre lagring og behandling av personopplysninger til en skytjeneste som ligger i utlandet.

a. Er dette lovlig i henhold til GDPR (Personopplysningsloven i Norge)?
b. Hva må selskapet gjøre for å gjøre outsourcing lovlig i henhold til GDPR?

Spørsmål 10: Straff for brudd på GDPR

a. To IT-selskaper, la oss kalle dem Alfa og Omega, utvikler hvert sitt IT-system som skal behandle persondata. Begge selskaper følger prinsipper (a)-(e) i artikkel 5 i GDPR. Alfa foretar ingen trussel/risikovurdering av sikkerhet under systemutviklingen, men systemet blir testet for kjente sårbarheter under drift. Omega, på den annen side, utfører trussel og risikovurdering av sikkerhet, og fjerner sårbarheter som blir oppdaget under utviklingen av systemet. Anta at begge IT-systemer, både det fra Alfa og Omega, blir hacket, noe som resulterer i sikkerhetshendelses med alvorlig personvernkonsekvens og lekkasje av sensitive personopplysninger. I henhold til Perwonopplysningsloven (GDPR), hadde Alfa og/eller Omega lov til å sette sine systemer i drift?
b. Kan Alfa og/eller Omega bli bøtelagt etter Personopplysningsloven (GDPR) som følge av sikkerhetshendelser og/eller som følge av hvordan systemene ble utviklet/driftett?
c. Hva er maksimal bøtelegging for brudd på Personopplysningsloven (GDPR) ?