Innføring i Datasikkerhet 2023 – Sensorveiledning

Dette dokumentet er ment som en veiledning for sensurering av eksamen i kurset Innføring i Datasikkerhet våren 2023. Dokumentet er likevel ikke en fasit på eksamensoppgavene og sensor er fri til å benytte egen bedømmelse ved vurdering av individuelle oppgaver hvis vedkommende anser det nødvendig.

Generell informasjon

Eksamensoppgaven består av 3 deler som teller forskjellig mot helhetsvurderingen:

- Del 1 – Sant/Usant - 30%
- Del 2 – Flervalg – 15%
- Del 3 – Skriftlig besvarelse – 55%

Av disse er Del 1 og 2 automatisert i henhold til poengutgivning, men kandidatene har muligheten til å kommentere på oppgaver de anser som uklare. Hvis det oppdages slike uklarheter, kan poenguttelling eller karaktergrenser justeres for å kompensere.

Del 3 består av 5 oppgaver hvor kandidatene selv skal formulere besvarelser. Som utgangspunkt skal hver av oppgavene telles like mye mot den totale 55% av delen, altså 11%, men vektlegging av individuelle oppgaver kan justeres noe hvis det anses hensiktsmessig. Spesifikke retningslinjer for sensur av disse oppgavene er beskrevet i seksjonene under, men det er her generelt viktig at kandidatene viser evne til å forklare, begrunne og drøfte for å få uttelling. Svar som "Fordi det er farlig", eller lignende, er dermed ikke tilstrekkelig. Kandidatene bør også belønnes for å lage strukturerte og gode besvarelse da å evne til å disponere/organisere/formulere innholdet samtidig viser høy grad av kunnskap. Utover dette er det ikke en forventning til at kandidatene skal skrive altomfattende besvarelser. Mange av oppgavene er åpne nok til at man kan vise meget mange eksempler eller diskutere veldig mange vinklinger. I slike tilfeller er det ikke forventet at kandidatene skal dekke alle disse for å få full uttelling, men det er viktig at de demonstrerer noen forskjellige for å vise at de har en overordnet god forståelse.

Den endelige karakteren for en gitt kandidat fastsettes basert på en helhetsvurdering av kandidatens besvarelse av oppgavesettet. Helhetsvurderingen skal i utgangspunktet vektlegges i henhold til prosentfordelingene av de 3 delene, men den nøyaktige vektleggingen kan justeres hvis dette anses å være hensiktsmessig for å balansere oppgavesettet. Alternativt, og mer vanlig, er imidlertid å justere karaktergrensene, som tar utgangspunkt i det følgende:

- A – 90% - 90 poeng
- B – 80% - 80 poeng
- C – 60% - 60 poeng
- D – 50% - 50 poeng
- E – 40% - 40 poeng

Del 1

Det følgende er svarene på oppgavene i Del 1. Riktig svar gir 1 poeng, feil gir -0.5:

1. Begrepet *ARP-spoofing* er forbundet med en type man-in-the-middle-angrep som kan utføres internt i et nettverk.- **Sant**

2. Dersom en nettside benytter HTTPS er det nesten garantert at nettsiden IKKE er svindel. - **Usant**

3. Begrepene *white hat*, *gray hat* og *black hat* benyttes til å klassifisere hackeres kompetansenivåer. Spesifikt betegner white hat en uerfaren og offentlig ukjent hacker, en gray hat har noe erfaring og er offentlig kjent for enkelte angrep, mens en black hat er en meget erfaren hacker som er godt kjent både innenfor hackermiljøer og utenfor. - **Usant**

4. Å benytte POST som overføringsteknikk i HTTP forhindrer avlytting av dataene, selv uten kryptering. - **Usant**

5. *Port scanning* handler om/innebærer å avsløre hvilke tjenester som kjører på en maskin.- **Sant**

6. Kryptering kan benyttes for *signering* ved at avsender krypterer en melding med sin private nøkkel, og videre for *verifisering* ved at mottaker dekrypterer meldingen med avsenders offentlige nøkkel. - **Sant**

7. Sikkerhetstjenestene *authentication* (autentisering) og *access control* (tilgangskontroll) omhandler det samme, men authentication er vinklet mer mot innlogging, og access control mot fysisk tilgang og dørlåser. - **Usant**

8. *Simple Network Management Protocol* (SNMP) og er en protokoll for hvordan nettverk-kommunikasjon bør struktureres i henhold til nettverkspakker for å forhindre/redusere avlytting av innhold. - **Usant**

9. Trådløse nett har gjennom tidene hatt diverse protokoller for kryptering. Disse er hovedsakelig WEP, WPA, WPA 2 og WPA 3. Av disse er WPA 2 den som er mest benyttet i dag. - **Sant**

10. En DMZ, eller *demilitarized zone* (demilitarisert sone), er et prinsipp som handler om å skille de offentlige delene av et system (slik som offentlige nettsteder) og de private delene (skal bare være tilgjengelig for systemeiere). Skillet gjøres ofte med brannmurer. - **Sant**

11. Kryptering kan være en effektiv mekanisme for å oppnå sikkerhetstjenesten *tilgjengelighet*. - **Usant**

12. DNS er en grunnleggende, men utdatert, funksjonalitet som inneholder sårbarheter for uautorisert fjernstyring av brukens datamaskin. - **Usant**

13. Når vi snakker om "IT-sikkerhet" omhandler dette kun hackerangrep/-forsøk gjort av personer med onde hensikter – **Usant**

14. Et *makrovirus* er en spesifikk type datavirus som ofte har vært basert på å inkludere skadelig kode i makrodokumenter, altså tekstdokumenter som inneholder et script som kjøres når dokumentet åpnes. - **Sant**

15. En *logic bomb* (logisk bombe) er en betegnelse som beskriver en skadevare som først ikke har (eller har få) skadelige effekter, men som aktiveres for full effekt på et senere tidspunkt. Dette kan for eksempel være basert på et definert tidspunkt eller en dynamisk hendelse. - **Sant**

16. Smarttelefoner kan, på grunn av måten de er utviklet, ikke bli infisert av skadevare. - **Usant**

17. Backups kan benyttes som en metode for å regelmessig kontrollere om et system er blitt infisert av skadevare. - **Sant**

18. Samtidig som du besøker en nettside i nettleseren din kan du potensielt også gi fra deg informasjon, slik som type maskin/system du benytter og hvilken nettside du var på før dette besøket. - **Sant**

19. For å innføre sikkerhet ved oversending av *cookies/informasjonskapsler* kan vi blant annet aktivere attributten HTTPOnly. Denne attributten forhindrer slikt som JavaScript-kode fra å hente ut informasjonen. - **Sant**

20. *Botnet* er en betegnelse for et type hackerkontrollert trådløst nettverk med en rekke falske tilkoblede enheter ("bots") som stjeler informasjon fra ekte enheter koblet til det samme nettverket. - **Usant**

21. Når vi snakker om et *passivt angrep* i datasikkerhet, betyr det at angrepet ble utført med uhell. Et eksempel på dette kan være at en ansatt med uhell offentliggjør hemmelig informasjon fra bedriften sin. - **Usant**

22. *Multi-faktor-autentisering* (MFA) fjerner fullstendig risikoen for *phishing*-angrep relatert til tjenester hvor MFA er innført. - **Usant**

23. At en epost er pen i utseende, med farger, logoer, spesialtilpassede fonter og så videre, er en god indikasjon på at eposten er ekte og ikke svindel. - **Usant**

24. Ved å benytte utviklerpanelet i nettleseren (typisk F12-tasten) kan man endre kildekoden (HTML/CSS/JS) bak en nettside vi besøker. Dette kan potensielt benyttes til å omgå eventuelle sikkerhetstiltak og begrensinger som er innført i nettsidens frontend, spesielt hvis det ikke er tilsvarende sikkerhetstiltak i backend. - **Sant**

25. En av de store fordelene med å benytte VPN er at du alltid er fullstendig anonym. - **Usant**

26. Ordet "hacker" hadde originalt ingen direkte kobling til kriminelle handlinger, men betegnet generelt en kompetent, dedikert og nysgjerrig person, oftest uten onde intensjoner. - **Sant**

27. Begrepet *script kiddie* betegner en type script med skadelige effekter for maskinen som kjører det. Script av denne typen skiller seg fra andre script i at de er små i størrelse og generert med ferdiglagde verktøy. - **Usant**

28. Metadata i bildefiler kan potensielt inneholde informasjon som kan benyttes til sporing, for eksempel den nøyaktige lokasjonen bildet ble tatt. - **Sant**

29. *Salting* er en teknikk som kan benyttes ved passordhashing for å redusere farene for *rainbow table*-angrep. - **Sant**

30. Å gjøre en ressurs vanskelig å finne (*security by obscurity*), for eksempel ved å gjøre en nettside kun tilgjengelig gjennom direktelenke, er et meget godt sikkerhetstiltak for å unngå uautorisert tilgang. - **Usant**

Del 2

Det følgende er riktige svar på "Velg en"-oppgavene. Riktig svar gir 1 poeng, feil svar gir 0 poeng.

1. Hvilket alternativ beskriver best begrepet *innsider*?

- En bit med kode eller ett program, som tillater en hacker å fjernstyre PC-en din.
- **En person på innsiden av en bedrift, oftest en ansatt, som aktivt utfører skadelige handlinger mot bedriften.**

- Dette er hva en hacker som med suksess har brutt seg inn i et system, og er nå på "innsiden", kalles.
- Et program som virker ekte og troverdig, men som inneholder skadelig kode.

2. Hvilket alternativ beskriver best begrepet *phishing* (nettfiske)?

- **En teknikk som lokker/lurer brukere til å oppgi informasjon de ellers ville holdt hemmelig.**
- En teknikk hackere benytter under avlytting av informasjon til å filtrere akkurat det de er ute etter.
- En søketeknikk hackere kan benytte for å samle informasjon på internettet om et potensielt angrepsmål.
- En teknikk hackere kan benytte for å knekke krypterte meldinger over nett, som er basert på å "fiske" frem velkjente/typiske deler av meldingen.

3. Hvilket av de følgende alternativene er IKKE en teknikk benyttet for håndtering av *risiko*?

- Risikoreduserende tiltak
- **Risikoforhandling**
- Risikoaksept
- Risikooverføring

4. Hvilket av de følgende alternativene beskriver best begrepet *hoax*?

- Dette er hva vi kaller en tidligere sikkerhetstrussel som har blitt avdekket å egentlig være harmløs.
- Navnet på et verktøy i kali som kan benyttes av svindlere/hackere for å kartlegge aktuelle mål.
- En type skadevare som sender brukeren falske advarsler med jevne mellomrom.
- **En strategi svindlere/hackere kan benytte for å lure ofre til å selv ta kontakt**.

5. Hvilket av de følgende alternativene passer best for å beskrive begrepet *personvernombud*?

- Et personvernombud er en person fra Datatilsynet som regelmessig besøker en organisasjon for å kontrollere at personvernregler følges riktig.
- "Personvernombudet" er navnet på et lovverk som angir retningslinjer for personvern i en organisasjon, samt konsekvensene ved brudd.
- **En rolle i en organisasjon hvor den ansatte med denne rollen er ansvarlig for å gi organisasjonen råd i henhold til personvern og GDPR.**
- Et personvernombud betegner en type bot som kan utgis til organisasjoner som har brutt GDPR.

6. Hvilket av de følgende alternativene er IKKE et aspekt som er dekket i GDPR?

- Alle tjenester skal ha en personvernserklæring som er skrevet til å være forståelig for alle som leser den.
- Bedrifter underlagt GDPR er pålagt å gjennomføre vurderinger av risiko og konsekvenser.
- Brukere av en tjeneste skal alltid ha muligheten til å hente ut og slette alle personopplysninger lagret av tjenestens produsent/bedrift
- **Ved et hackerangrep er bedriften som er blitt angrepet ansvarlig for å spore opp hackeren(e) og legge frem bevis for politiet.**

7. Gitt den følgende beskrivelsen, hvilket av alternativene under passer best? - "En type skadevare som er et selvstendig program og sprer seg helt på egenhånd, for eksempel ved å automatisk sende mail med seg selv som vedlegg".

- Rootkit
- Trojaner
- **Orm**
- Virus

8. Hvilket av de følgende alternativene beskriver best *signaturbaserte teknikker* i sammenheng med antivirusprogramvare?

- Skadevare oppdages ved å kjøre den undersøkte programvaren i et kontrollert og isolert miljø og analysere hvordan den oppfører seg, sammenlignet med hvordan skadevare typisk oppfører seg.
- **Skadevare oppdages ved å gjenkjenne kodesekvenser, eller annet fil-innhold, som tidligere er dokumentert til å være skadevare.**
- Skadevare oppdages ved å kontinuerlig sammenligne nåværende systemfiler med slik de var på et tidligere tidspunkt. Hvis uventede endringer har forekommet, flagges dette som potensiell skadevare.
- Skadevare oppdages/unngås hovedsakelig av brukeren ved at antivirusprogramvaren tilbyr brukeren innsikt og statistikk over slikt som forskjellige typer skadevare, kjente infiserte produkter og typiske infeksjonsmetoder.

9. Hvilket av alternativene under passer best til å beskrive begrepet *whitelist*?

- En liste over "farlige" tegn vi må oversette eller fjerne ved input-validering.
- **En liste over programmer, nettsider, funksjoner eller lignende, som er tillatt å benytte. Alt annet er ikke tillatt som standard.**
- En liste over brukere som er ekstra sikkerhetskritiske og som derfor krever flere sikkerhetstiltak
- En liste over tjenester/nettsider som aldri har blitt hacket.

10. Hvilket av alternativene beskriver best begrepet *spoofing*?

- **At noe (eller noen) utgir seg for å være noe annet enn hva som er tilfellet**
- At en sårbarhet eller et sikkerhetshull utnyttes for å utføre et angrep.
- At pakker og informasjon som går over nettrafikk blir overvåket.
- At tilgangrettighetene for en eller flere brukere blir endret av hackere.

11. Hvilket av alternativene er generelt et godt sikkerhetstiltak brukere kan gjøre mot *Cross Site Request Forgery* (CSRF/Webtrojaner)?

- **Logge ut av tjenester når man ikke benytter dem**
- Jevnlig slette aktivitetslogger i nettleser og tjenester
- Avinstallere alle nettlesertillegg (plugins)
- Benytte Tor-browser for nettsurfing

12. Hvilket av alternativene passer best for å beskrive begrepet *denial of service* (DoS)?

- **Et type angrep som gjør en tjeneste midlertidig eller permanent utilgjengelig.**

- Et lovmessig brudd på systembrukeres rettigheter, hvor brukere ikke har fått eller har mistet tilgang til en tjeneste de har betalt for.
- En metode hackere benytter for å skjule seg selv etter angrep, ved å stenge ned alle maskiner som ble benyttet i angrepet.
- En teknikk tjenesteprodusenter kan benytte ved et oppdaget hackerangrep, hvor hackerene blir utestengt fra å benytte tjenesten videre.

Det følgende er svarene på "Velg en eller flere"-oppgavene. Avkrysning på ALLE riktige besvarelser gir 1 poeng, ellers 0 poeng:

13. Hvilke av alternativene under kan bli benyttet som faktorer i *multi-faktor-autentisering*? (For kontekst: De riktige alternativene er faglig etablerte faktorer og er ikke en tolkningssak.)

- **Noe du HAR**
- Noe du GJØR
- **Noe du ER**
- **Noe du VET**

14. Hvilke av alternativene under er aspekter/angrep en VPN kan beskytte mot?

- Drive-by-download
- Falske plugins (utvidelser) i nettleser
- **Falske/usikrede nettverk**
- Svindelstrategier

15. Hvilke av alternativene under er aspekter i den generelle oppbygningen av en skadevare?

- **Stridshode (Warhead)**
- Integritet (Integrity)
- **Spredning (Propagation)**
- **Nyttelast (Payload)**

Del 3 - Oppgave 1 – Sletting av data

Oppgaven er delt opp i 3 deloppgaver som i utgangspunktet skal vektlegges like mot oppgavens totale uttelling (11 poeng). Vektlegging av deloppgavene kan likevel justeres hvis dette anses hensiktsmessig.

a) Forklar hvorfor det er vanskelig å slette digital informasjon/data fra slikt som harddisker, SSD-er eller andre lagringsmedier.

Her der det viktig av kandidaten klarer å overordnet forklare hvordan slike lagringsmedier lagrer data. Altså at dataene skrives til disk og at det lages en (fil)tabell med oversikt over hva som ligger hvor. Det kan her være fordelaktig (men ikke fullstendig nødvendig) om kandidaten også klarer å sette dette i en kontekst for å enkelt demonstrere dette. For eksempel: "Vi lagrer en fil på 3000 bit. Dette skrives til disk fra en ledig posisjon og tabellen oppdateres for å reflektere dette, med filnavn, startposisjon, størrelse og filsti (bare for visning i operativsystemet).

Videre er det vesentlig at kandidaten kan forklare greit teknisk at hvis man sletter data fra disk vil typisk bare informasjonen i tabellen slettes. Altså vil vi miste oversikt over nøyaktig hvor den "slettede" filen ligger på disk, men filen vil teknisk sett fremdeles være lagret (inntil den blir

overskrevet av noe nytt). Utover dette har vi ingen kontroll over hvor ny data blir satt inn. Dermed er det meget vanskelig å forsikre at data faktisk er slettet med denne metoden alene. Enkle utsagn som at "det blir igjen", "vanskelig å slette skikkelig" osv gir i seg selv lite uttelling.

Det følgende kan være vanlige feil i besvarelser:

- Forklarer at data slettes fra disk, men blir igjen i filtabellen, og at et wipe-verktøy fjerner oppføring fra filtabellen. Altså at kandidaten sier motsatt fra det som er tilfellet.
- Snakker kun om filer i mappestruktur vs. filer i "papirkurv"

b) Drøft hva har dette å si for slikt som gjenbruk/salg og kasting/avhending av brukte lagringsmedier (eller enheter som inneholder lagringsmedier).

Her bør kandidaten forklare at det fort kan bli problematisk å kvitte seg med lagringsmedier fordi dataene fortsatt kan ligge igjen, samt at det finnes verktøy som er i stand til å gjenopprette disse. Kandidaten bør også kunne drøfte at slikt som personlig/sensitiv informasjon, hemmelig bedriftdata eller annen praktisk nyttig informasjon kan komme på avveie. Generelt bør man ikke gi fra seg/selge utstyr med datalagring. Alternativt kan man fjerne lagringskomponentene fra utstyr som skal gjenbrukes der dette er mulig.

c) Forklar hva som må til for at dataene faktisk skal bli "slettet" (eller praktisk oppnå samme effekt), og gi noen råd til hvordan man kan oppnå dette.

Her bør kandidaten i det minste drøfte at dataene må overskrives fullstendig for at de skal være "slettet", samt at det finnes formateringsverktøy som kan gjøre dette (for eksempel tilfeldige 0-ere og 1-ere på hele disken). Alternativt kan man gjøre dette mer manuelt. For eksempel ved å først slette dataene på normal måte og deretter fylle opp disk med noe ubetydelig (video med blank skjerm). Disse kan dermed være råd. Et annet alternativ er å fullstendig ødelegge utstyret (kverne opp eller knuse), men dette betyr ikke nødvendigvis at det umulig å gjenopprette dataene. Det sikreste kan dermed være å kombinere alle alternativene.

Vanlige feil:

- Råd lignende "Se i filutforskeren om du fremdeles kan se filene. Hvis filene ikke er synlige, er dataene fjernet."

Del 3 - Oppgave 2 – Cookies og Sessions

Oppgaven er delt opp i 3 deloppgaver som i utgangspunktet skal vektlegges like mot oppgavens totale uttelling (11 poeng). Vektlegging av deloppgavene kan likevel justeres hvis dette anses hensiktsmessig.

a) Forklar hva en *cookie/informasjonskapsel* er, og overordnet hvordan/hvorfor disse er relevante for sikkerhet.

Kandidaten kan her trekke frem at disse er informasjon som lagres lokalt i brukerens nettleser for hver nettside og benyttes typisk for at nettsider/nettjenester skal kunne huske og gjenbruke slik informasjon mellom besøk på nettsiden (ofte for brukeropplevelse). Det er her positivt om kandidaten nevner noen typer informasjon og overordnet hvordan de brukes.

Disse er generelt relevante for sikkerhet fordi disse kan inneholde hemmelig/sikkerhetskritisk informasjon (positivt om kandidaten kan gi eksempler) som kan bli stjålet og benyttet videre. Utover dette, blir informasjonskapsler også ofte benyttet til former for overvåkning (lovlig og i grenseland), som fort kan gå utover brukerens personvern. Her kan det også være fordelaktig om kandidaten nevner GDPR.

b) Forklar videre hva en *session* er og den overordnede prosessen av hvordan disse blir opprettet og lukket.

En session er mest essensielt tilfeller hvor cookies blir benyttet for å autentisere brukeren. Ofte for å huske at brukeren er innlogget over en lengre tid, og underforstått automatisk logge brukeren inn hver gang dette er nødvendig. Sessions kan imidlertid også benyttes for ting som er uavhengig av innlogging og typisk mindre sikkerhetskritiske. Det typiske eksemplet er en handlevogn i nettbutikk, hvor brukeren, selv om de ikke er logget inn, kan legge til varer i handlekurven som vil huskes mellom besøk.

Sessions opprettes overordet (i tilfellet av innlogging-sesjon) ved at brukeren logger seg inn og blir autentisert av serveren. Serveren oppretter så en sesson-id som blir notert å være gyldig (ofte inntil et visst tidspunkt). Serveren sender session-id tilbake til brukeren og ber at denne blir lagret i en cookie (uavhengig av om dette er en innlogging-sesjon eller ikke). Ved videre bruk av tjenesten vil brukeren kunne benytte sesjonen til å autentisere seg ved å sende session-id til serveren, som sjekker om denne er gyldig. Er id-en gyldig anses brukeren å være autentisert.

En session kan lukkes ved at brukeren logger seg ut av tjenesten. Da vil serveren umiddelbart gjøre session-id-en ugyldig og/eller slette den. Videre forsøk på å logge inn med denne sesjonen vil dermed ikke være mulig. Alternativt kan sesjonen automatisk lukkes når gyldighetstiden utløper. Gyldighetstiden varierer for hver nettside/-tjeneste og typen sesjon. Mer sikkerhetskritiske sesjoner har ofte en kortere gyldighetstid.

c) Drøft ulike måter en *session* kan komme på avveie og hvilke negative konsenser dette kan medføre.

Det følgende kan være eksempler på måter en session kan komme på avveie:

- En session kan bli stjålet ved fysisk tilgang til en ulåst PC ettersom alle informasjonskapsler er lesbare i utviklerpanelet av nettleseren.
- "Falske" nettleser-plugins kan potensielt aksessere og videresende sesjoner til hackere.
- Det finnes diverse typer angrep som benytter skript til å hente ut/stjele informasjonskapsler, og dermed også sessions. For eksempel Cross Site Scripting (XSS). En annen variant er Cross Site Request Forgery (CSRF), som ikke direkte sjeler sesjonen, men som "lurer" brukeren til å automatisk utføre en handling i en tjeneste basert på en lagret og gyldig sesjon.
- Hvis nettverkskommunikasjonen ikke er kryptert kan sessions potensielt observeres i klartekst ved oversending.
- Svindlere kan lure brukere gjennom sosial manipulasjon til å gi fra seg en session-id ettersom disse typisk ikke gir mening for vanlige brukere.
- En session-id kan potentielt bruteforces/gjettes frem til av hackere hvis disse er generert på en forutsigbar måte.

De mest essentielle konsekvensene av en stjålet sesjon (session hijacking) vil være at hackeren/svindleren som får tak i denne også vil ha muligheten til å være innlogget som brukeren uten å vite brukernavn og passord. Dette kan overordnet føre til at konfidensiell informasjon blir lest eller at hackeren gjør handlinger på vegne av brukeren. Dette kan være enten former for direkte angrep, for eksempel slette brukens data eller spre svindel eller skadevare til brukenes venner. Det kan også være typer forangrep, for eksempel legge inn "bakdører" eller passivt følge med på innhold og handlinger (Meget interessant for angrep mot bedrifter).

Del 3 - Oppgave 3 – SQL injection

Oppgaven er delt opp i 2 deloppgaver som i utgangspunktet skal vektlegges like mot oppgavens totale uttelling (11 poeng). Vektlegging av deloppgavene kan likevel justeres hvis dette anses hensiktsmessig.

a) Forklar hva *SQL-injection* er og overordnet hvordan dette fungerer. Du kan gjerne også vise et eksempel eller to på relevante angrepsteknikker, men dette er ikke nødvendig for å få full uttelling.

En SQL-injection er et type angrep hvor hackere kan benytte inputfelter til å utføre egendefinert eller modifisert SQL-kode mot den bakenforliggende databasen. Dette kan være mulig å gjøre i tilfeller hvor innholdet av inputfeltene benyttes direkte i SQL-spørringer mot databasen. Hackere kan da benytte spesialtegn for å "escape" inputen, altså gjøre vanlig tekst til eksekverbar kode, og kan dermed legge til eller endre logikken av SQL-spørringen(e). Dette er imidlertid under forutsetning at det ikke gjøres former for inputvalidering som filtrer bort slike spesialtegn, eller som ellers filtrerer bort/blokkerer kode som gjenkjennes som SQL.

Enkle eksempler av teknikker for SQL-injection kan for eksempel leses om her: https://www.w3schools.com/sql/sql_injection.asp

Det er også forskjellige former for SQL-injection angrep, slik som In-band SQLi, Blind SQLi og Out-of-band SQLi. Det teller positivt om kandidaten nevner og diskuterer noen av disse, men det er ikke direkte forventet.

For å få god uttelling på denne oppgaven må kandidaten:

1) Koble trusselen mot nettsider med bakenforliggende databaser. Database må altså nevnes direkte eller indirekte.

2) Forklare at SQL-koden som skrives, for eksempel i inputfelt, er deler av SQL som settes inn i bakenforliggende SQL-spørring

3) Nettsiden må ha brukerinput som flettes inn i SQL-spørringer uten god nok inputvalidering.

Det er ikke tilstrekkelig å ha en forklaring lignende "Hackeren sender skummel SQL-kode til en server", som om dette går med enhver nettside.

b) Hva kan konsekvensene av en suksessfull *SQL-injection* være? Her er det mulig å tenke både generelt og konkret. Det viktigste er imidlertid å vise forskjellige vinklinger/kategorier, ikke å liste absolutt alle konkrete muligheter.

Konsekvensene av en suksessfull SQL-injection kan essensielt kategoriseres basert på CRUD-operasjoner (Create, Read, Update, Delete), men merk at det ikke er nødvendig at kandidaten strukturerer det slik, selv om det er fornuftig hvis de gjør det. Under er noen eksempler, men det kan være mange flere som er relevante:

- Opprette ny data:
    - Legge til ny bruker med admin-rettigheter
    - Legge til falsk informasjon.
- Lese data:
    - Lese konfidensiell data. (Kan være problematisk i seg selv, eller kan benyttes som innsikt til videre angrep)
- Endre data:
    - Endre rettigheter for sin egen bruker eller andres.
    - Endre passord på en adminbruker til noe man selv vet.
    - Endre data som benyttes andre steder i tjenesten for missledende effekter eller praktiske effekter. (For eksempel system-/tjenestekonfigurasjoner)
- Slette (Ofte for Denial of Service):
    - Slette rader i database (brukere, informasjon osv.)
    - Slette hele database-tabeller eller databasen i sin helhet

Del 3 - Oppgave 4 – Social Engineering

Oppgaven er delt opp i 2 deloppgaver som i utgangspunktet skal vektlegges like mot oppgavens totale uttelling (11 poeng). Vektlegging av deloppgavene kan likevel justeres hvis dette anses hensiktsmessig.

a) Forklar hva *social engineering* (sosial manipulasjon) er. Benytt gjerne eksempler og konkrete begreper for å demonstrere forskjellige former dette kan forekomme. Det er imidlertid ikke nødvendig å gå veldig dypt i hver form og du kan gjerne lage/vise kategorier.

Social Engineering/sosial manipulasjon kan enkelt forklares som psykologiske triks/teknikker sammen med (ofte) enkel teknologi som lurer brukere til å gjøre noe de ikke burde. Under er noen abstrakte aspekter som kan være relevante:

- Phishing/Spearphishing/Smishing - Svindlerene tar kontakt med ofre
    - Epost, meldinger, nettsider, telefon – Benyttes ofte til å lure ofre til å oppgi sikkerhetskritisk informasjon (innlogging, betalingsopplysninger, sensitiv/hemmelig informasjon, informasjon til videre angrep osv.)
    - Sprearphishing: Benytter personlig informasjon tilpasset for å gjøre innholdet av "meldingen" mer troverdig. Ofte mer effektiv en vanlig phishing.
- Lure brukere til å utføre handlinger
    - Endre konfigurasjoner/innstillinger i maskiner/systemer de administrerer – Kan være forangrep eller for direkte skade.
        - Åpne inngang/motta rettigheter som gjør det mulig å utføre ytterligere handlinger - forangrep
        - Installere skadevare, slette/endre data osv – mer direkte skadelig effekt
- Reverse social engineering – Lure/oppfordre ofre til å selv ta kontakt med svindlerne.
    - Hoax ("Du har virus! Søk hjelp her!")
    - Reklame for et "falskt" produkt/tjeneste.

b) Drøft forskjellige aspekter som ofte er inkludert i *social engineering* angrep og hvordan disse har en sammenheng med hvordan brukere kan beskytte seg selv mot slike angrep. Igjen; Det er ikke nødvendig å liste alt, men prøv å vise noen forskjellige kategorier.

Det følgende kan være overordnede eksempler på aspekter som ofte er inkludert i social engineering angrep:

- Troverdig utseende, innhold og/eller avsender (spoofing). Ofte basert på personlig tilpasset informasjon, slik at innholdet best passer og virker reelt.
- Spiller ofte på følelser eller fristelser (et resultat av kjærlighet, autoritet, økonomisk fortjeneste osv.).
- Skaper en situasjon som haster (for eksempel risiko av å miste penger).
- Forvirrende eller komplisert informasjon/begrunnelser (effektiv mot de med lav kompetanse/kunnskap).

Å beskytte seg handler mye om å være bevisst på kjennetegn og varianter av sosial manipulasjon og generelt tenke seg om før man gjør drastiske handlinger. Observer hvilke følelser som blir skapt i deg, og ikke la deg stresse på oppfordring. Utover dette, kan det følgende være noen eksempler på strategier for å beskytte seg:

- Vær kritisk, også til "ting" som ser reelt ut.
- God holdning: "Hvis det virker for godt til å være sant, så er det oftest det"
- Begrens tilgjengelig informasjon om deg selv på internett.
- Ikke trykk på lenker - Gå heller manuelt til den offentlige siden.
- Kontroller at slikt som domener av nettsider og innhold i mottatte meldinger er legitimt.
- Kontroller personene som tilsynelatende tar kontakt ved bruk av andre kommunikasjonskanaler.
- Søk opp og undersøk legitimiteten av eventuelle tjenester som er markedsført å skulle "hjelpe" deg.

Del 3 - Oppgave 5 – Minnepenn og Fysisk tilgang

Oppgaven er delt opp i 2 deloppgaver som i utgangspunktet skal vektlegges like mot oppgavens totale uttelling (11 poeng). Vektlegging av deloppgavene kan likevel justeres hvis dette anses hensiktsmessig.

a) Ta perspektivet av en hacker. Hvordan kan du benytte en minnepenn for å angripe en PC du har fysisk tilgang til. Her lønner det seg å tenke kreativt og diskutere forskjellige metoder. Det er også lov å gjøre forutsetninger, slik som hva for slags minnepenn dette er og hva brukeren/offeret gjør.

Under er en liste over eksempler på aspekter som kan diskuteres. Merk at det ikke nødvendigvis er forventet at kandidaten diskuterer alle for å få full uttelling, men bør likevel kunne vise en forståelse for en god del av dem, samt begrunne det som nevnes.

- Minnepenn med skadevare eller lignende
    - Virus, orm, rootkits osv.
    - Spyware (trafikk/handlinger)
- Minnepenn med annen skadelig effekt.

    - Keylogger (script eller spesiell minnepenn)
    - Passwordcracker (script)
    - Scanne og kopiere over filer fra maskinen (Podslurping)
    - Bootdrive med alternativt operativsystem - Gå forbi sikkerhet i det originale operativsystemet (typisk skjermlås). Hvis Kali Linux, eller lignende, kan også inneholdte verktøy benyttes for angrep.
- Hvis minnepennen er en rubberducky eller lignende
    - Utføre handlinger når den blir plugget inn (Kan være alt en bruker kan gjøre, men kan utføres mye raskere)
        - Alt i tidligere punkter
        - Gjøre handlinger på ting som ikke direkte ligger på maskinen – For eksempel navigere til en nettjeneste og utføre handlinger der
- Minnepenn spesialdesignet for å benytte kondensatorer og sende strøm tilbake i systemet
    - Ødelegge hardware.
- Andre teknikker (Krever ikke direkte fysisk tilgang)
    - Låne bort en minnepenn med enkelte av aspektene over
    - "Miste" en minnepenn på et sted hvor noen vil finne den. Det er stor sannsynlighet for at noen vil plugge den inn og interagere med innholdet - kjøre programmer/script.
    - Selge billige minnepenner på ett eller annet marked (for eksempel finn.no), men som egentlig har skadelige effekter.

b) Drøft hva kan en bruker gjøre for å beskytte seg mot angrep som benytter minnepenner (kan også gjelde andre USB-enheter). Diskuter gjerne i forhold til noen tiltenkte situasjoner

Under er en liste av aspekter som kan benyttes for å beskytte seg mot angrep som benytter minnepenner. Igjen er det ikke nødvendig at kandidaten diskuterer alle, men bør likevel kunne vise en forståelse for en god del av dem, samt begrunne det som nevnes:

- Essensielt former for fysisk sikring.
    - Låse inne utstyr når man ikke benytter det (kontor, skap, safe osv.)
    - Ikke gå fra utstyr, ta det heller med deg.
    - Benytt skjermlås.
    - Sjekk jevnlig etter ukjente USB-enheter som er koblet til maskinen.
- Hvis noen andre benytter pcen din (med eller uten minnepenn), følg veldig nøye med hva de gjør. Enda bedre, ikke la andre benytte PCen din. Det er mange angrep som ikke er synlige.
- Antivirus er lurt mot angrep som baseres på skadevare, selv om dette ikke er en garanti.
- Hvis du skal plugge inn en ukjent/risikabel minnepenn, plugg den inn i en test-PC eller virtuell PC. Ellers bør du ikke plugge inn ukjente USB-enheter i egen maskin.
- Du kan blokkere ukjente USB-enheter som standard (Kreve passord ved tilkobling). Eventuelt fysisk blokkere/låse ubrukte porter. USB-kondom for å ikke koble USB-enheten direkte i maskinen.
- Undersøk leverandører/selgere av minnepenner du vurderer å kjøpe. Hvor seriøse og etablerte er de?
- Ikke gjenbruk minnepenner du har mottatt fra andre personer. Kjøp heller en ny.
- Krypter sikkerhetskritiske filer/disker for å redusere faren ved for eksempel Podslurping.