IN1020

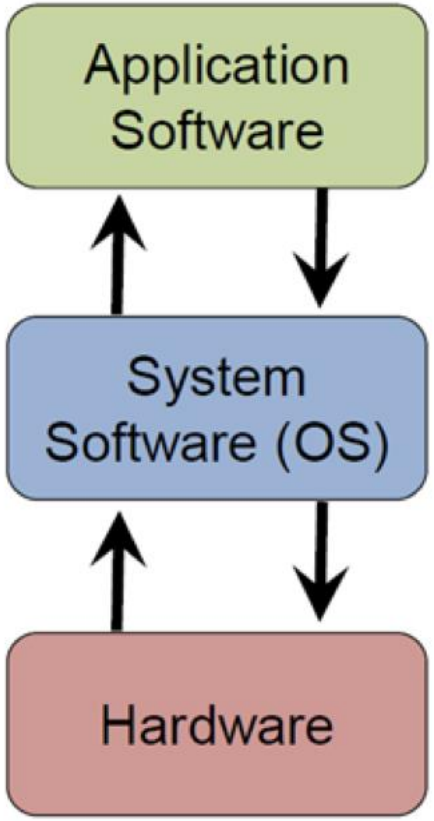
Gruppe 19

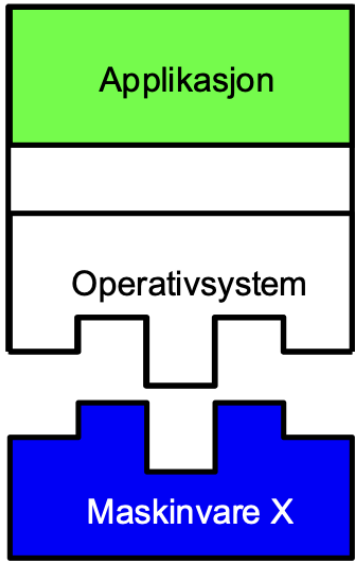
Plan for gruppetimen

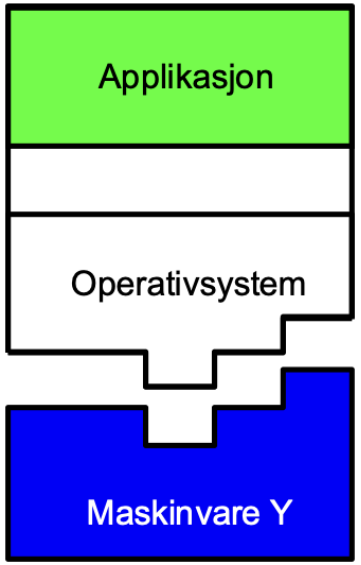
- Kort gjennomgang av forrige ukes pensum
  - Operativsystemer
  - Hvordan hackes vi?
- Quiz?
- Ukesoppgaver

Operativsystemer

- Et programvaresystem som fungerer som et **mellomlag** mellom maskinvaren i en datamaskin og brukeren/programmer, og som gjør det mulig å bruke maskinen på en **enkel**, **trygg** og **effektiv måte.**
- Vi har OS fordi vi ønsker:
  - Portable programmer
  - Å abstrahere bort maskinvaredetaljer
  - Dele ressursene i maskinen
  - Sikkerhet. Programmer skal ikke kunne se og forandre hverandres minneområder
- To perspektiver
  - Extended machine → gjemme unna detaljer om maskinvare så det blir enklere å bruke maskinen
  - Resource manager → deler ressursene mellom programmene som kjører på datamaskinen

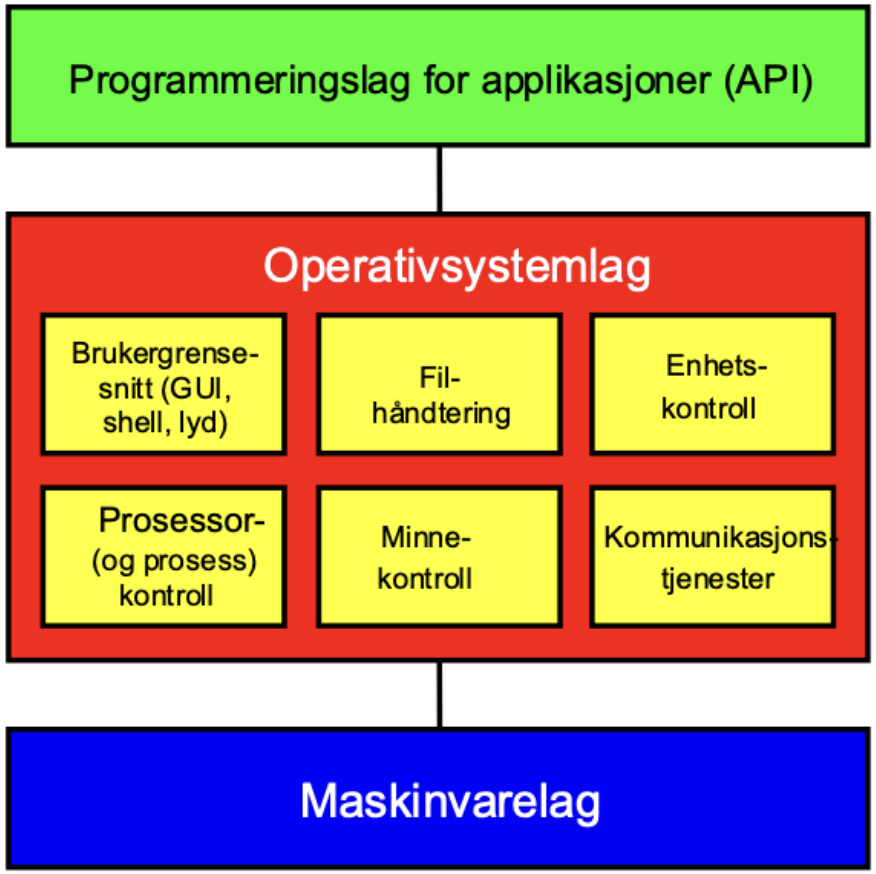






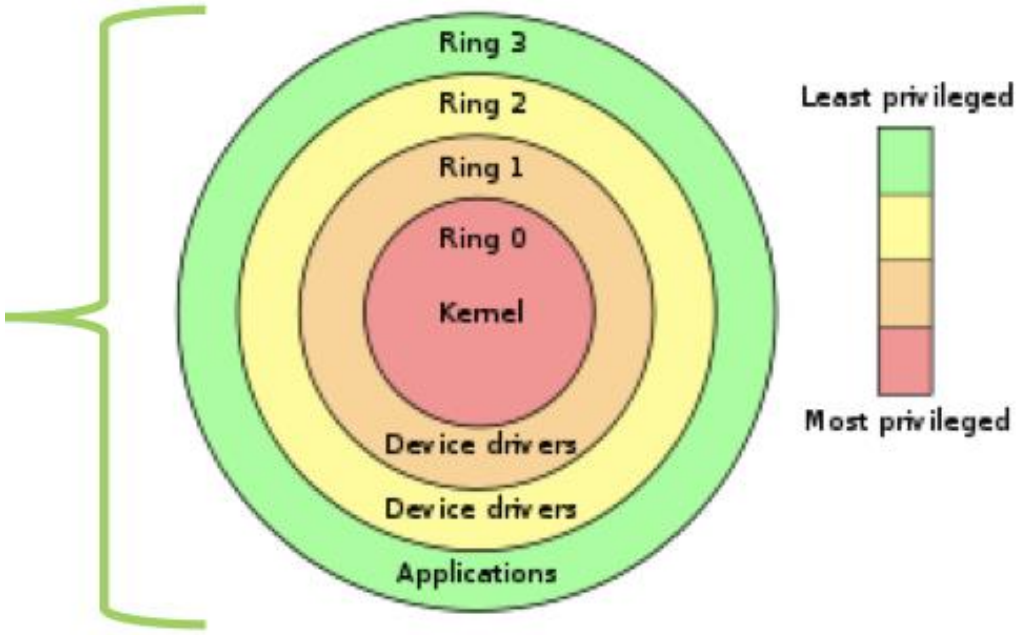
Hovedkomponenter

- Synlig for bruker:
  - Filhåndtering - Lagring, organisering og tilgang til filer og mapper
  - Enhetskontroll - Kontrollerer maskinvare som tastatur, skjerm, skrivere
  - Brukergrensesnitt - Kommunikasjon mellom bruker og system (f.eks. skrivebord, terminal)
- Ikke synlig for bruker:
  - Kommunikasjonstjenester - Håndterer datautveksling mellom prosesser og over nettverk
  - Minnekontroll - Fordele minneresurser og allokere plass til programmer
  - Prosesskontroll - Styrer kjøring av programmer og fordeler CPU-tid



Sikkerhet: Brukernivå vs. Kjernenivå

- Brukernivå
  - Vanlige programmer kjøres her
  - Kan ikke kontakte maskinvare eller enheter direkte, kun gjennom API
  - Begrenset tilgang til prosessoren
  - Begrenset tilgang til minneområder
- Kjernenivå - Kernel
  - Interne komponenter i OS-et kjøres her
  - Tilgang til hele minnet
  - Alle instruksjoner kan bli kjørt
  - Går forbi all sikkerhet



Overføringshastighet

Du ønsker å laste ned en fil på 150 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 20 megabit per sekund opp.

Hva er den teoretisk korteste overføringstiden?

Hvordan gå frem?

- Megabyte vs megabit
- Gjøre om byte → bit (*8)
- Skal vi laste ned eller opp?
- Dele størrelsen på hastigheten

Overføringshastighet

Du ønsker å laste ned en fil på 150 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 20 megabit per sekund opp.

Hva er den teoretisk korteste overføringstiden?

Hvordan gå frem?

- Megabyte vs megabit
- Gjøre om byte → bit (*8)
- Skal vi laste ned eller opp?
- Dele størrelsen på hastigheten

Overføringshastighet

Du ønsker å laste ned en fil på 150 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 20 megabit per sekund opp.

Hva er den teoretisk korteste overføringstiden?

Hvordan gå frem?

- Megabyte vs megabit
- Gjøre om byte → bit (*8)
- Skal vi laste ned eller opp?
- Dele størrelsen på hastigheten

Filen er 150 megabyte * 8 = 1200 megabit stor

1200 / 50 = 24 sek overføringshastighet

Overføringshastighet

Du ønsker å laste ned en fil på 150 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 20 megabit per sekund opp. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ:

- 150 sekunder
- 60 sekunder
- 3 sekunder
- 7,5 sekunder
- 24 sekunder ✔

Overføringshastighet

Du ønsker å laste ned en fil på 250 megabyte, og den maksimale nedlastingshastigheten på din Internettforbindelse er 25 megabit per sekund. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ:

- 25 sekunder
- 10 sekunder
- 120 sekunder
- 80 sekunder ✔

Overføringshastighet

Du ønsker å laste ned en fil på 800 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 25 megabit per sekund opp. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ:

- 60 sekunder
- 10 sekunder
- 32 sekunder
- 256 sekunder
- 128 sekunder

Overføringshastighet

Du ønsker å laste ned en fil på 200 megabyte, og den maksimale nedlastingshastigheten på din Internettforbindelse er 20 megabit per sekund. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ

- 100 sekunder
- 10 sekunder
- 5 sekunder
- 80 sekunder ✔
- 20 sekunder

Hvordan hackes vi?

- Sikker datalagring
- Nettverkssikkerhet
- Systemsikkerhet
- Applikasjonssikkerhet
- Sosial manipulasjon

Sikkerhet for data som lagres

- Kryptere dataen
  - Beskytte mot innsyn og endring
- Ta sikkerhetskopier
  - Lagres separat
- Redundante systemer
  - Et feiler? → et annet tar over
- Rutiner for sletting av data

Kommunikasjonssikkerhet

- Håndterer behovet for å sikre informasjon under overføring av data
  - Mellom ulike virksomheter
  - og noder innad i egen virksomhet
- F.eks komprimitterte eller falske aksesspunkter, ødelagte kabler, signalforstyrrelser

Datanettsikkerhet

- Skallsikring/perimeterforsvar
- Brannmur og inntregningsdeteksjon
- Beskytte virksomhetens dataressursser
  - Mot angrep
  - Og mot uautorisert tilgang fra omverden (internett)
- F.eks datatyveri, spionasje eller sabotasje

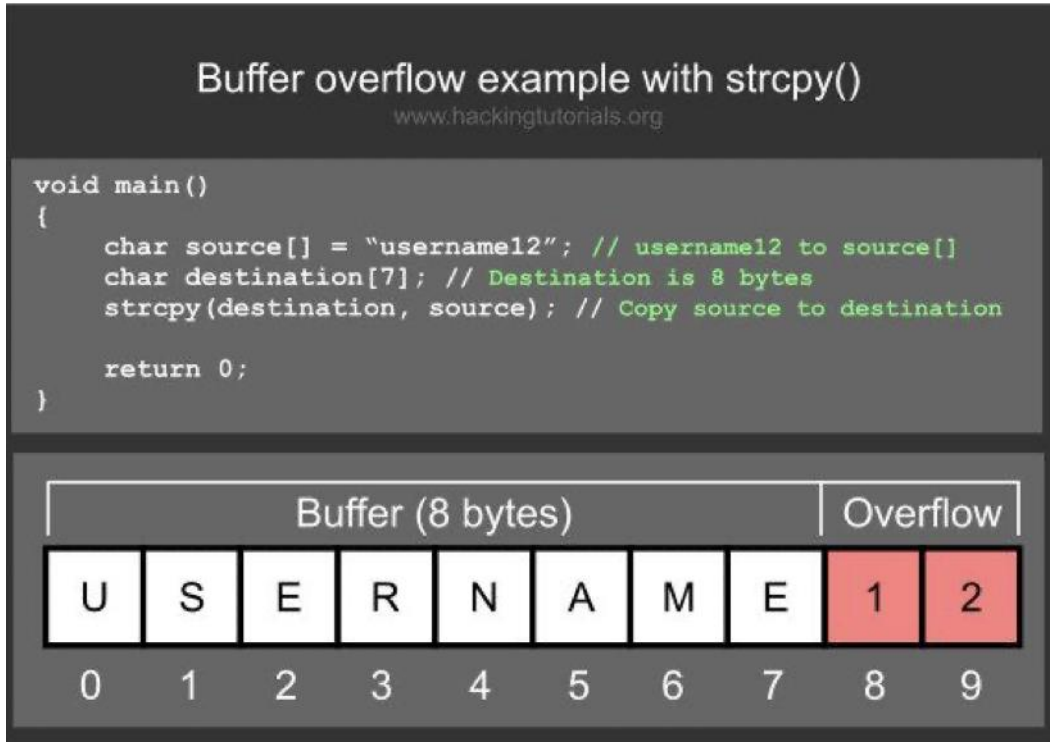
Et utvalg av typer skadevare:

 Virus	Kjennetegnes ved at det sprer seg hver gang en fil med virus blir åpnet av bruker eller systemet.
 Dataorm	Skadevare som på egenhånd er i stand til å spre seg og finne nye ofre.
 Trojaner	Skadevare som utgir seg for å være et nyttig program.
Bakdør	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper.
 Spionvare	Programvare for å spionere på en bruker i håp om å få tak i f.eks. informasjon, passord, kontoinformasjon.
 Tastelogger (Keylogger)	En enhet eller programvare som er koblet til tastatur eller maskin og som lagrer eller videresender alle tastetrykk. En variant av spionvare.
Rootkit	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller et system.
Exploit	Et program, en sekvens med data, eller en oppskrift på hvordan en sårbarhet kan utnyttes.

Se Notat sikkerhet uke 5 for mer om disse

Systemsikkerhet

- Handler om å beskytte operativsystemet og systemprogramvaren mot angrep
- Operativsystemet har høyere privilegier enn vanlige programmer.
- Hvis angripere får tilgang til sårbarheter i OS, kan de få full kontroll over systemet.
- Det er viktig å sørge for at **kjernen og drivere er sikre og oppdaterte**.



Buffer overflow

- En **buffer** er et område i minnet som brukes til å lagre data midlertidig.
- **Buffer overflow** skjer når et program skriver **mer data enn bufferet har plass til**.
- Dette kan føre til at:
  - Programmet **krasjer**.
  - Viktig data i minnet **overskrives**.
  - Angriperen kan **kjøre sin egen kode**.

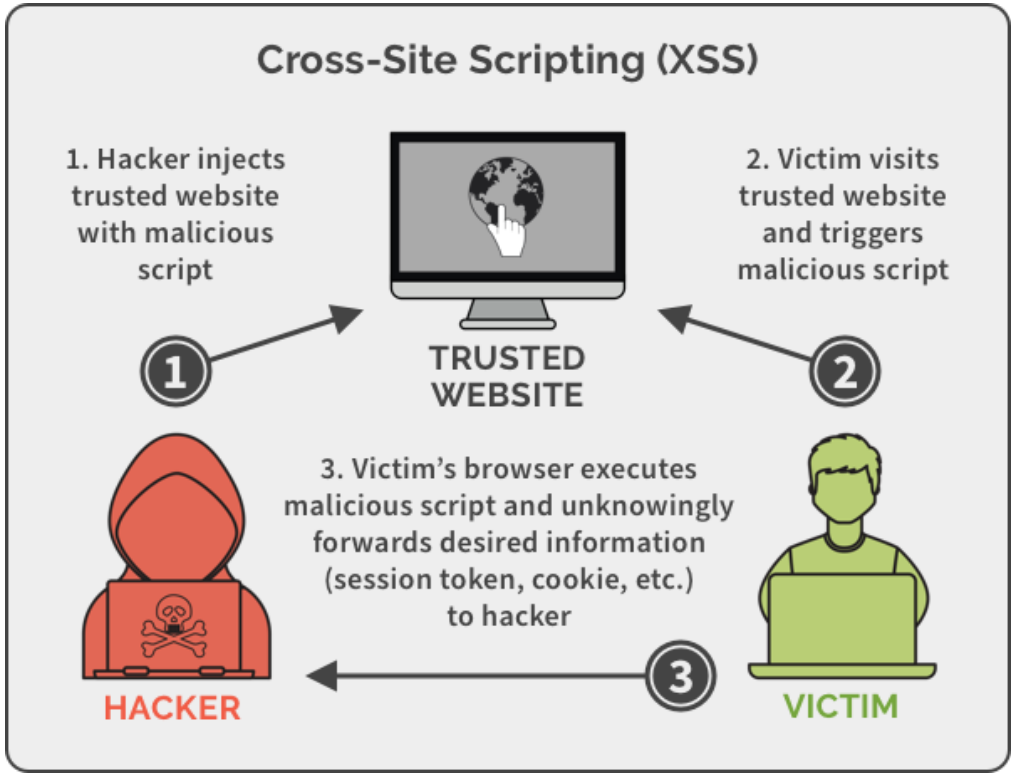
Applikasjonssikkerhet

- Applikasjoner har et grensesnitt mot brukere
- Stor grad eksponert for angrep og skadevare utenfra

- Cross-site scripting (XSS)
- SQL-injeksjon

Cross Site Scripting (XSS)

- Et type angrep der en angriper **injiserer ondsinnet kode** (ofte JavaScript) inn i en nettside.
- Angriperen legger inn skadelig JavaScript (f.eks. i et kommentarfelt eller skjema).
- Koden lagres på serveren (eller sendes direkte via URL).
- Når en annen bruker besøker siden, **kjøres koden automatisk i nettleseren deres** – som om det var legitimt innhold.
- Angriperen kan da:
  - Stjele informasjonskapsler (cookies)
  - Etterligne brukerens handlinger
  - Omdirigere brukeren til falske nettsider
  - Utføre handlinger på vegne av brukeren



SQL injection

UserId	Username	Password
0001	admin	passwd123
0002	matildad	67efg3ndfa

- Utnytter nettsider som ikke filtrerer input
- Etter å ha skrevet inn brukernavn og passord kjøres det en SQL spørring til databasen
  - Username: **admin**
  - Password: **passwd123**
- Om dette er riktig så får jeg tilgang

SQL Copy

```
"SELECT Count(*) FROM Users WHERE
Username=' " + txt.User.Text+" ' AND
Password=' "+ txt.Password.Text+" ' ";

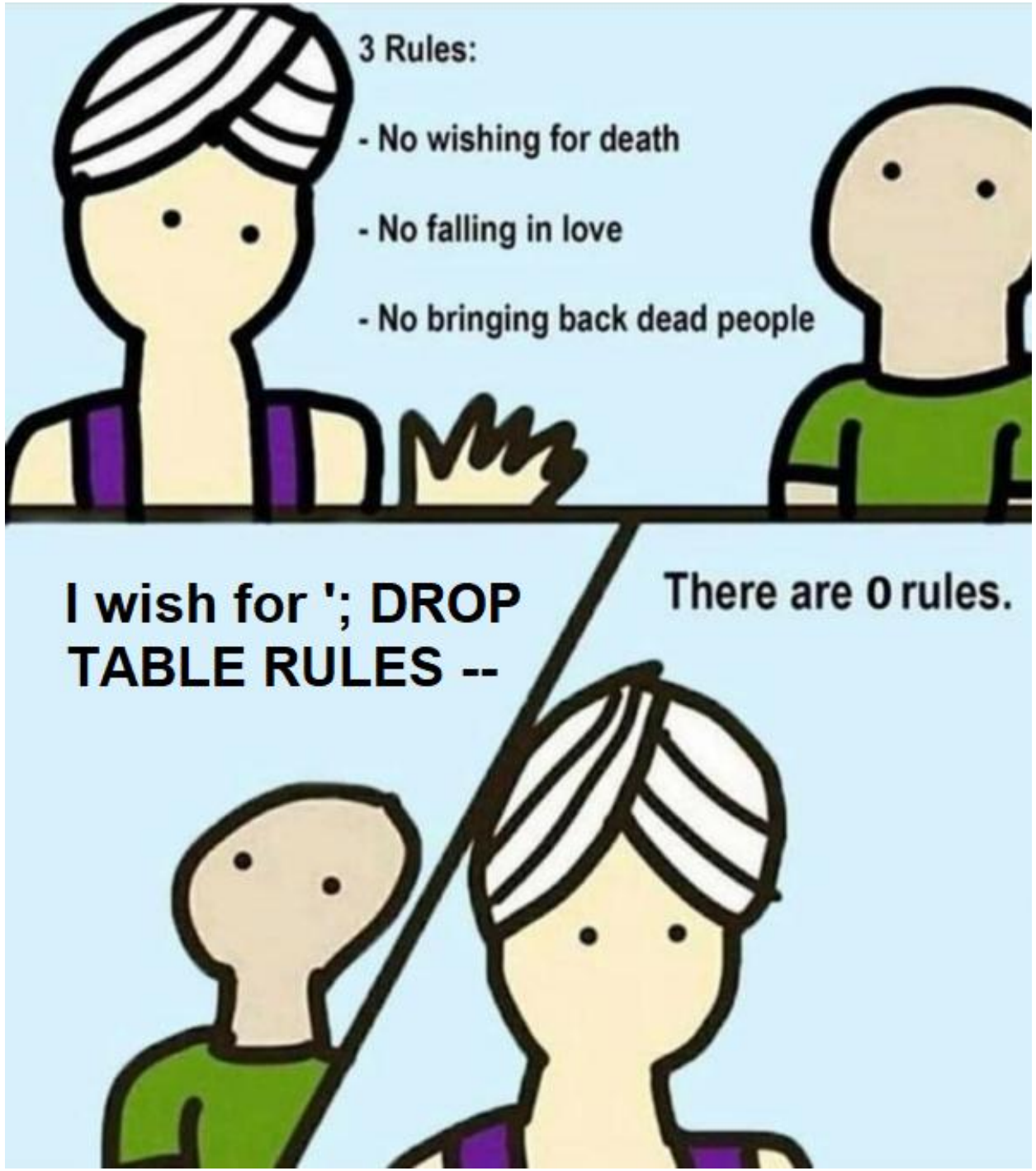
"SELECT Count(*) FROM Users WHERE
Username=' admin ' AND Password='
passwd123 ' ";
```

SQL injection

- Vi kan bruke *Magical String*
  - Username: **admin**
  - Password: ***anything ‘or'1’=‘1***
- I SQL brukes ' for å markere tekstverdier. Når vi skriver ' OR '1'='1, **bryter vi ut av den opprinnelige teksten**, og legger til ny logikk
- Passordet er ikke «anything» så Password = anything blir FALSE
- Men 1 = 1 er en sann statement og returnerer TRUE
- OR operasjonen trenger bare at en er sann for at det skal bli sant

Og woops så var hele databasen komprimittert

```
"SELECT Count(*) FROM Users WHERE
Username=' admin ' AND Password='
anything 'or'1'='1 ' ";
```


3 Rules:
- No wishing for death
- No falling in love
- No bringing back dead people
I wish for '; DROP TABLE RULES --
There are 0 rules.

Sosial manipulasjon

- Et svindelangrep hvor angriperen utnytter sider av deg som menneske
- Spiller ofte på tillit eller svakheter
- **Spoofing** - forfalskning av avsender
- **Phishing** - "fisker» etter info
  - Masse-phishing – sendes til mange, ikke detaljert
  - Spear-phishing – mer målrettet, samlet info om mottaker

Hvordan beskytte seg?

- **Opplæring og bevissthet**: Kjenn igjen faresignaler
- **Sikkerhetskultur**: Gode vaner og holdninger i organisasjonen
- **Tekniske tiltak**: Spamfilter, tofaktorautentisering, e-postsikring

Ukesoppgaver

Høst 2025 → sidemenyen → Ukeoppgaver → uke 39

Quiz fasit

Operativsystemer

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

		Sann	Usann
1	Operativsystemet sørger for at flere brukere kan dele en datamaskin		
2	Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.		
3	Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		
4	Operativsystemet sørger for at flere programmer kan kjøre samtidig.		
5	Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.		
6	Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.		
7	Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		
8	I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet		

Hvilke påstander om operativsystemer er sanne og hvilke er usanne?

	Sann	Usann
Operativsystemet sørger for at flere brukere kan dele en datamaskin	✔	
Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre.	✔	
Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem.		✔
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	✔	
Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk.	✔	
Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare.	✔	
Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt.		✔
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.		✔

Symmetrisk kryptering

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

	Sann	Usann
Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?		
Benyttes til kryptering av hemmelige meldinger.		
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.		
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres		
Benyttes til såkalt digital signatur.		
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.		
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring		
Kan brukes for å sikre konfidensialitet for data.		
Kan brukes for å sikre uavviselighet.		

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Sant	Usant
Benyttes til kryptering av hemmelige meldinger.	✔	
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.		✔
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres		✔
Benyttes til såkalt digital signatur.		✔
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.	✔	
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.	✔	
Kan brukes for å sikre konfidensialitet for data.	✔	
Kan brukes for å sikre uavviselighet.		✔

Overføringshastighet

Du ønsker å laste ned en fil på 800 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 25 megabit per sekund opp.

Hva er den teoretisk korteste overføringstiden?

Hvordan gå frem?

- Megabyte vs megabit
- Gjøre om byte → bit (*8)
- Skal vi laste ned eller opp?
- Dele størrelsen på hastigheten

Overføringshastighet

Du ønsker å laste ned en fil på 800 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 25 megabit per sekund opp.

Hva er den teoretisk korteste overføringstiden?

Hvordan gå frem?

- Megabyte vs megabit
- Gjøre om byte → bit (*8)
- Skal vi laste ned eller opp?
- Dele størrelsen på hastigheten

Filen er 800 megabyte * 8 = 6400 megabit stor

6400 / 50 = 128 sek overføringshastighet

Plasser begrepene under sammen med riktig tekst. Merk: Halvparten av begrepene vil være til overs.

Hjelp

Nulldagssårbarhet	Hash-algoritme	Verdier
Trusselmodellering	Dataorm	Asymmetrisk kryptering
PKI	Leveransekjedeangrep	Risiko
Personopplysninger	Trojaner	Digitale sertifikater

[ ] er en svakhet som ikke er kjent for leverandør av en tjeneste.

[ ] brukes for å sjekke dataintegritet.

[ ] brukes for å sikre ektheten av offentlige nøkler, samt trygg nøkkel-distribusjon.

[ ] har både en nyttig og en skadelig funksjon.

[ ] har lovpålagte krav om konfidensialitet, integritet og/eller tilgjengelighet.

[ ] er en kombinasjon av sannsynlighet for en hendelse og konsekvens av hendelsen.

Plasser begrepene under sammen med riktig tekst. Merk: Halvparten av begrepene vil være til overs.

Hjelp

Personopplysninger	Nulldagssårbarhet	Risiko
Digitale sertifikater	Trojaner	Asymmetrisk kryptering
Dataorm	Verdier	Leveransekjedeangrep
Trusselmodellering	Hash-algoritme	PKI

Nulldagssårbarhet ✓ er en svakhet som ikke er kjent for leverandør av en tjeneste.

Hash-algoritme ✓ brukes for å sjekke dataintegritet.

PKI ✓ brukes for å sikre ektheten av offentlige nøkler, samt trygg nøkkel-distribusjon.

Trojaner ✓ har både en nyttig og en skadelig funksjon.

Personopplysninger ✓ har lovpålagte krav om konfidensialitet, integritet og/eller tilgjengelighet.

Risiko ✓ er en kombinasjon av sannsynlighet for en hendelse og konsekvens av hendelsen.