Navn: _____ Dato: _____ Poeng: _____

Passordlekkasjer og sikkerhet for påloggingsopplysninger

Credential stuffing, datainnbrudd, hash-algoritmer, flerfaktorautentisering og passordsikkerhet.

LÆRINGSOVERSIKT: PASSORDLEKKASJER

SIKRET
DATAKRYPTERING
256-bits AES-standard

I SAMSVAR
GLOBALE STANDARDER
Rammeverk for GDPR og CCPA

ZERO TRUST
TILGANGSPOLICY
Flerfaktorautentisering

Velkommen! Dette aktivitetsheftet veileder deg gjennom passordlekkasjer og sikkerhet for legitimasjon. Du utforsker credential stuffing, datainnbrudd, hashalgoritmer, flerfaktorautentisering og passordbehandlere.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk cybersikkerhet og forebygging av trusler.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om cybersikkerhet

URL: https://www.vpn.com/no/cybersikkerhet/passord-lekket/

Din læringsveiledning for passordsikkerhet

- Forstå risikoen for at legitimasjon eksponeres på fora på det mørke nettet.
- Innfør flerfaktorautentisering (MFA) og overvåking av kompromittert påloggingsinformasjon.
- Utform forsvar for bedriftens sikkerhet mot målrettede svindelforsøk med sosial manipulering.

INSTRUKSJONER FOR VEILEDNINGEN OM PASSORDLEKKASJER

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på beskyttelse av legitimasjon. Avslutt med bonusaktiviteten Tenk raskt.

PASSORDLEKKASJER OG SIKKERHET FOR PÅLOGGINGSOPPLYSNINGER (INNLEDNING)

Passordlekkasjer eksponerer brukernes påloggingsopplysninger på offentlige nettsteder og på dark web. Unike passord fra en passordbehandler, kontroll mot kjente lekkasjer og flerfaktorautentisering (MFA) reduserer risikoen for credential stuffing, mens saltet, langsom passordhashing begrenser skaden hvis en passorddatabase blir stjålet.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er credential stuffing?

- A. Å bruke automatisering til å teste lekkede kombinasjoner av brukernavn og passord på flere nettsteder
- B. Å kryptere lokale databaselagringsfiler
- C. Å overbelaste webservere med forespørsler om nettverkstrafikk
- D. Å overvåke tastetrykk i det skjulte

2. Hvilken algoritme oppgir OWASP som førstevalg for lagring av passord i dag?

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3. Hvordan reduserer flerfaktorautentisering (MFA) risikoen ved passordlekkasjer?

- A. Den krever en ekstra verifiseringsfaktor, så et stjålet passord alene ikke er nok
- B. Den bytter passordet automatisk hver time
- C. Den krypterer brukernavnet under overføring
- D. Den varsler kredittopplysningsbyrået om svindelforsøk

4. Hva er et datalekkasjedump?

- A. En samling lekket brukerlegitimasjon som er publisert på nettet eller solgt på hackerfora
- B. En sikkerhetskopi av databasefiler lagret eksternt
- C. En midlertidig hurtigbuffer for webserverlogger
- D. Et administrativt verktøy som brukes til å tilbakestille brukerpassord

5. Hva er rollen til en passordbehandler?

- A. Å generere og lagre unike, sterke passord for hver konto
- B. Å overvåke nettverkstrafikk for passordlekkasjer
- C. Å blokkere automatiserte brute force-angrep i gatewayen
- D. Å skanne lagringsblokker i databasen etter ukrypterte passord

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Gjenbruk av passord på flere kontoer øker risikoen for credential stuffing.

○ Sant ○ Usant

7 Spørsmål 7

7. SHA-1 er en anbefalt hashfunksjon for moderne lagring av passord.

○ Sant ○ Usant

8 Spørsmål 8

8. Å håndheve passordkompleksitet alene (uten MFA) stopper credential stuffing fullstendig.

○ Sant ○ Usant

9 Spørsmål 9

9. Verktøy for overvåking av darknet skanner internett etter kompromitterte påloggingsopplysninger for bedrifter.

○ Sant ○ Usant

10 Spørsmål 10

10. Saltede hasher legger til unike tilfeldige data i passord før hashing for å motvirke angrep med regnbuetabeller.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Å teste lekkede påloggingsopplysninger mot mange nettapplikasjoner kalles _____ .
2. En treg, adaptiv passordhashingalgoritme som fortsatt godtas av OWASP, er _____ .
3. Eksponering av konfidensielle databasefiler på internett er et _____ .
4. Å legge til tilfeldige verdier i passord før hashing kalles _____ .
5. En sikker lokal database for brukernes påloggingsopplysninger kalles et _____ .
6. Å legge til et andre verifiseringstrinn ved pålogging bruker _____ -autentisering.

ORDBANK

BCRYPT DATABRUDD FLERFAKTOR NETTFISKING PASSORDBEHANDLER PASSORDFYLLING REGNBUETABELL SALTING

Skriv svarene dine her:

1.
2.
3.
4.
5.
6.

Kontrollpunkt 4: Koble sikkerhetsbegreper

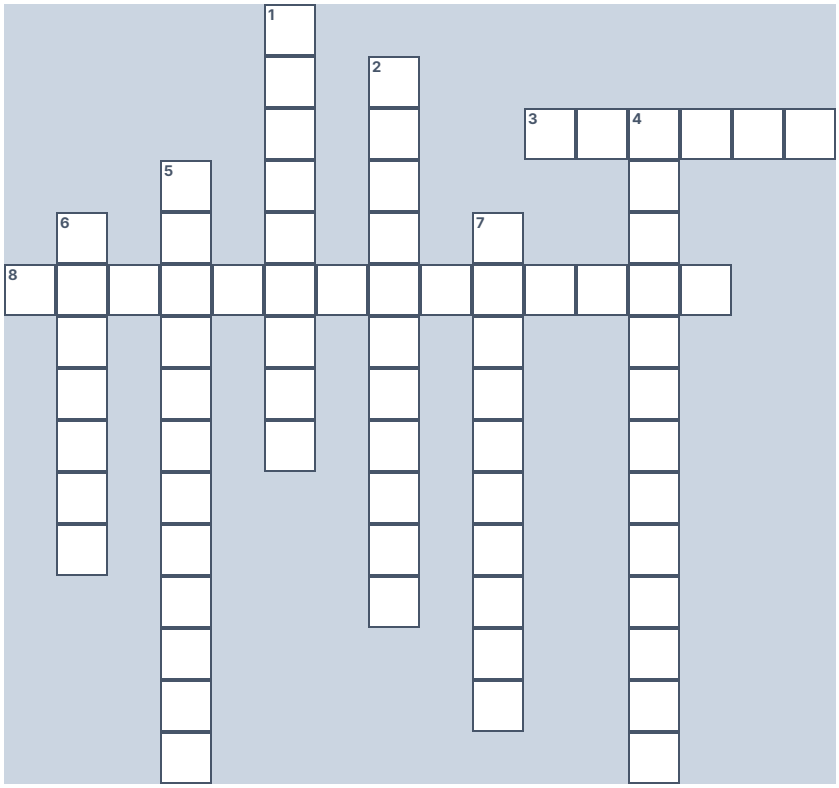
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. STUFFING	A	Forhåndsberegnet tabell over passordhasjer.
☐	2. BCRYPT	B	Påloggingskontroll med flere faktorer.
☐	3. DATABRUDD	C	Verktøy for lagring av legitimasjon.
☐	4. SALTING	D	Uautorisert eksponering av databaser.
☐	5. BEHANDLER	E	Sosial manipulering for å stjele påloggingsopplysninger.
☐	6. MFA	F	Testing av lekkede påloggingsopplysninger.
☐	7. RAINBOW	G	Å legge til tilfeldig salt i passordhashen.
☐	8. NETTFISKING	H	Treg algoritme for passordhashing.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

3. Treg algoritme for hashing av passord. (6)

8. Testing av lekkede påloggingsopplysninger. (14)

LODDRETT

1. Uautorisert eksponering av en database. (9)

2. Sosial manipulering for å stjele påloggingsopplysninger. (11)

4. Forhåndsberegnet tabell over passordhasher. (13)

5. Verktøy for lagring av påloggingsopplysninger. (12)

6. Å legge til tilfeldig salt i en passordhash. (7)

7. Pålogging med kontroll i flere trinn. (10)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

3 vannrett: Treg algoritme for hashing av passord. (6 bokstaver):

8 vannrett: Testing av lekkede påloggingsopplysninger. (14 bokstaver):

LODDRETT

1 loddrett: Uautorisert eksponering av en database. (9 bokstaver):

2 loddrett: Sosial manipulering for å stjele påloggingsopplysninger. (11 bokstaver):

4 loddrett: Forhåndsberegnet tabell over passordhasher. (13 bokstaver):

5 loddrett: Verktøy for lagring av påloggingsopplysninger. (12 bokstaver):

6 loddrett: Å legge til tilfeldig salt i en passordhash. (7 bokstaver):

7 loddrett: Pålogging med kontroll i flere trinn. (10 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

L Å N L Y T W A U Z K N N H I
L G N I K S I F T T E N O I T
E G M V S A L T I N G M T Z I
B B W G Ø P Ø Z U I V Æ A R X
A P P Å Q J T R V I R X W Q W
T W L A F P Q O M B P X G H R
E S Z Ø Y K L X K Ø Y Æ R L J
U Å J R K D D U R B A T A D O
B A C F J B V A K F Y F L Å L
N B R O T K A F R E L F E M S
G P A S S O R D F Y L L I N G
E O K A G Q L P D O C D I J B
R B P A S S O R D H V E L V Q
T N R Y W J Ø G Ø U H Æ Z I F
T W P W L T E V U N R M O U I

ORDLISTE

PASSORDFYLLING BCRYPT DATABRUDD SALTING PASSORDHVELV
FLERFAKTOR REGNBUETABELL NETTFISKING

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. PASSORDFYLLING
B. BCRYPT
C. DATABRUDD
D. SALTING
E. PASSORDHVELV
F. FLERFAKTOR
G. REGNBUETABELL
H. NETTFISKING

DEFINISJONER OG TILHØRENDE FELT

_____ 1. Sosial manipulering for å stjele påloggingsopplysninger.

_____ 2. Uautorisert eksponering av en database.

_____ 3. Treg algoritme for hashing av passord.

_____ 4. Forhåndsberegnet tabell over passordhasher.

_____ 5. Testing av lekkede påloggingsopplysninger.

_____ 6. Å legge til tilfeldig salt i en passordhash.

_____ 7. Verktøy for lagring av påloggingsopplysninger.

_____ 8. Pålogging med kontroll i flere trinn.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. LRFLDSAYIPN GOS
2. DDDAARUBT
3. PAHDLVSRVO ES
4. ULAGTBLEEB REN
5. YRTBPC
6. NLISTGA
7. LRFKATORFE
8. ISGITNFENKT

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Trygge vaner du kan begynne med i dag			
2	Regler for et sterkt passord			
3	Passordbehandlere du kjenner til			
4	Sikkerhetsverktøy du kjenner til			
5	Advarselstegn i en e-post			
6	Morsomme ord til en lang passfrase			
7	Måter å logge inn på uten passord			
8	Informasjon du aldri bør dele			
9	Grunner til å oppdatere programvare			
10	Ting å gjøre når et passord lekker			
11	Kontoer som trenger MFA			
12	Steder passord aldri bør lagres			
13	Tegn på at en datamaskin er infisert			
14	Dårlige passord folk bruker			
15	Ting du tar sikkerhetskopi av			

Kontrollpunkt 8: Casestudier om cybersikkerhet

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: UTBEDRING AV LEKKASJE AV BEDRIFTSLEGITIMASJON

👷

Scenario: En tjeneste for overvåking av det mørke nettet varsler en organisasjon om at et datadump som inneholder passord til systemadministratorer i selskapet er publisert på nettet.

Diskusjonsspørsmål: Analyser risikoene ved lekkasjen av påloggingsopplysninger, og foreslå en administrativ strategi for tilbakestilling.

CASESTUDIE 2: INNFØRE STANDARDER FOR PASSORDHASHING

👷

Scenario: En database i et selskap lagrer i dag brukerpassord med utdaterte MD5-hasher uten kryptografisk salt, noe som gjør dem sårbare for rask uthenting.

Diskusjonsspørsmål: Utform en migreringsstrategi for å oppgradere hashalgoritmen i databasen.

Kontrollpunkt 9: Knekk chifferet

En cybersikkerhetsekspert beskytter nettverksressurser mot trusselaktører på nettet. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Æ=27 Ø=28 Å=29

19	9	11	18	5		12	5	11	11	5	4	5		16	1	19	19	15	18	4
					13	5	4		6	12	5	18	6	1	11	20	15	18		
								16	29	12	15	7	7	9	14	7				

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del A)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q1: Hva er en passordlekkasje?

En passordlekkasje oppstår når påloggingsinformasjon for brukere eksponeres gjennom datainnbrudd eller feilkonfigurerte servere.

Q2: Hvordan finner hackere lekkede passord?

Hackere skanner fora på det mørke nettet, offentlige databasedumper og paste-nettsteder der data fra datalekkasjer publiseres [8].

Q3: Er gjenbruk av passord farlig?

Ja, fordi hvis ett nettsted blir kompromittert, kan hackere teste de samme påloggingsopplysningene på tusenvis av andre plattformer [3].

Q4: Hva er et kryptografisk salt?

Et salt er tilfeldige data som legges til et passord før hashing, slik at angrep med forhåndsberegnede oppslagstabeller blir ineffektive [2].

Q5: Hvorfor er MD5 foreldet?

MD5 er en rask, foreldet generell hashfunksjon, så angripere kan teste passordgjetninger ekstremt raskt, særlig når hashene er uten salt [2].

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del B)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q6: Hvordan beskytter en passordbehandler brukerne?

Den genererer automatisk komplekse, unike påloggingsopplysninger for hvert nettsted, noe som reduserer menneskelige hukommelsesfeil og gjenbruk.

Q7: Hva er et brute force-angrep?

Et angrep som systematisk tester alle mulige tegnkombinasjoner til riktig passord er funnet [4].

Q8: Hvordan hjelper kontosperre?

Utelåsing eller hastighetsbegrensning bremser gjentatte gjettinger på nett og reduserer, sammen med overvåking og MFA, risikoen for brute force-angrep [4].

Q9: Er hovedpassord sikre?

De er sikre hvis de er passfraser med høy entropi som aldri gjenbrukes på andre websystemer.

Q10: Bør passord byttes jevnlig?

NIST sier at man ikke skal tvinge fram periodiske bytter; bytt ved tegn på kompromittering og prioriter lengde, blokkeringslister og MFA [1].

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del C)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q1: Hvordan er Argon2 sammenlignet med bcrypt?

OWASP oppgir Argon2id som førstevalg; de minnekrevende innstillingene motstår knekking med GPU og ASIC bedre enn bcrypt [2].

Q2: Hva er nøkkelstrekking (key stretching)?

En teknikk som kjører en hashing-algoritme i løkke tusenvis av ganger for å bremse verifiseringen av passord, slik at knekking blir kostbart [2].

Q3: Hvordan fungerer rainbow tables?

De er forhåndsberegnede oppslagstabeller som kobler passord i klartekst til hashverdiene deres, og brukes til å reversere hasher uten salt raskt [2].

Q4: Hva er gjenbruk av legitimasjon?

Gjenbruk av stjålne kombinasjoner av brukernavn og passord fra ett datainnbrudd for å forsøke å få tilgang til andre tjenester, særlig der folk har gjenbrukt passord [3].

Q5: Kan passordbehandlere bli hacket?

Ja. Mange bruker kryptering med null kunnskap, slik at et serverbrudd bare eksponerer krypterte hvelv, men svake hovedpassord kan likevel knekkes frakoblet.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del D)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q6: Hva er et ordbokangrep?

En variant av brute force som tester vanlige ord, fraser og tidligere lekkede passord i stedet for tilfeldige bokstaver.

Q7: Hvorfor foretrekkes passfraser?

Passordfraser bruker flere tilfeldige ord, noe som gir høy entropi som er lett for mennesker å huske, men beregningsmessig kostbar å knekke [1].

Q8: Hvordan påvirker enkel pålogging (SSO) lekkasjer av passord?

SSO reduserer passordspredning, men identitetsleverandøren blir et attraktivt mål som trenger sterk, helst phishing-resistent MFA [6].

Q9: Hva er øktkapring (session hijacking)?

En angriper skaffer seg eller misbruker en gyldig øktkode for å utgi seg for å være en pålogget bruker uten å trenge passordet på nytt [5].

Q10: Hvordan oppdager du passordsprøyting (password spraying)?

Ved å se etter de samme få passordene som prøves på mange kontoer, ofte langsomt for å holde seg under terskler for utestenging [7].

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

NIST SP 800-63B krever at nye passord sjekkes mot blokkeringslister over vanlige og kompromitterte passord [1].

2. SIKKERHETSINNSIKT

Dumpen 'Collection #1' fra 2019 slo sammen data fra mange tidligere datainnbrudd til én enorm fil med par av e-postadresser og passord [8].

3. SIKKERHETSINNSIKT

NIST krever nå at passord som brukes som eneste autentiseringsfaktor, er minst 15 tegn lange [1].

4. SIKKERHETSINNSIKT

ASIC-maskinvare kan beregne milliarder av SHA-256-hasher per sekund, noe som gjør rå SHA-hashing utrygt for brukerpassord [2].

5. SIKKERHETSINNSIKT

Unike salter betyr at to brukere med nøyaktig samme passord får ulike hashverdier i databasen [2].

6. SIKKERHETSINNSIKT

Mange passordbehandlere krypterer hvelvdata lokalt med sterk kryptografi utledet fra brukerens hovedpassord.

7. SIKKERHETSINNSIKT

Credential stuffing fungerer fordi mange gjenbruker det samme passordet på tvers av nettbutikker, banker og e-postkontoer [3].

8. SIKKERHETSINNSIKT

NIST SP 800-63B sier at verifikatorer ikke skal kreve periodiske passordbytter, bare bytte etter tegn på kompromittering [1].

9. SIKKERHETSINNSIKT

Å legge til én enkelt stor bokstav og ett symbol i et kort passord stopper ikke moderne automatiserte GPU-ordlisteangrep [1].

10. SIKKERHETSINNSIKT

MFA kan blokkere mange forsøk på credential stuffing selv etter at et passord har lekket; phishing-resistent MFA er sterkere enn SMS-koder [3].

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale standarder fra NIST og OWASP og standarder for etterlevelse av personvern.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Fasit: Kontrollpunkt 1 – flervalg

1 **Spørsmål 1** — **Riktig svar: A**

MERKNAD TIL LÆREREN

Credential stuffing bruker automatisering til å prøve lekkede brukernavn/passord-par på andre nettsteder [3].

2 **Spørsmål 2** — **Riktig svar: A**

MERKNAD TIL LÆREREN

OWASP anbefaler Argon2id først; bcrypt er hovedsakelig for eldre systemer der Argon2id eller scrypt ikke er tilgjengelig [2].

3 **Spørsmål 3** — **Riktig svar: A**

MERKNAD TIL LÆREREN

MFA krever en ekstra faktor, så et stjålet passord alene ikke kan låse opp kontoen [3].

4 **Spørsmål 4** — **Riktig svar: A**

MERKNAD TIL LÆREREN

Databrudd-dumper er samlinger av lekkede påloggingsopplysninger, som sammenstillingen Collection #1 fra 2019 [8].

5 **Spørsmål 5** — **Riktig svar: A**

MERKNAD TIL LÆREREN

En passordbehandler genererer og lagrer et unikt, sterkt passord for hver konto og forhindrer gjenbruk [3].

Fasit: Kontrollpunkt 2 – sant eller usant

6 Spørsmål 6

Riktig svar: Sant

MERKNAD TIL LÆREREN

Sant: gjenbrukte passord lar angripere spille av påloggingsopplysninger som er lekket fra ett nettsted, på andre nettsteder [3].

7 Spørsmål 7

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: SHA-1 er en rask hash; OWASP anbefaler Argon2id, scrypt, bcrypt eller PBKDF2 i stedet [2].

8 Spørsmål 8

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: kompleksitetsregler alene kan ikke stoppe credential stuffing med gjenbrukte lekkede passord; MFA trengs [3].

9 Spørsmål 9

Riktig svar: Sant

MERKNAD TIL LÆREREN

Sant: overvåkingstjenester søker i databrudd-dumper og kilder på det mørke nettet etter eksponerte påloggingsopplysninger [8].

10 Spørsmål 10

Riktig svar: Sant

MERKNAD TIL LÆREREN

Sant: et unikt salt per passord gjør forhåndsberegnede regnbuetabeller ineffektive [2].

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

F 1. STUFFING	H 2. BCRYPT	D 3. DATABRUDD	G 4. SALTING
C 5. BEHANDLER	B 6. MFA	A 7. RAINBOW	E 8. NETTFISKING

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 PASSORDFYLLING	2 BCRYPT	3 DATABRUDD	4 SALTING
5 PASSORDBEHANDLER	6 FLERFAKTOR		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 H – NETTFISKING	2 C – DATABRUDD	3 B – BCRYPT	4 G – REGNBUETABELL
5 A – PASSORDFYLLING	6 D – SALTING	7 E – PASSORDHVELV	8 F – FLERFAKTOR

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare STUFFING, BCRYPT og DATABRUDD med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

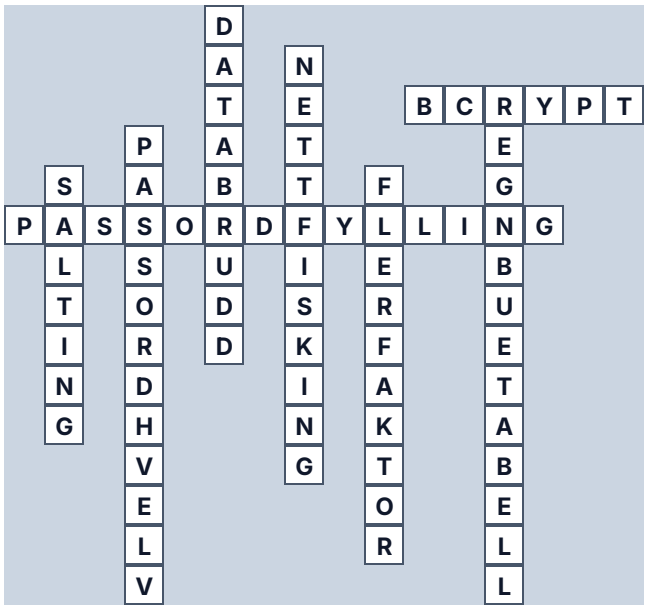
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

L	Å	N	L	Y	T	W	A	U	Z	K	N	N	H	I
L	G	N	I	K	S	I	F	T	T	E	N	O	I	T
E	G	M	V	S	A	L	T	I	N	G	M	T	Z	I
B	B	W	G	Ø	P	Ø	Z	U	I	V	Æ	A	R	X
A	P	P	Å	Q	J	T	R	V	I	R	X	W	Q	W
T	W	L	A	F	P	Q	O	M	B	P	X	G	H	R
E	S	Z	Ø	Y	K	L	X	K	Ø	Y	Æ	R	L	J
U	Å	J	R	K	D	D	U	R	B	A	T	A	D	O
B	A	C	F	J	B	V	A	K	F	Y	F	L	Å	L
N	B	R	O	T	K	A	F	R	E	L	F	E	M	S
G	P	A	S	S	O	R	D	F	Y	L	L	I	N	G
E	O	K	A	G	Q	L	P	D	O	C	D	I	J	B
R	B	P	A	S	S	O	R	D	H	V	E	L	V	Q
T	N	R	Y	W	J	Ø	G	Ø	U	H	Æ	Z	I	F
T	W	P	W	L	T	E	V	U	N	R	M	O	U	I

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

3 vannrett: BCRYPT Treg algoritme for hashing av passord. (6 bokstaver)

8 vannrett: PASSORDFYLLING Testing av lekkede påloggingsopplysninger. (14 bokstaver)

LODDRETT

1 loddrett: DATABRUDD Uautorisert eksponering av en database. (9 bokstaver)

2 loddrett: NETTFISKING Sosial manipulering for å stjele påloggingsopplysninger. (11 bokstaver)

4 loddrett: REGNBUETABELL Forhåndsberegnet tabell over passordhasher. (13 bokstaver)

5 loddrett: PASSORDHVELV Verktøy for lagring av påloggingsopplysninger. (12 bokstaver)

6 loddrett: SALTING Å legge til tilfeldig salt i en passordhash. (7 bokstaver)

7 loddrett: FLERFAKTOR Pålogging med kontroll i flere trinn. (10 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. LRFLDSAYIPNGOS — **PASSORDFYLLING**
2. DDDAARUBT — **DATABRUDD**
3. PAHDLVSRVOES — **PASSORDHVELV**
4. ULAGTBLEEBREN — **REGNBUETABELL**
5. YRTBPC — **BCRYPT**
6. NLISTGA — **SALTING**
7. LRFKATORFE — **FLERFAKTOR**
8. ISGITNFENKT — **NETTFISKING**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"SIKRE LEKKEDE PASSORD MED FLERFAKTOR PÅLOGGING"

Fasit til casestudiene

A Casestudie 1: Utbedring av lekkasje av bedriftslegitimasjon

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En tjeneste for overvåking av det mørke nettet varsler en organisasjon om at et databaseutslipp med passord til bedriftens systemadministratorer er publisert på nett.
- Anbefalt strategi og løsning: Opphev alle aktive administratorøkter og tilbakestill legitimasjonen med en generator med høy entropi. Håndhev phishing-resistent MFA på administratorportaler [6], roter berørte API-nøkler, gå gjennom innloggingslogger, finn den første eksponeringen og kontroller andre privilegerte kontoer.

B Casestudie 2: Innføre standarder for passordhashing

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En bedriftsdatabase lagrer for tiden brukerpassord med utdaterte MD5-hasher uten kryptografisk salt, noe som gjør dem sårbare for rask uthenting.
- Anbefalt strategi og løsning: Ta i bruk Argon2id (eller bcrypt på eldre systemer) med et unikt salt per bruker [2]. Pakk inn eksisterende MD5-hasher i den nye algoritmen nå, hash på nytt direkte ved hver brukers neste pålogging, og tving tilbakestilling for kontoer som lenge har vært inaktive.