Navn: _____ Dato: _____ Point: _____

Lækkede adgangskoder og sikre logins

Credential stuffing, databrud, hashalgoritmer, multifaktorgodkendelse og adgangskodesikkerhed.

OVERBLIK OVER LÆKKEDE ADGANGSKODER

SIKRET
DATAKRYPTERING
256-bit AES-standard

OVERHOLDER KRAV
GLOBALE STANDARDER
GDPR- og CCPA-rammer

ZERO-TRUST
ADGANGSPOLITIK
Multifaktorgodkendelse

Velkommen! Dette opgavehæfte guider dig gennem lækkede adgangskoder og sikre logins. Du vil udforske credential stuffing, databrud, hashalgoritmer, flerfaktorgodkendelse og adgangskodeadministratorer.

OPGAVEARKETS KONTROLPUNKTER

- [ ] **Del 1-4: Lær cybersikkerhed og trusselsforebyggelse.**
- [ ] **Del 5-7: Løs kryds og tværs samt ordjagt.**
- [ ] **Del 8-9: Løs casestudier og chifferudfordring.**
- [ ] **Del 10: Gennemgå grundlæggende og avanceret FAQ.**
- [ ] **Del 11: Udforsk 10 interessante fakta fra virkeligheden.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

Åbn VPN.com's guide til cybersikkerhed

URL: https://www.vpn.com/da/cybersikkerhed/adgangskoder-laekket/

Din læringsplan for sikre adgangskoder

- Forstå risikoen, når loginoplysninger dukker op på fora på det mørke net.
- Indfør flerfaktorgodkendelse (MFA) og overvågning af kompromitterede loginoplysninger.
- Design virksomhedens forsvar mod målrettet social manipulation.

VEJLEDNING TIL GUIDEN OM LÆKKEDE ADGANGSKODER

Besvar flervalgs- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden om beskyttelse af logins. Slut af med bonusaktiviteten Tænk hurtigt.

LÆKKEDE ADGANGSKODER OG SIKRE LOGINS (INTRODUKTION)

Adgangskodelæk afslører brugeres loginoplysninger på offentlige websteder og på dark web. Unikke adgangskoder fra en adgangskodeadministrator, screening mod lækkede adgangskoder og flerfaktorgodkendelse (MFA) mindsker risikoen for credential stuffing, mens saltet, langsom hashing af adgangskoder begrænser skaden, hvis en adgangskodedatabase bliver stjålet.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE SVAR.

Kontrolpunkt 1: Flervalgsopgave

1. Hvad er credential stuffing?

- A. Automatisk afprøvning af lækkede brugernavne og adgangskoder på mange websteder
- B. Kryptering af lokale databasefiler
- C. Overbelastning af servere med trafik
- D. Skjult overvågning af tastetryk

2. Hvilken algoritme angiver OWASP i dag som sit førstevalg til lagring af adgangskoder?

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

3. Hvordan mindsker multifaktorgodkendelse (MFA) risikoen ved lækkede adgangskoder?

- A. Den kræver en ekstra verifikationsfaktor, så en stjålen adgangskode alene ikke er nok
- B. Den ændrer automatisk adgangskoden hver time
- C. Den krypterer brugernavnet under overførslen
- D. Den advarer kreditbureauet om svigagtige anmodninger

4. Hvad er et datadump fra et brud?

- A. En samling lækkede logins, der offentliggøres eller sælges på hackerfora
- B. En backup af databasefiler uden for huset
- C. En midlertidig cache af serverlogfiler
- D. Et værktøj til at nulstille adgangskoder

5. Hvad gør en adgangskodeadministrator?

- A. Laver og gemmer unikke, stærke adgangskoder til hver konto
- B. Overvåger trafikken for lækkede adgangskoder
- C. Blokerer automatiske brute force-angreb ved porten
- D. Scanner databaser for ukrypterede adgangskoder

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Genbrug af adgangskoder på flere konti øger risikoen for credential stuffing.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. SHA-1 anbefales til moderne opbevaring af adgangskoder.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. Krav om komplekse adgangskoder alene (uden MFA) stopper credential stuffing helt.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. Værktøjer til overvågning af det mørke net søger efter kompromitterede firmalogins.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. Saltede hashes tilføjer unikke, tilfældige data før hashing og slår angreb med regnbuetabeller.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. Afprøvning af lækkede loginoplysninger på tværs af mange webapps kaldes credential _____ .
2. En langsom, adaptiv hashalgoritme til adgangskoder, som OWASP stadig accepterer, er _____ .
3. Når fortrolige databasefiler bliver eksponeret på internettet, er det et _____ .
4. At tilføje tilfældige værdier til adgangskoder før hashing kaldes _____ .
5. En sikker lokal database til brugerens loginoplysninger er en adgangskode- _____ .
6. Et ekstra bekræftelsestrin ved login bruger _____ .

ORDBANK MED FAGUDTRYK

ADMINISTRATOR · BCRYPT · DATABRUD · MFA · PHISHING · REGNBUETABEL · SALTNING · STUFFING

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

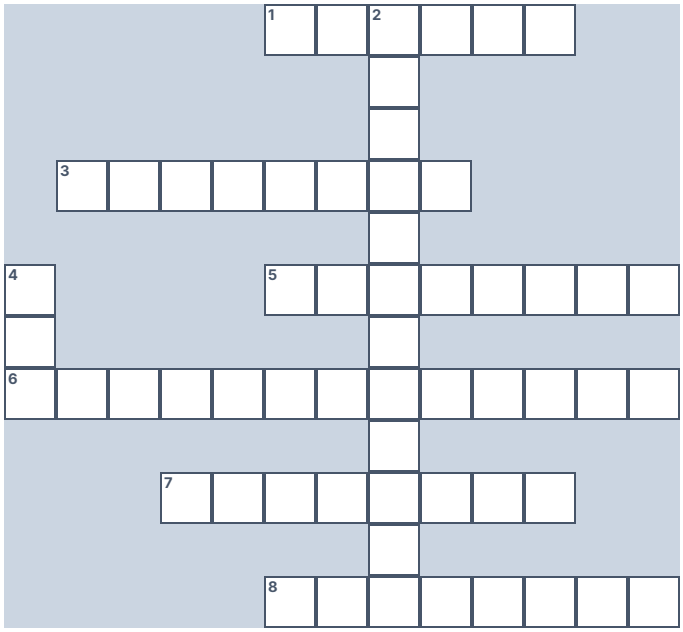
MATCH BEGREBER OG DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

☐	1. STUFFING	A	Forudberegnet tabel over hashes.
☐	2. BCRYPT	B	Login med flere faktorer.
☐	3. BRUD	C	Værktøj til opbevaring af logins.
☐	4. SALTNING	D	Uautoriseret afsløring af en database.
☐	5. ADMINISTRATOR	E	Social manipulation, der stjæler logins.
☐	6. MFA	F	Afprøvning af lækkede logins.
☐	7. REGNBUETABEL	G	Tilfældigt salt tilføjet før hashing.
☐	8. PHISHING	H	Langsom hashalgoritme til adgangskoder.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

1. Langsom hashalgoritme til adgangskoder (6)

3. Social manipulation, der skal stjæle loginoplysninger (8)

5. Afprøvning af lækkede loginoplysninger (8)

6. Adgangskode…: værktøj til opbevaring af loginoplysninger (13)

7. Uautoriseret eksponering af en database (8)

8. Tilføjelse af tilfældigt salt til en adgangskodes hash (8)

LODRETTE NØGLER

2. Forudberegnet tabel over hashværdier for adgangskoder (12)

4. Kontrol af login med flere faktorer (3)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.

VANDRETTE NØGLER

1 vandret: Langsom hashalgoritme til adgangskoder (6 bogstaver):

3 vandret: Social manipulation, der skal stjæle loginoplysninger (8 bogstaver):

5 vandret: Afprøvning af lækkede loginoplysninger (8 bogstaver):

6 vandret: Adgangskode…: værktøj til opbevaring af loginoplysninger (13 bogstaver):

7 vandret: Uautoriseret eksponering af en database (8 bogstaver):

8 vandret: Tilføjelse af tilfældigt salt til en adgangskodes hash (8 bogstaver):

LODRETTE NØGLER

2 lodret: Forudberegnet tabel over hashværdier for adgangskoder (12 bogstaver):

4 lodret: Kontrol af login med flere faktorer (3 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

L J U Å U G S S Y F A A S Q O

E G R W Æ S L T T W D U D O Ø

B N B G U Z Z U K A A T Å Ø Ø

A I M H B J O F T L T N N V Q

T N I S C S H F Å A A Q X G X

E T A C R Ø T I Ø B B I N Å H

U L F K Y P R N P Z R C N Å Ø

B A M G P Æ Q G Y X U M X R B

N S P Y T V N H X D D Ø X L T

G B Z Å Æ N T S Æ J Q E A D L

E A D M I N I S T R A T O R S

R Y Z Z M K I W I G B F J L V

U Y P H I S H I N G T Å F I F

U C A M R C Å N L Y T W A U Z

K N N H I O I T G M V M T Z I

ORDLISTE MED FAGUDTRYK

STUFFING BCRYPT DATABRUD SALTNING ADMINISTRATOR MFA REGNBUETABEL PHISHING

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK
A. STUFFING
B. BCRYPT
C. DATABRUD
D. SALTNING
E. ADMINISTRATOR
F. MFA
G. REGNBUETABEL
H. PHISHING

DEFINITIONER OG MATCHFELTER	
	1. Social manipulation, der skal stjæle loginoplysninger.
	2. Uautoriseret eksponering af en database.
	3. Langsom hashalgoritme til adgangskoder.
	4. Forudberegnet tabel over hashværdier for adgangskoder.
	5. Afprøvning af lækkede loginoplysninger.
	6. Tilføjelse af tilfældigt salt til en adgangskodes hash.
	7. Adgangskode...: værktøj til opbevaring af loginoplysninger.
	8. Kontrol af login med flere faktorer.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige cybersikkerhedsbegreber. Skriv dine svar i indtastningsfelterne.

1. NFFSITGU
2. ADDAURBT
3. DATARORMSNITI
4. ETBGELUBAREN
5. YRTBPC
6. NGTISNAL
7. AFM
8. SHHGPNII

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Sikkerhedsvaner, du kan starte i dag			
2	Regler for en stærk adgangskode			
3	Adgangskodeadministratorer, du kender			
4	Sikkerhedsværktøjer, du kender			
5	Advarselstegn i en e-mail			
6	Sjove ord til en lang adgangssætning			
7	Måder at logge ind uden adgangskode			
8	Oplysninger, du aldrig bør dele			
9	Grunde til at opdatere software			
10	Ting at gøre, når en kode er lækket			
11	Konti, der har brug for MFA			
12	Steder, hvor koder ikke skal gemmes			
13	Tegn på, at en computer er inficeret			
14	Dårlige adgangskoder, folk bruger			
15	Ting, du tager backup af			

Kontrolpunkt 8: Casestudier om cybersikkerhed

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

CASESTUDIE 1: OPRYDNING EFTER LÆKKEDE FIRMALOGINS



Scenarie: En overvågningstjeneste advarer en organisation om, at et datadump med systemadministratorernes adgangskoder er lagt på nettet.

Diskussion: Analysér risikoen ved lækket, og foreslå en strategi for nulstilling.

CASESTUDIE 2: INDFØRELSE AF SIKKER HASHING



Scenarie: En virksomhedsdatabase gemmer adgangskoder med forældede MD5-hashes uden salt, så de hurtigt kan knækkes.

Diskussion: Design en plan for at opgradere databasens hash-algoritme.

Kontrolpunkt 9: Afkod chifferet

En cybersikkerhedsekspert beskytter netværkets aktiver mod trusselsaktører online. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter.

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

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

2	18	21	7		21	14	9	11	11	5

1	4	7	1	14	7	19	11	15	4	5	18		15	7		13	6	1

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del A)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q1: Hvad er et læk af adgangskoder?

Når loginoplysninger afsløres gennem databrud eller fejlopsatte servere.

Q2: Hvordan finder hackere lækkede adgangskoder?

Hackere gennemsøger dark web-fora, offentlige databasedumps og paste-sider, hvor data fra læk offentliggøres [8].

Q3: Er genbrug af adgangskoder farligt?

Ja, for hvis ét websted kompromitteres, kan hackere afprøve de samme loginoplysninger på tusindvis af andre platforme [3].

Q4: Hvad er et kryptografisk salt?

Et salt er tilfældige data, der tilføjes en adgangskode før hashing, så angreb med forudberegnede opslagstabeller bliver virkningsløse [2].

Q5: Hvorfor er MD5 forældet?

MD5 er en hurtig, forældet hashfunktion til generelle formål, så angribere kan afprøve gæt på adgangskoder ekstremt hurtigt, især når hashene ikke er saltede [2].

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvordan beskytter en adgangskodeadministrator?

Den laver komplekse, unikke logins til hvert websted og mindsker genbrug og huskefejl.

Q7: Hvad er et brute force-angreb?

Et angreb, der systematisk afprøver alle mulige tegnkombinationer, indtil den korrekte adgangskode er fundet [4].

Q8: Hvordan hjælper spærring af konti?

Kontospærring eller hastighedsbegrænsning bremser gentagne onlinegæt og mindsker sammen med overvågning og MFA risikoen for brute force-angreb [4].

Q9: Er hovedadgangskoder sikre?

Ja, hvis de er lange, tilfældige sætninger, der aldrig genbruges andre steder.

Q10: Skal adgangskoder skiftes jævnligt?

NIST siger, at man ikke skal tvinge periodiske skift; skift dem ved belæg for kompromittering, og prioritér længde, blokeringslister og MFA [1].

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q1: Hvordan er Argon2 i forhold til bcrypt?

OWASP angiver Argon2id som sit førstevalg; dets hukommelseskrævende indstillinger modstår GPU- og ASIC-knækning bedre end bcrypt [2].

Q2: Hvad er key stretching?

En teknik, der kører en hashalgoritme i løkke tusindvis af gange for at forsinke verificeringen af adgangskoden og gøre knækning dyr [2].

Q3: Hvordan virker regnbuetabeller?

Det er forudberegnede opslagstabeller, der forbinder adgangskoder i klartekst med deres hashværdier, og som bruges til hurtigt at vende usaltede hashværdier [2].

Q4: Hvad er genbrug af lækkede logins?

Genbrug af stjålne par af brugernavn/adgangskode fra ét læk til at forsøge at få adgang til andre tjenester, især hvor folk har genbrugt adgangskoder [3].

Q5: Kan adgangskodeadministratorer hackes?

Ja. Mange krypterer dataene lokalt, så udbyderen ikke kan læse dem (zero-knowledge), og et brud på serveren afslører kun krypterede adgangskodedata, men svage hovedadgangskoder kan stadig knækkes offline.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q6: Hvad er et ordbogsangreb?

En variant af brute force, der afprøver almindelige ord, sætninger og lækkede adgangskoder.

Q7: Hvorfor foretrækkes adgangssætninger?

Adgangssætninger bruger flere tilfældige ord og giver høj entropi, der er let for mennesker at huske, men beregningsmæssigt dyr at knække [1].

Q8: Hvad betyder single sign-on (SSO) for lækager?

SSO mindsker spredningen af adgangskoder, men identitetsudbyderen bliver et værdifuldt mål, der kræver stærk, helst phishing-resistent MFA [6].

Q9: Hvad er kapring af sessioner?

En angriber skaffer eller misbruger et gyldigt sessionstoken til at udgive sig for en indlogget bruger uden at skulle bruge adgangskoden igen [5].

Q10: Hvordan opdager man password spraying?

Ved at holde øje med de samme få adgangskoder, der afprøves på mange konti, ofte langsomt for at holde sig under grænserne for kontospærring [7].

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

NIST SP 800-63B kræver, at nye adgangskoder kontrolleres mod blokeringslister over almindelige og kompromitterede adgangskoder [1].

2. SIKKERHEDSINDSIGT

Dumpet 'Collection #1' fra 2019 samlede data fra mange tidligere læk i én enorm fil med par af e-mailadresser og adgangskoder [8].

3. SIKKERHEDSINDSIGT

NIST kræver nu, at adgangskoder, der bruges som eneste godkendelsesfaktor, er mindst 15 tegn lange [1].

4. SIKKERHEDSINDSIGT

ASIC-hardware kan beregne milliarder af SHA-256-hashværdier i sekundet, hvilket gør rå SHA-hashing usikker til brugeradgangskoder [2].

5. SIKKERHEDSINDSIGT

Unikke salte betyder, at to brugere med nøjagtig den samme adgangskode får forskellige hashværdier i databasen [2].

6. SIKKERHEDSINDSIGT

Mange adgangskodeadministratorer krypterer boksens data lokalt med stærk kryptografi afledt af brugerens hovedadgangskode.

7. SIKKERHEDSINDSIGT

Credential stuffing (genbrug af lækkede logins) virker, fordi mange genbruger den samme adgangskode til webshops, netbank og e-mail [3].

8. SIKKERHEDSINDSIGT

NIST SP 800-63B siger, at verifikatorer ikke må kræve periodiske skift af adgangskoder, kun skift efter belæg for kompromittering [1].

9. SIKKERHEDSINDSIGT

At tilføje ét stort bogstav og ét symbol til en kort adgangskode stopper ikke moderne automatiserede GPU-ordbogsangreb [1].

10. SIKKERHEDSINDSIGT

MFA kan blokere mange forsøg på credential stuffing, selv efter at en adgangskode er lækket; phishing-resistent MFA er stærkere end sms-koder [3].

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale standarder fra NIST, OWASP og regler om databeskyttelse.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[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/

Facitliste: Kontrolpunkt 1 – Flervalg

1 Spørgsmål 1

Rigtigt svar: A

UNDERVISNINGSNOTE

Credential stuffing bruger automatisering til at afprøve lækkede par af brugernavn/adgangskode på andre websteder [3].

2 Spørgsmål 2

Rigtigt svar: A

UNDERVISNINGSNOTE

OWASP anbefaler Argon2id først; bcrypt er primært til ældre systemer, hvor Argon2id eller scrypt ikke er tilgængelige [2].

3 Spørgsmål 3

Rigtigt svar: A

UNDERVISNINGSNOTE

MFA kræver en ekstra faktor, så en stjålen adgangskode alene ikke kan låse kontoen op.

4 Spørgsmål 4

Rigtigt svar: A

UNDERVISNINGSNOTE

Lækdumps er lækkede samlinger af loginoplysninger, såsom samlingen Collection #1 fra 2019 [8].

5 Spørgsmål 5

Rigtigt svar: A

UNDERVISNINGSNOTE

En adgangskodeadministrator genererer og gemmer en unik, stærk adgangskode til hver konto og forhindrer dermed genbrug [3].

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Spørgsmål 6** **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Sandt: genbrugte adgangskoder lader angribere genbruge loginoplysninger lækket fra ét websted på andre websteder [3].

7 **Spørgsmål 7** **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Falsk: SHA-1 er en hurtig hashfunktion; OWASP anbefaler i stedet Argon2id, scrypt, bcrypt eller PBKDF2.

8 **Spørgsmål 8** **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Falsk: kompleksitetsregler alene kan ikke stoppe stuffing med genbrugte lækkede adgangskoder; der er brug for MFA.

9 **Spørgsmål 9** **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Sandt: overvågningstjenester gennemsøger lækdumps og kilder på dark web efter eksponerede loginoplysninger [8].

10 **Spørgsmål 10** **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Sandt: et unikt salt pr. adgangskode gør forudberegnede rainbow tables virkningsløse [2].

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

F 1. STUFFING	H 2. BCRYPT	D 3. BRUD	G 4. SALTNING
C 5. ADMINISTRATOR	B 6. MFA	A 7. REGNBUETABEL	E 8. PHISHING

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 STUFFING	2 BCRYPT	3 DATABRUD	4 SALTNING
5 ADMINISTRATOR	6 MFA		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 H – PHISHING	2 C – DATABRUD	3 B – BCRYPT	4 G – REGNBUETABEL
5 A – STUFFING	6 D – SALTNING	7 E – ADMINISTRATOR	8 F – MFA

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare STUFFING, BCRYPT og BRUD med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

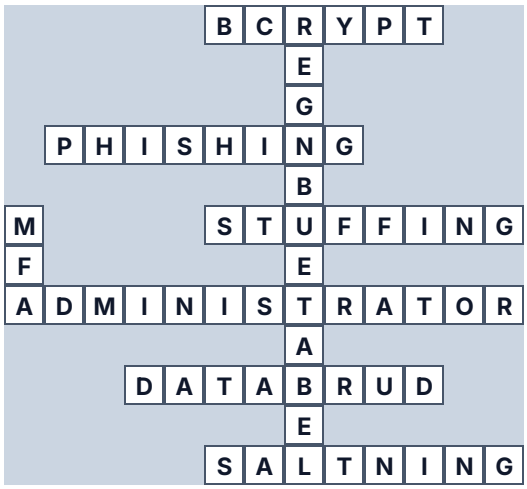
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

1 vandret: BCRYPT Langsom hashalgoritme til adgangskoder (6 bogstaver)

3 vandret: PHISHING Social manipulation, der skal stjæle loginoplysninger (8 bogstaver)

5 vandret: STUFFING Afprøvning af lækkede loginoplysninger (8 bogstaver)

6 vandret: ADMINISTRATOR Adgangskode...: værktøj til opbevaring af loginoplysninger (13 bogstaver)

7 vandret: DATABRUD Uautoriseret eksponering af en database (8 bogstaver)

8 vandret: SALTNING Tilføjelse af tilfældigt salt til en adgangskodes hash (8 bogstaver)

LODRETTE NØGLER

2 lodret: REGNBUETABEL Forudberegnet tabel over hashværdier for adgangskoder (12 bogstaver)

4 lodret: MFA Kontrol af login med flere faktorer (3 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1.	NFFSITGU	STUFFING	5.	YRTBPC	BCRYPT
2.	ADDAURBT	DATABRUD	6.	NGTISNAL	SALTNING
3.	DATARORMSNITI	ADMINISTRATOR	7.	AFM	MFA
4.	ETBGELUBAREN	REGNBUETABEL	8.	SHHGPNII	PHISHING

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"BRUG UNIKKE ADGANGSKODER OG MFA"

Facit til casestudier

A Casestudie 1: Oprydning efter lækkede firmalogins

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En overvågningstjeneste advarer om, at administratorernes adgangskoder er lagt på nettet.
- Anbefalet strategi og løsning: Tilbagekald alle aktive administratorsessioner, og nulstil loginoplysningerne med en generator med høj entropi. Håndhæv phishing-resistent MFA på administratorportaler [6], rotér berørte API-nøgler, gennemgå loginlogs, find den oprindelige eksponering, og kontrollér andre privilegerede konti.

B Casestudie 2: Indførelse af sikker hashing

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En database gemmer adgangskoder som MD5-hashes uden salt, så de hurtigt kan knækkes.
- Anbefalet strategi og løsning: Tag Argon2id (eller bcrypt på ældre systemer) i brug med et unikt salt pr. bruger [2]. Pak eksisterende MD5-hashværdier ind i den nye algoritme nu, hash direkte igen ved hver brugers næste login, og gennemtving nulstilling for konti, der længe har været inaktive.