Naam: _____ Datum: _____ Score: _____

Uitgelekte wachtwoorden en beveiliging van inloggegevens

Credential stuffing, datalekken, hashalgoritmen, meervoudige authenticatie en wachtwoordbeveiliging.

LEEROVERZICHT UITGELEKTE WACHTWOORDEN

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door wachtwoordlekken en de beveiliging van inloggegevens. Je verkent credential stuffing, datalekken, hashingalgoritmen, multifactorauthenticatie en wachtwoordmanagers.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers cyberbeveiliging en dreigingspreventie.**
- [ ] **Deel 5-7: Los kruiswoord- en woordzoekpuzzels op.**
- [ ] **Deel 8-9: Los casestudy's en de codeopdracht op.**
- [ ] **Deel 10: Bekijk de pagina's met veelgestelde vragen (basis en gevorderd).**
- [ ] **Deel 11: Ontdek 10 interessante feiten uit de praktijk.**
- [ ] **Bonus: Snel denken-uitdaging.**

Open de VPN.com-gids over cyberbeveiliging

URL: https://www.vpn.com/nl/cyberbeveiliging/wachtwoorden-lek/

Jouw leertraject: wachtwoordbeveiliging

- Begrijp de risico's van blootgestelde inloggegevens op darkwebforums.
- Voer multifactorauthenticatie (MFA) en monitoring van gecompromitteerde inloggegevens in.
- Ontwerp bedrijfsbeveiligingsmaatregelen tegen gerichte social-engineeringoplichting.

INSTRUCTIES VOOR DE GIDS OVER UITGELEKTE WACHTWOORDEN

Beantwoord de meerkeuzevragen en de vragen waar/onwaar, vul de zinnen aan met behulp van de woordenbank, koppel de definities en los de kruiswoordpuzzel en de woordzoeker op. Pas je kennis toe op bescherming van inloggegevens. Sluit af met de bonusopdracht Snel denken.

UITGELEKTE WACHTWOORDEN EN BEVEILIGING VAN INLOGGEGEVENS (INLEIDING)

Wachtwoordlekken maken inloggegevens zichtbaar op openbare websites en het dark web. Unieke wachtwoorden uit een wachtwoordmanager, controle op gelekte wachtwoorden en meerfactorauthenticatie (MFA) verkleinen het risico op credential stuffing, terwijl gezouten, trage wachtwoordhashing de schade beperkt als een wachtwoorddatabase wordt gestolen.

LEES ELK CONTROLEPUNT ZORGVULDIG EN KIES OF SCHRIJF HET JUISTE ANTWOORD.

Controlepunt 1: Meerkeuzeopdracht

1. Wat is credential stuffing?

- A. Met automatisering gelekte combinaties van gebruikersnaam en wachtwoord op meerdere sites testen
- B. Lokale databaseopslagbestanden versleutelen
- C. Webservers overspoelen met netwerkverkeersaanvragen
- D. Toetsenbordinvoer heimelijk bewaken

2. Welk algoritme noemt OWASP tegenwoordig als eerste keuze voor het opslaan van wachtwoorden?

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

3. Hoe beperkt multifactorauthenticatie (MFA) het risico van gelekte wachtwoorden?

- A. Het vereist een extra verificatiefactor, dus een gestolen wachtwoord alleen is niet genoeg
- B. Het wijzigt het wachtwoord elk uur automatisch
- C. Het versleutelt de gebruikersnaam tijdens de verzending
- D. Het waarschuwt het kredietbureau voor frauduleuze verzoeken

4. Wat is een datalek-dump?

- A. Een verzameling gelekte inloggegevens van gebruikers die online is gepubliceerd of op hackerforums wordt verkocht
- B. Een back-up van databasebestanden die extern wordt opgeslagen
- C. Een tijdelijke cache van logs van de webserver
- D. Een beheertool om gebruikerswachtwoorden te resetten

5. Wat is de rol van een wachtwoordmanager?

- A. Voor elk account unieke, sterke wachtwoorden genereren en opslaan
- B. Netwerkverkeer bewaken op lekken van wachtwoorden
- C. Geautomatiseerde brute-forceaanvallen bij de gateway blokkeren
- D. Opslagblokken van de database scannen op onversleutelde wachtwoorden

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Het hergebruiken van wachtwoorden voor meerdere accounts vergroot het risico op credential stuffing.

- ◯ Waar
- ◯ Onwaar

7 Vraag 7

7. SHA-1 is een aanbevolen hashfunctie voor de opslag van moderne wachtwoorden.

- ◯ Waar
- ◯ Onwaar

8 Vraag 8

8. Het afdwingen van wachtwoordcomplexiteit alleen (zonder MFA) stopt credential stuffing volledig.

- ◯ Waar
- ◯ Onwaar

9 Vraag 9

9. Tools voor darkwebmonitoring scannen het internet op gecompromitteerde bedrijfsinloggegevens.

- ◯ Waar
- ◯ Onwaar

10 Vraag 10

10. Gesalte hashes voegen unieke willekeurige gegevens toe aan wachtwoorden voordat ze worden gehasht, om rainbowtable-aanvallen te verslaan.

- ◯ Waar
- ◯ Onwaar

Controlepunt 3: Kernbegrippen invullen

Lees elke zin hieronder en vul de open plek in met de juiste term uit de woordenbank.

1. Het testen van gelekte inloggegevens bij veel webapplicaties heet credential _____ .
2. Een traag, adaptief hashalgoritme voor wachtwoorden dat OWASP nog steeds accepteert, is _____ .
3. Het op internet blootstellen van vertrouwelijke databasebestanden is een _____ .
4. Het toevoegen van willekeurige waarden aan wachtwoorden vóór het hashen heet _____ .
5. Een veilige lokale database voor inloggegevens van gebruikers is een _____ .
6. Het toevoegen van een tweede verificatiestap bij het inloggen gebeurt met _____ .

WOORDENBANK

BCRYPT DATALEK MFA-VERIFICATIE PHISHING REGENBOOGTABEL SALTING STUFFING WACHTWOORDMANAGER

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

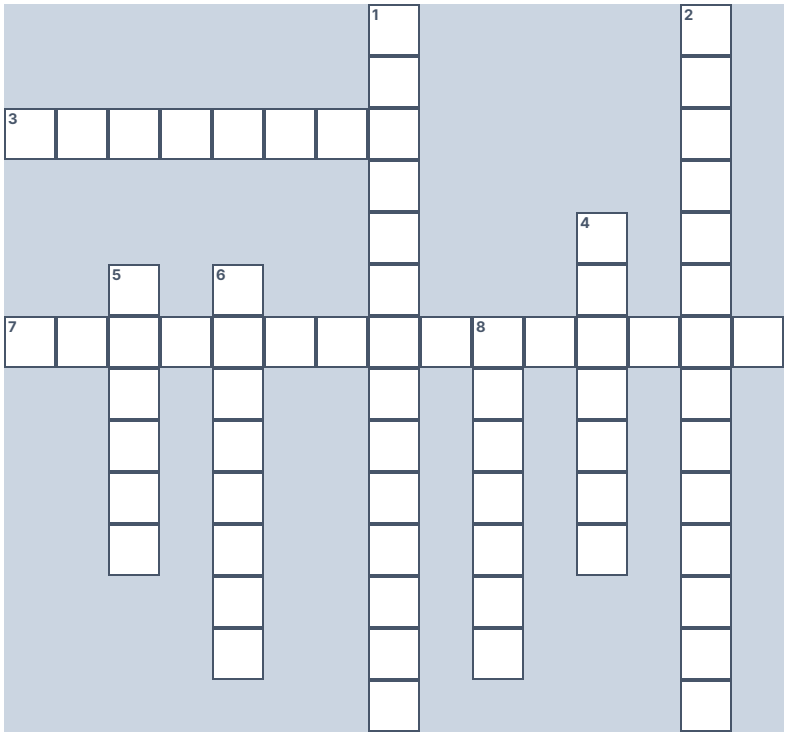
DEFINITIES KOPPELEN

Koppel elke term aan de linkerkant aan de juiste definitie aan de rechterkant door de bijbehorende letter (A-H) in het invulvak te schrijven.

☐	1. STUFFING	A	Vooraf berekende tabel met wachtwoordhashes.
☐	2. BCRYPT	B	Aanmeldcontrole met meerdere factoren.
☐	3. DATALEK	C	Tool voor het opslaan van inloggegevens.
☐	4. SALTING	D	Ongeautoriseerde blootstelling van een database.
☐	5. WACHTWOORDMANAGER	E	Social engineering om inloggegevens te stelen.
☐	6. MFA	F	Gelekte inloggegevens testen.
☐	7. RAINBOW	G	Willekeurige salt aan de wachtwoordhash toevoegen.
☐	8. PHISHING	H	Traag algoritme voor wachtwoordhashing.

Controlepunt 5: Kruiswoordpuzzel

Los de kruiswoordpuzzel op door letters in de actieve witte vakjes te typen. De nummers komen overeen met de aanwijzingen hieronder.



HORIZONTAAL

3. Social engineering om inloggegevens te stelen. (8)

7. Tool voor het opslaan van inloggegevens. (15)

VERTICAAL

1. Vooraf berekende tabel met wachtwoordhashes. (14)

2. Inlogcontrole met meerdere factoren. (14)

4. Willekeurige salt toevoegen aan een wachtwoordhash. (7)

5. Traag hashalgoritme voor wachtwoorden. (6)

6. Het testen van gelekte inloggegevens. (8)

8. Ongeautoriseerde blootstelling van een database. (7)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

Gebruikers van schermlezers en toetsenborden kunnen de antwoorden van de kruiswoordpuzzel rechtstreeks typen in de tekstvelden hieronder.

HORIZONTAAL

3 horizontaal: Social engineering om inloggegevens te stelen. (8 letters):

7 horizontaal: Tool voor het opslaan van inloggegevens. (15 letters):

VERTICAAL

1 verticaal: Vooraf berekende tabel met wachtwoordhashes. (14 letters):

2 verticaal: Inlogcontrole met meerdere factoren. (14 letters):

4 verticaal: Willekeurige salt toevoegen aan een wachtwoordhash. (7 letters):

5 verticaal: Traag hashalgoritme voor wachtwoorden. (6 letters):

6 verticaal: Het testen van gelekte inloggegevens. (8 letters):

8 verticaal: Ongeautoriseerde blootstelling van een database. (7 letters):

Controlepunt 6: Verborgen woorden zoeken

Zoek de 8 belangrijkste vakwoorden die in het onderstaande rooster verborgen zijn. Woorden kunnen horizontaal, verticaal of diagonaal staan.

A F G O K N D W N C D H I B A

P R N L P W T A I Y M F L Y S

G X I W H T F C R T F N E U K

R D H T S P L H P L A M B S H

K P S H Y Y P T L W V U A N Y

Q Q I B A R L W P M E B T L S

I F H I S C N O Y B R Z G Z A

Y B P N T B V O X M I C O F L

K P W Q U Q X R H E F Y O C T

E W L F F G H D Z W I C B O I

L R J X F X R K K Z C A N N N

A R Z R I M G L S W A G E L G

T W J B N Y C U C Y T O G U Z

A O Z U G T B I H V I P E X C

D N M H P X Y S Z X E H R O I

WOORDENLIJST

STUFFING BCRYPT DATALEK SALTING WACHTWOORDKLUIS MFAVERIFICATIE REGENBOOGTABEL PHISHING

Controlepunt 6, alternatief: Toegankelijk woordenschat koppelen

Koppel elk van de 8 vaktermen uit de woordzoeker aan de juiste definitie door de letter (A-H) in de lege ruimte te schrijven.

BEGRIPPEN

- **A. STUFFING**
- **B. BCRYPT**
- **C. DATALEK**
- **D. SALTING**
- **E. WACHTWOORDKLUIS**
- **F. MFAVERIFICATIE**
- **G. REGENBOOGTABEL**
- **H. PHISHING**

DEFINITIES EN KOPPELVELDEN

1. Social engineering om inloggegevens te stelen.
2. Ongeautoriseerde blootstelling van een database.
3. Traag hashalgoritme voor wachtwoorden.
4. Vooraf berekende tabel met wachtwoordhashes.
5. Het testen van gelekte inloggegevens.
6. Willekeurige salt toevoegen aan een wachtwoordhash.
7. Tool voor het opslaan van inloggegevens.
8. Inlogcontrole met meerdere factoren.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van cyberbeveiliging te onthullen. Schrijf je antwoorden in de invulvelden.

1. NFFSITGU
2. DTKELAA
3. WCDAIWRKLH OSOUT
4. EOETEGBLOB ARGN
5. YRTBPC
6. NLISTGA
7. AICMIFAERTF VIE
8. SHHGPNII

Bonusopdracht: Snel denken

3 ANTWOORDEN PER CATEGORIE. WIE DE LIJST ALS EERSTE INVULT, WINT.

1	Veilige gewoonten die je vandaag kunt beginnen			
2	Regels voor een sterk wachtwoord			
3	Wachtwoordmanagers die je kent			
4	Beveiligingstools die je kent			
5	Waarschuwingssignalen in een e-mail			
6	Leuke woorden voor een lange wachtzin			
7	Manieren om zonder wachtwoord in te loggen			
8	Informatie die je nooit zou moeten delen			
9	Redenen om software bij te werken			
10	Dingen die je doet als een wachtwoord uitlekt			
11	Accounts die MFA nodig hebben			
12	Plekken waar wachtwoorden nooit opgeslagen mogen worden			
13	Tekenen dat een computer is geïnfecteerd			
14	Slechte wachtwoorden die mensen gebruiken			
15	Dingen waarvan je een back-up maakt			

Controlepunt 8: Casestudy's cyberbeveiliging

Pas de concepten die je hebt geleerd toe om de onderstaande praktijkscenario's op te lossen.

CASESTUDY 1: HERSTEL NA EEN LEK VAN ZAKELIJKE INLOGGEGEVENS

👷

Scenario: Een monitoringdienst voor het dark web waarschuwt een organisatie dat een databasedump met wachtwoorden van systeembeheerders van het bedrijf online is gepubliceerd.

Discussievraag: Analyseer de risico's van het lekken van inloggegevens en stel een strategie voor het opnieuw instellen door beheerders voor.

CASESTUDY 2: STANDAARDEN VOOR WACHTWOORDHASHING IMPLEMENTEREN

👷

Scenario: Een bedrijfsdatabase slaat wachtwoorden van gebruikers momenteel op met verouderde MD5-hashes zonder cryptografische salt, waardoor ze kwetsbaar zijn voor snelle extractie.

Discussievraag: Ontwerp een migratiestrategie om het hashingalgoritme van de database te upgraden.

Controlepunt 9: De code ontcijferen

Een cyberbeveiligingsprofessional beschermt netwerkmiddelen tegen online bedreigers. Gebruik de onderstaande letter-naar-cijfersleutel om het bericht te ontcijferen door de bijbehorende letters in de lege vakjes te schrijven.

LETTER-NAAR-CIJFER-VERSLEUTELINGSSLEUTEL

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

2	5	22	5	9	12	9	7		7	5	12	5	11	20	5

23	1	3	8	20	23	15	15	18	4	5	14		13	5	20		13	6	1

Ontcijferd bericht:

TIP: ELK GETAL STAAT VOOR DE POSITIE VAN DIE LETTER IN HET ALFABET (BIJV. 1 = A, 2 = B, 26 = Z).

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel A)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q1: Wat is een wachtwoordlek?

Een wachtwoordlek treedt op wanneer inloggegevens van gebruikers worden blootgesteld door datalekken of verkeerd geconfigureerde servers.

Q2: Hoe vinden hackers uitgelekte wachtwoorden?

Hackers doorzoeken darkwebforums, openbare databasedumps en pastesites waar gegevens uit datalekken worden gepubliceerd [8].

Q3: Is hergebruik van wachtwoorden gevaarlijk?

Ja, want als één site is gecompromitteerd, kunnen hackers dezelfde inloggegevens op duizenden andere platforms uitproberen [3].

Q4: Wat is een cryptografische salt?

Een salt is willekeurige data die vóór het hashen aan een wachtwoord wordt toegevoegd, waardoor aanvallen met vooraf berekende opzoektabellen niet werken [2].

Q5: Waarom is MD5 verouderd?

MD5 is een snelle, verouderde algemene hash, dus aanvallers kunnen wachtwoordgokken extreem snel testen, vooral als de hashes geen salt hebben [2].

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel B)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q6: Hoe beschermt een wachtwoordmanager gebruikers?

Het genereert automatisch complexe, unieke inloggegevens voor elke site, wat menselijke geheugenfouten en hergebruik vermindert.

Q7: Wat is een brute-forceaanval?

Een aanval die systematisch elke mogelijke tekencombinatie test totdat het juiste wachtwoord is gevonden [4].

Q8: Hoe helpt accountblokkering?

Vergrendeling of snelheidsbeperking vertraagt herhaald online raden en verkleint, in combinatie met monitoring en MFA, het risico op brute-force-aanvallen [4].

Q9: Zijn hoofdwachtwoorden veilig?

Ze zijn veilig als het passphrases met hoge entropie zijn die nooit op andere websystemen worden hergebruikt.

Q10: Moeten wachtwoorden regelmatig worden gewijzigd?

NIST zegt dat je periodieke wijzigingen niet moet afdwingen; wijzig ze bij aanwijzingen voor een compromittering en geef prioriteit aan lengte, blokkeerlijsten en MFA [1].

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel C)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe verhoudt Argon2 zich tot bcrypt?

OWASP noemt Argon2id als eerste keuze; de geheugenintensieve instellingen ervan bieden beter weerstand tegen kraken met GPU's en ASIC's dan bcrypt [2].

Q2: Wat is key stretching?

Een techniek waarbij een hashingalgoritme duizenden keren wordt herhaald om het verifiëren van wachtwoorden te vertragen, waardoor kraken duur wordt [2].

Q3: Hoe werken rainbow tables?

Het zijn vooraf berekende opzoektabellen die wachtwoorden in platte tekst aan hun hashes koppelen en worden gebruikt om hashes zonder salt snel om te keren [2].

Q4: Wat is het hergebruiken van inloggegevens (credential recycling)?

Gestolen combinaties van gebruikersnaam en wachtwoord uit één datalek hergebruiken om toegang te proberen te krijgen tot andere diensten, vooral wanneer mensen wachtwoorden hebben hergebruikt [3].

Q5: Kunnen wachtwoordmanagers gehackt worden?

Ja. Veel gebruiken zero-knowledge-versleuteling, zodat een serverinbraak alleen versleutelde kluizen blootlegt, maar zwakke hoofdwachtwoorden kunnen nog steeds offline worden gekraakt.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel D)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Wat is een woordenboekaanval?

Een variant van brute force die veelvoorkomende woorden, zinnen en eerder gelekte wachtwoorden test in plaats van willekeurige letters.

Q7: Waarom hebben wachtzinnen de voorkeur?

Wachtzinnen gebruiken meerdere willekeurige woorden, wat een hoge entropie oplevert die voor mensen makkelijk te onthouden is maar rekenkundig duur om te kraken [1].

Q8: Hoe beïnvloedt single sign-on (SSO) het lekken van wachtwoorden?

SSO beperkt wildgroei van wachtwoorden, maar de identiteitsprovider wordt een doelwit van hoge waarde dat sterke, bij voorkeur phishingbestendige MFA nodig heeft [6].

Q9: Wat is sessiekaping?

Een aanvaller verkrijgt of misbruikt een geldig sessietoken om zich voor te doen als een ingelogde gebruiker zonder het wachtwoord opnieuw nodig te hebben [5].

Q10: Hoe detecteer je password spraying?

Door te letten op dezelfde paar wachtwoorden die op veel accounts worden geprobeerd, vaak langzaam om onder de blokkeerdrempels te blijven [7].

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

Bekijk feiten uit de praktijk over beveiligingsincidenten, verdedigingsmechanismen en compliancenormen.

1. BEVEILIGINGSINZICHT

NIST SP 800-63B vereist dat nieuwe wachtwoorden worden gecontroleerd aan de hand van blokkeerlijsten met veelgebruikte en gecompromitteerde wachtwoorden [1].

2. BEVEILIGINGSINZICHT

De 'Collection #1'-dump uit 2019 voegde gegevens uit veel eerdere datalekken samen tot één enorm bestand met combinaties van e-mailadressen en wachtwoorden [8].

3. BEVEILIGINGSINZICHT

NIST vereist nu dat wachtwoorden die als enige authenticatiefactor worden gebruikt minstens 15 tekens lang zijn [1].

4. BEVEILIGINGSINZICHT

ASIC-hardware kan miljarden SHA-256-hashes per seconde berekenen, waardoor ruwe SHA-hashing onveilig is voor gebruikerswachtwoorden [2].

5. BEVEILIGINGSINZICHT

Unieke salts betekenen dat twee gebruikers met precies hetzelfde wachtwoord verschillende hashes in de database krijgen [2].

6. BEVEILIGINGSINZICHT

Veel wachtwoordmanagers versleutelen de kluisgegevens lokaal met sterke cryptografie die is afgeleid van het hoofdwachtwoord van de gebruiker.

7. BEVEILIGINGSINZICHT

Credential stuffing werkt omdat veel mensen hetzelfde wachtwoord hergebruiken voor accounts bij webwinkels, banken en e-mail [3].

8. BEVEILIGINGSINZICHT

NIST SP 800-63B zegt dat verifiers geen periodieke wachtwoordwijzigingen mogen eisen, alleen wijzigingen na aanwijzingen voor een compromittering [1].

9. BEVEILIGINGSINZICHT

Een enkele hoofdletter en een symbool aan een kort wachtwoord toevoegen houdt moderne geautomatiseerde GPU-woordenboekaanvallen niet tegen [1].

10. BEVEILIGINGSINZICHT

MFA kan veel aanvallen met hergebruikte inloggegevens (credential stuffing) blokkeren, zelfs nadat een wachtwoord is gelekt; phishingbestendige MFA is sterker dan sms-codes [3].

Technische referenties en bronnen

De studiegids en de interactieve puzzels zijn samengesteld uit wereldwijde NIST- en OWASP-standaarden en standaarden voor naleving van gegevensprivacy.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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/

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: A

DOCENTENNOTITIE

Credential stuffing gebruikt automatisering om gelekte combinaties van gebruikersnaam en wachtwoord op andere sites te proberen [3].

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

OWASP beveelt Argon2id als eerste aan; bcrypt is vooral bedoeld voor verouderde systemen waar Argon2id of scrypt niet beschikbaar zijn [2].

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

MFA vereist een extra factor, dus een gestolen wachtwoord alleen kan het account niet ontgrendelen [3].

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Breach-dumps zijn verzamelingen van gelekte inloggegevens, zoals de compilatie Collection #1 uit 2019 [8].

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Een wachtwoordmanager genereert en bewaart een uniek, sterk wachtwoord voor elk account, waardoor hergebruik wordt voorkomen [3].

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Vraag 6** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Waar: hergebruikte wachtwoorden laten aanvallers inloggegevens die van één site zijn gelekt, op andere sites opnieuw gebruiken [3].

7 **Vraag 7** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onwaar: SHA-1 is een snelle hash; OWASP beveelt in plaats daarvan Argon2id, scrypt, bcrypt of PBKDF2 aan [2].

8 **Vraag 8** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onwaar: complexiteitsregels alleen kunnen stuffing met hergebruikte gelekte wachtwoorden niet stoppen; MFA is nodig [3].

9 **Vraag 9** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Waar: monitoringdiensten doorzoeken breach-dumps en bronnen op het dark web naar blootgestelde inloggegevens [8].

10 **Vraag 10** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Waar: een uniek salt per wachtwoord maakt vooraf berekende rainbow tables nutteloos [2].

Woordenlijstsleutels en beoordelingsrubriek

Beoordelingsrubriek voor docenten: Geef 1 punt voor elke juiste koppeling (totaal 8 punten) en elk juist contextbegrip (totaal 6 punten).

CONTROLEPUNT 4: ANTWOORDEN BEGRIPPEN KOPPELEN

F 1. STUFFING	H 2. BCRYPT	D 3. DATALEK	G 4. SALTING
C 5. WACHTWOORDMANAGER	B 6. MFA	A 7. RAINBOW	E 8. PHISHING

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 STUFFING	2 BCRYPT	3 DATALEK	4 SALTING
5 WACHTWOORDMANAGER	6 MFA-VERIFICATIE		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 H – PHISHING	2 C – DATALEK	3 B – BCRYPT	4 G – REGENBOOGTABEL
5 A – STUFFING	6 D – SALTING	7 E – WACHTWOORDKLUIS	8 F – MFAVERIFICATIE

DISCUSSIENOTITIES VOOR DOCENTEN

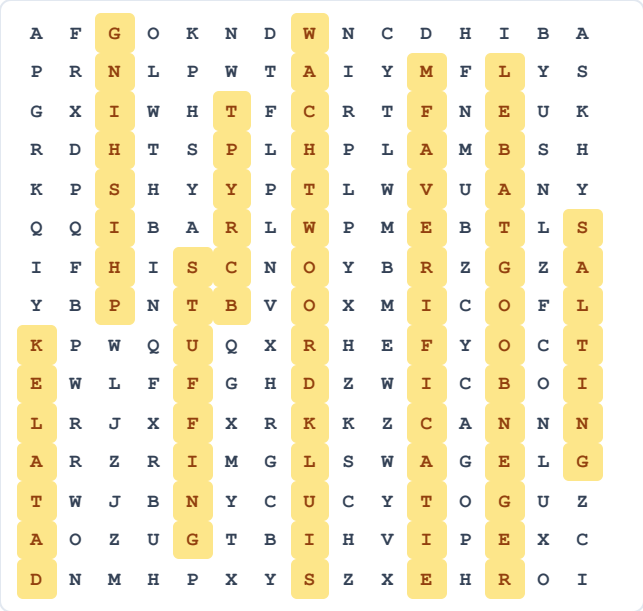
Kernbegrippen:
Controleer of leerlingen STUFFING, BCRYPT en DATALEK in eigen woorden kunnen uitleggen en van elk een voorbeeld kunnen geven.

Casestudy's:
Laat leerlingen hun aanbevelingen onderbouwen met feiten uit het werkblad in plaats van met aannames.

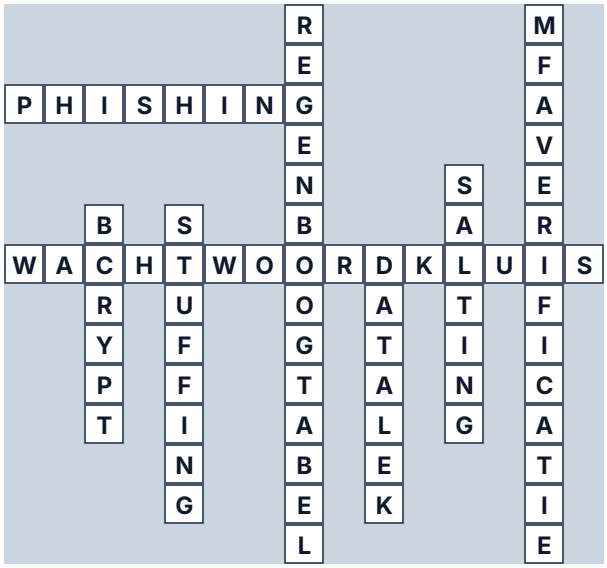
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER



OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

3 horizontaal: PHISHING Social engineering om inloggegevens te stelen. (8 letters)

7 horizontaal: WACHTWOORDKLUIS Tool voor het opslaan van inloggegevens. (15 letters)

VERTICAAL

1 verticaal: REGENBOOGTABEL Vooraf berekende tabel met wachtwoordhashes. (14 letters)

2 verticaal: MFAVERIFICATIE Inlogcontrole met meerdere factoren. (14 letters)

4 verticaal: SALTING Willekeurige salt toevoegen aan een wachtwoordhash. (7 letters)

5 verticaal: BCRYPT Traag hashalgoritme voor wachtwoorden. (6 letters)

6 verticaal: STUFFING Het testen van gelekte inloggegevens. (8 letters)

8 verticaal: DATALEK Ongeautoriseerde blootstelling van een database. (7 letters)

Sleutel voor husselwoorden en coderaadsel

Beoordelingssleutel voor de woordenschatopdracht met door elkaar gehusselde woorden en de Geheime codeopdracht.

SLEUTEL WOORDEN ORDENEN

1. NFFSITGU — STUFFING
2. DTKELAA — DATALEK
3. WCDAIWRKLHOSOUT — WACHTWOORDKLUIS
4. EOETEGBLOBARGN — REGENBOOGTABEL
5. YRTBPC — BCRYPT
6. NLISTGA — SALTING
7. AICMIFAERTFVIE — MFAVERIFICATIE
8. SHHGPNII — PHISHING

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"BEVEILIG GELEKTE WACHTWOORDEN MET MFA"

Antwoordsleutel casestudy's

A Casestudy 1: Herstel na een lek van zakelijke inloggegevens

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een dark-webmonitoringdienst waarschuwt een organisatie dat een databasedump met wachtwoorden van systeembeheerders van het bedrijf online is gepubliceerd.
- Aanbevolen strategie en oplossing: Trek alle actieve beheerderssessies in en reset de inloggegevens met een generator van hoge entropie. Dwing phishingbestendige MFA af op beheerportalen [6], roteer de getroffen API-sleutels, bekijk de inloglogs, zoek de eerste blootstelling en controleer andere accounts met bevoegdheden.

B Casestudy 2: Standaarden voor wachtwoordhashing implementeren

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een bedrijfsdatabase slaat gebruikerswachtwoorden momenteel op met verouderde MD5-hashes zonder cryptografische salt, waardoor ze kwetsbaar zijn voor snelle extractie.
- Aanbevolen strategie en oplossing: Stap over op Argon2id (of bcrypt op oudere systemen) met een unieke salt per gebruiker [2]. Verpak bestaande MD5-hashes nu in het nieuwe algoritme, hash ze rechtstreeks opnieuw bij de volgende login van elke gebruiker en dwing een reset af voor accounts die al lange tijd inactief zijn.