Nume: _____ **Data:** _____ **Punctaj:** _____

Parole divulgate și securitatea credențialelor

Credential stuffing, breșe de date, algoritmi hash, autentificare multifactor și securitatea parolelor.

PREZENTARE GENERALĂ DESPRE PAROLELE DIVULGATE

SECURIZAT
CRIPTAREA DATELOR
Standardul AES pe 256 de biți

CONFORM
STANDARDE GLOBALE
Cadrele GDPR și CCPA

ZERO-TRUST
POLITICĂ DE ACCES
Autentificare multifactor

Bun venit! Acest pachet de activități te ghidează prin scurgerile de parole și securitatea acreditărilor. Vei explora credential stuffing, breșele de date, algoritmii de hashing, autentificarea multifactor și managerii de parole.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește securitatea cibernetică și prevenirea amenințărilor.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com de securitate cibernetică

URL: https://www.vpn.com/ro/securitate-cibernetica/parole-scurse/

Harta ta de învățare despre securitatea parolelor

- Înțelege riscurile expunerii credențialelor pe forumurile din dark web.
- Implementează autentificarea multifactor (MFA) și monitorizarea datelor de autentificare compromise.
- Proiectează apărări de securitate corporative împotriva escrocheriilor de inginerie socială țintite.

INSTRUCȚIUNI DESPRE PAROLELE DIVULGATE

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre protecția datelor de autentificare. Încheie cu activitatea bonus Gândește repede.

PAROLE DIVULGATE ȘI SECURITATEA CREDENȚIALELOR (INTRODUCERE)

Divulgarea parolelor expune credențialele utilizatorilor pe site-uri publice și pe dark web. Parolele unice generate de un manager de parole, verificarea parolelor compromise și autentificarea multifactor (MFA) reduc riscul de credential stuffing, în timp ce hashing-ul lent și cu salt al parolelor limitează daunele dacă o bază de date de parole este furată.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Ce este credential stuffing?

- A. Folosirea automatizării pentru a testa combinații de nume de utilizator și parolă scurse pe mai multe site-uri
- B. Criptarea fișierelor locale de stocare a bazelor de date
- C. Supraîncărcarea serverelor web cu cereri de trafic de rețea
- D. Monitorizarea secretă a intrărilor de la tastatură

2. Ce algoritm listează OWASP drept prima alegere pentru stocarea parolelor astăzi?

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

3. Cum reduce autentificarea multifactor (MFA) riscul scurgerilor de parole?

- A. Cere un factor suplimentar de verificare, deci o parolă furată nu este suficientă
- B. Schimbă automat parola în fiecare oră
- C. Criptează numele de utilizator în timpul transmisiei
- D. Alertează biroul de credit cu privire la cererile frauduloase

4. Ce este un dump de date din urma unei breșe de securitate?

- A. O colecție de date de autentificare scurse ale utilizatorilor, publicate online sau vândute pe forumuri de hackeri
- B. O copie de rezervă a fișierelor bazei de date, stocată în afara sediului
- C. Un cache temporar al jurnalelor serverului web
- D. Un instrument administrativ folosit pentru resetarea parolelor utilizatorilor

5. Care este rolul unui manager de parole?

- A. Generarea și stocarea de parole unice și puternice pentru fiecare cont
- B. Monitorizarea traficului de rețea pentru scurgeri de parole
- C. Blocarea atacurilor automate de tip forță brută la nivelul gateway-ului
- D. Scanarea blocurilor de stocare a bazei de date în căutarea parolelor necriptate

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Reutilizarea parolelor pe mai multe conturi crește riscul de credential stuffing.

- ○ Adevărat
- ○ Fals

7 Întrebare 7

7. SHA-1 este o funcție de hash recomandată pentru stocarea modernă a parolelor.

- ○ Adevărat
- ○ Fals

8 Întrebare 8

8. Impunerea complexității parolelor, singură (fără MFA), oprește complet credential stuffing.

- ○ Adevărat
- ○ Fals

9 Întrebare 9

9. Instrumentele de monitorizare a dark web-ului scanează internetul în căutarea datelor de autentificare corporative compromise.

- ○ Adevărat
- ○ Fals

10 Întrebare 10

10. Hash-urile cu salt adaugă date aleatorii unice la parole înainte de hashing, pentru a contracara atacurile cu rainbow tables.

- ○ Adevărat
- ○ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Testarea credențialelor scurse în multe aplicații web este numită credential _____ .

2. Un algoritm lent și adaptiv de hash pentru parole, încă acceptat de OWASP, este _____ .

3. Expunerea fișierelor confidențiale ale bazelor de date pe internet este o _____ de date.

4. Adăugarea de valori aleatorii la parole înainte de hashing se numește _____ .

5. Un instrument local sigur pentru stocarea credențialelor utilizatorilor este un _____ de parole.

6. Adăugarea unui al doilea pas de verificare la conectare folosește autentificarea _____ .

BANCĂ DE CUVINTE DIN VOCABULAR

BCRYPT BREȘĂ MANAGER MULTIFACTOR PHISHING RAINBOW SALTING STUFFING

Scrie răspunsurile aici:

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

Punct de control 4: Asocierea conceptelor despre securitate

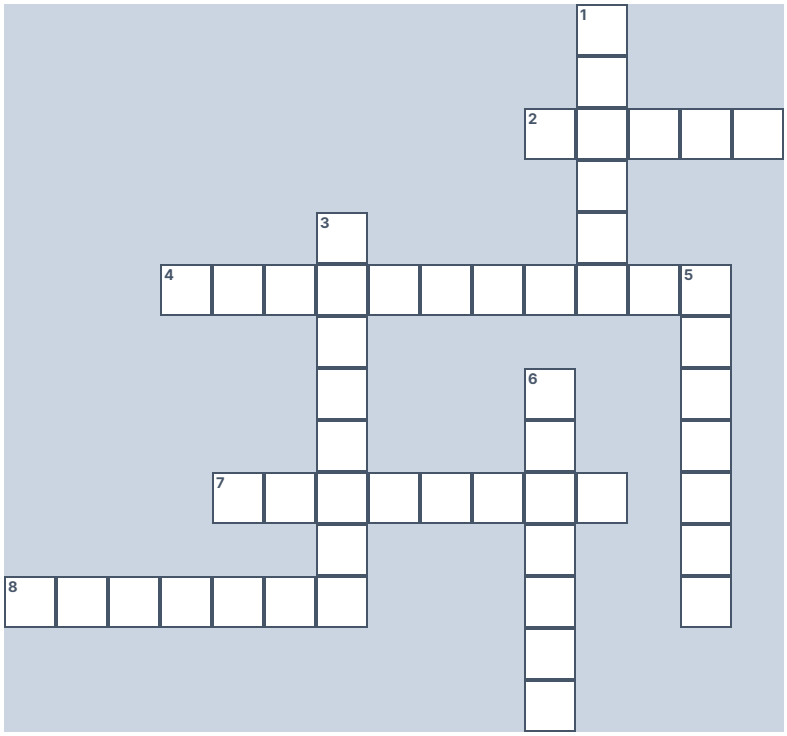
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. STUFFING	A	Tabel precalculat de hash-uri de parole.
☐	2. BCRYPT	B	Verificare de autentificare multifactor.
☐	3. BRESĂ	C	Instrument de stocare a credențialelor.
☐	4. SALTING	D	Expunerea neautorizată a unei baze de date.
☐	5. MANAGER	E	Inginerie socială pentru furtul datelor de autentificare.
☐	6. MFA	F	Testarea datelor de autentificare scurse.
☐	7. RAINBOW	G	Adăugarea unui salt aleatoriu la hash-ul parolei.
☐	8. PHISHING	H	Algoritm lent de hashing al parolelor.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

2. Expunerea neautorizată a unei baze de date. (5)

4. Verificare de autentificare cu mai mulți factori. (11)

7. Inginerie socială pentru a fura datele de autentificare. (8)

8. Adăugarea unui salt aleatoriu la hash-ul parolei. (7)

VERTICAL

1. Algoritm lent de hash pentru parole. (6)

3. Testarea credențialelor scurse. (8)

5. Tabel precalculat de hash-uri de parole. (7)

6. Instrument de stocare a credențialelor. (7)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

2 orizontal: Expunerea neautorizată a unei baze de date. (5 litere):

4 orizontal: Verificare de autentificare cu mai mulți factori. (11 litere):

7 orizontal: Inginerie socială pentru a fura datele de autentificare. (8 litere):

8 orizontal: Adăugarea unui salt aleatoriu la hash-ul parolei. (7 litere):

VERTICAL

1 vertical: Algoritm lent de hash pentru parole. (6 litere):

3 vertical: Testarea credențialelor scurse. (8 litere):

5 vertical: Tabel precalculat de hash-uri de parole. (7 litere):

6 vertical: Instrument de stocare a credențialelor. (7 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

Ț	Ș	Ș	D	K	Î	Â	A	Ă	Â	O	X	K	Î	X
J	X	T	J	C	R	M	Î	S	C	I	M	M	J	Q
P	G	M	M	Q	R	S	T	T	A	F	Â	Ș	Q	O
H	S	W	O	B	N	I	A	R	Â	L	V	C	Ș	Y
G	Ă	U	Â	Z	M	V	F	J	G	Z	T	C	M	M
N	Ș	C	R	W	U	P	S	Â	Ț	Ă	A	I	A	Z
I	E	N	C	J	L	A	C	T	O	C	E	G	N	I
H	R	C	R	Q	T	L	D	I	U	S	Z	Ș	A	G
S	B	E	R	U	I	D	A	A	R	F	O	M	G	P
I	T	X	Q	Î	F	B	S	T	S	B	F	M	E	Y
H	Ă	F	S	W	A	C	W	Î	A	R	Z	I	R	Y
P	Y	K	F	I	C	R	M	R	Î	L	L	T	N	O
G	Q	Q	G	Z	T	Y	A	O	U	F	Ț	Â	Y	G
S	Y	Ă	G	L	O	P	Z	F	Î	N	P	N	W	Â
L	Z	Y	F	X	R	T	O	V	Ț	J	U	P	Ă	N

LISTĂ DE CUVINTE DIN VOCABULAR

STUFFING BCRYPT BREȘĂ SALTING MANAGER MULTIFACTOR RAINBOW PHISHING

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR
A. STUFFING
B. BCRYPT
C. BREȘĂ
D. SALTING
E. MANAGER
F. MULTIFACTOR
G. RAINBOW
H. PHISHING

DEFINIȚII ȘI CÂMPURI DE ASOCIERE
1. Inginerie socială pentru a fura datele de autentificare.
2. Expunerea neautorizată a unei baze de date.
3. Algoritm lent de hash pentru parole.
4. Tabel precalculat de hash-uri de parole.
5. Testarea credențialelor scurse.
6. Adăugarea unui salt aleatoriu la hash-ul parolei.
7. Instrument de stocare a credențialelor.
8. Verificare de autentificare cu mai mulți factori.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. NFFSITGU
2. BĂȘER
3. AMGRNEA
4. WABNORI
5. YRTBPC
6. NLISTGA
7. CIMUARTOLFT
8. SHHGPNII

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Obiceiuri sigure pe care le poți începe de azi			
2	Reguli pentru o parolă puternică			
3	Manageri de parole pe care îi cunoști			
4	Instrumente de securitate pe care le cunoști			
5	Semnale de avertizare într-un e-mail			
6	Cuvinte amuzante pentru o frază de acces lungă			
7	Moduri de a te autentifica fără parolă			
8	Informații pe care nu ar trebui să le dai niciodată			
9	Motive pentru care ar trebui să actualizezi software-ul			
10	Lucruri de făcut când o parolă este divulgată			
11	Conturi care au nevoie de MFA			
12	Locuri în care parolele nu ar trebui stocate niciodată			
13	Semne că un calculator este infectat			
14	Parole proaste pe care le folosesc oamenii			
15	Lucruri pe care le salvezi într-o copie de rezervă			

Punct de control 8: Studii de caz despre securitatea cibernetică

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

STUDIU DE CAZ 1: REMEDIEREA SCURGERII DE CREDENȚIALE ÎNTR-O ORGANIZAȚIE



Scenariu: Un serviciu de monitorizare a dark web-ului alertează o organizație că a fost publicat online un dump de bază de date care conține parolele administratorilor de sistem ai companiei.

Întrebare de discuție: Analizează riscurile scurgerii de credențiale și propune o strategie administrativă de resetare.

STUDIU DE CAZ 2: IMPLEMENTAREA STANDARDELOR DE HASHING PENTRU PAROLE



Scenariu: O bază de date a unei companii stochează în prezent parolele utilizatorilor folosind hash-uri MD5 învechite, fără salt criptografic, ceea ce le face vulnerabile la extragerea rapidă.

Întrebare de discuție: Proiectează o strategie de migrare pentru a actualiza algoritmul de hashing al bazei de date.

Punct de control 9: Descifrează codul

Un profesionist în securitate cibernetică protejează activele rețelei de actorii amenințărilor online. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11

Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22

Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

19	21	18	24	7	13	7	1	31	2		19	1	21	18	15	7	15	7
22	5	26	21	22	7		5	26			15	18	9	1	21	7		
16	26	15	24	11	8	1	5	24	18	21								

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea A)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q1: Ce este o scurgere de parole?

O scurgere de parole apare atunci când datele de autentificare ale utilizatorilor sunt expuse prin breșe de date sau configurări greșite ale serverelor.

Q2: Cum găsesc hackerii parolele divulgate?

Hackerii scanează forumurile din dark web, descărcările publice de baze de date și site-urile de tip paste unde sunt publicate datele din breșe de securitate [8].

Q3: Este periculoasă refolosirea parolelor?

Da, pentru că, dacă un site este compromis, hackerii pot testa aceleași credențiale pe mii de alte platforme [3].

Q4: Ce este un salt criptografic?

Un salt este o dată aleatorie adăugată unei parole înainte de hashing, ceea ce face ineficiente atacurile cu tabele precalculate [2].

Q5: De ce este MD5 depășit?

MD5 este un hash de uz general rapid și depășit, astfel încât atacatorii pot testa foarte rapid ghicirile de parole, mai ales când hash-urile nu au salt [2].

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea B)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Cum protejează un manager de parole utilizatorii?

Generează automat date de autentificare complexe și unice pentru fiecare site, reducând erorile de memorie ale oamenilor și reutilizarea.

Q7: Ce este un atac prin forță brută?

Un atac care testează sistematic fiecare combinație posibilă de caractere până când este găsită parola corectă [4].

Q8: Cum ajută blocarea contului după încercări eșuate?

Blocarea sau limitarea ratei încetinește ghicirea repetată online și, combinată cu monitorizarea și MFA, reduce riscul atacurilor prin forță brută [4].

Q9: Sunt sigure parolele principale?

Sunt sigure dacă sunt fraze de acces cu entropie ridicată, care nu sunt refolosite niciodată pe alte sisteme web.

Q10: Ar trebui parolele schimbate periodic?

NIST spune să nu se impună schimbări periodice; schimbă parolele la dovezi de compromitere și dă prioritate lungimii, listelor de blocare și MFA [1].

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea C)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q1: Cum se compară Argon2 cu bcrypt?

OWASP îl listează pe Argon2id ca prima alegere; setările sale intensive în memorie rezistă mai bine decât bcrypt la spargerea cu GPU și ASIC [2].

Q2: Ce este key stretching?

O tehnică ce rulează un algoritm de hashing în buclă de mii de ori pentru a încetini procesul de verificare a parolei, făcând spargerea costisitoare [2].

Q3: Cum funcționează rainbow tables?

Sunt tabele de căutare precalculate care leagă parolele în text simplu de hash-urile lor, folosite pentru a inversa rapid hash-urile fără salt [2].

Q4: Ce este reciclarea acreditărilor?

Reutilizarea perechilor de nume de utilizator și parolă furate dintr-o breșă pentru a încerca accesarea altor servicii, mai ales acolo unde oamenii au reutilizat parolele [3].

Q5: Pot fi sparte managerele de parole?

Da. Mulți folosesc criptare zero-knowledge, astfel că o breșă la server expune doar seifuri criptate, dar parolele principale slabe pot fi totuși sparte offline.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea D)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q6: Ce este un atac de tip dicționar?

O variantă de forță brută care testează cuvinte uzuale, expresii și parole scurse în trecut, în loc de litere aleatorii.

Q7: De ce sunt preferate frazele de acces?

Frazele-parolă folosesc mai multe cuvinte aleatorii, creând o entropie ridicată care este ușor de ținut minte pentru oameni, dar costisitoare din punct de vedere computațional de spart [1].

Q8: Cum afectează autentificarea unică (SSO) scurgerile de parole?

SSO reduce proliferarea parolelor, dar furnizorul de identitate devine o țintă de mare valoare, care necesită MFA puternic, de preferință rezistent la phishing [6].

Q9: Ce este deturnarea sesiunii (session hijacking)?

Un atacator obține sau abuzează de un token de sesiune valid pentru a se da drept un utilizator autentificat, fără a mai avea nevoie de parolă [5].

Q10: Cum detectezi atacurile de tip password spraying?

Prin căutarea acelorași câteva parole încercate pe multe conturi, adesea lent, pentru a rămâne sub pragurile de blocare [7].

Partea 11: 10 fapte și perspective din lumea reală despre securitatea cibernetică

Parcurge fapte din lumea reală despre breșele de securitate, mecanismele de apărare și standardele de conformitate.

1. INFORMAȚII DESPRE SECURITATE

NIST SP 800-63B cere ca parolele noi să fie verificate în raport cu liste de blocare ale parolelor comune și compromise [1].

2. INFORMAȚII DESPRE SECURITATE

Setul de date „Collection #1" din 2019 a unit datele din multe breșe anterioare într-un singur fișier uriaș cu perechi de e-mail și parolă [8].

3. INFORMAȚII DESPRE SECURITATE

NIST cere acum ca parolele folosite ca unic factor de autentificare să aibă cel puțin 15 caractere [1].

4. INFORMAȚII DESPRE SECURITATE

Hardware-ul ASIC poate calcula miliarde de hash-uri SHA-256 pe secundă, ceea ce face hashing-ul SHA simplu nesigur pentru parolele utilizatorilor [2].

5. INFORMAȚII DESPRE SECURITATE

Sărurile unice înseamnă că doi utilizatori cu exact aceeași parolă primesc hash-uri diferite în baza de date [2].

6. INFORMAȚII DESPRE SECURITATE

Mulți manageri de parole criptează local datele seifului cu criptografie puternică derivată din parola principală a utilizatorului.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Credential stuffing funcționează deoarece mulți oameni reutilizează aceeași parolă pentru conturile de comerț electronic, bancare și de e-mail [3].

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

NIST SP 800-63B spune că verificatorii nu trebuie să ceară schimbări periodice ale parolelor, ci doar schimbări după dovezi de compromitere [1].

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Adăugarea unei singure litere majuscule și a unui simbol la o parolă scurtă nu oprește atacurile automate moderne cu dicționar bazate pe GPU [1].

10. INFORMAȚII DESPRE SECURITATE

MFA poate bloca multe încercări de credential stuffing chiar și după ce o parolă a fost scursă; MFA rezistent la phishing este mai puternic decât codurile SMS [3].

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor globale NIST, OWASP și de conformitate privind confidențialitatea datelor.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[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/

Barem: Punct de control 1 – Alegere multiplă

1 **Întrebarea 1** — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Credential stuffing folosește automatizarea pentru a încerca perechi de nume de utilizator/parolă scurse pe alte site-uri [3].

2 **Întrebarea 2** — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

OWASP recomandă mai întâi Argon2id; bcrypt este folosit în principal pentru sisteme vechi, unde Argon2id sau scrypt nu sunt disponibile [2].

3 **Întrebarea 3** — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

MFA cere un factor suplimentar, deci o parolă furată nu poate debloca singură contul [3].

4 **Întrebarea 4** — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Dump-urile de brețe sunt colecții de credențiale scurse, precum compilația Collection #1 din 2019 [8].

5 **Întrebarea 5** — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Un manager de parole generează și stochează o parolă unică și puternică pentru fiecare cont, prevenind reutilizarea [3].

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Adevărat: parolele reutilizate le permit atacatorilor să reia credențialele scurse de pe un site pe alte site-uri [3].

7 Întrebarea 7

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: SHA-1 este un hash rapid; OWASP recomandă în schimb Argon2id, scrypt, bcrypt sau PBKDF2 [2].

8 Întrebarea 8

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: regulile de complexitate singure nu pot opri credential stuffing cu parole scurse reutilizate; este nevoie de MFA [3].

9 Întrebarea 9

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Adevărat: serviciile de monitorizare caută în dump-urile de breșe și în sursele de pe dark web credențiale expuse [8].

10 Întrebarea 10

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Adevărat: un salt unic pentru fiecare parolă face ineficiente tabelele rainbow precalculate [2].

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

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

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 STUFFING	2 BCRYPT	3 BREȘĂ	4 SALTING
5 MANAGER	6 MULTIFACTOR		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 H – PHISHING	2 C – BREȘĂ	3 B – BCRYPT	4 G – RAINBOW
5 A – STUFFING	6 D – SALTING	7 E – MANAGER	8 F – MULTIFACTOR

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica STUFFING, BCRYPT și BRESĂ cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

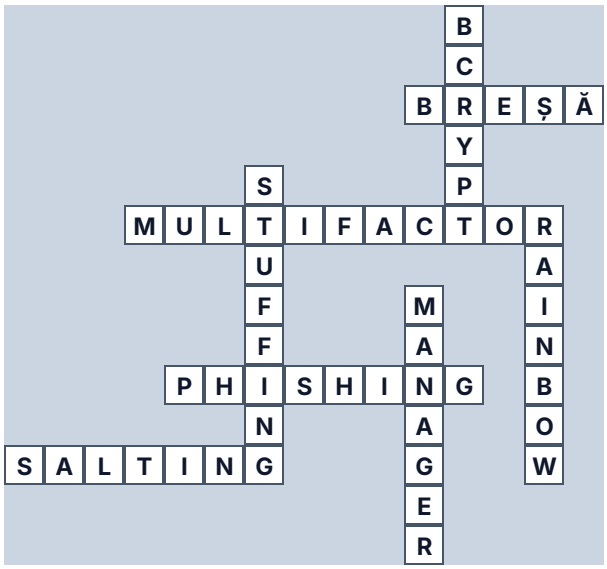
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

Ț	Ș	Ș	D	K	Î	Â	A	Ă	Â	O	X	K	Î	X
J	X	T	J	C	R	M	Î	S	C	I	M	M	J	Q
P	G	M	M	Q	R	S	T	T	A	F	Â	Ș	Q	O
H	S	W	O	B	N	I	A	R	Â	L	V	C	Ș	Y
G	Ă	U	Â	Z	M	V	F	J	G	Z	T	C	M	M
N	Ș	C	R	W	U	P	S	Â	Ț	Ă	A	I	A	Z
I	E	N	C	J	L	A	C	T	O	C	E	G	N	I
H	R	C	R	Q	T	L	D	I	U	S	Z	Ș	A	G
S	B	E	R	U	I	D	A	A	R	F	O	M	G	P
I	T	X	Q	Î	F	B	S	T	S	B	F	M	E	Y
H	Ă	F	S	W	A	C	W	Î	A	R	Z	I	R	Y
P	Y	K	F	I	C	R	M	R	Î	L	L	T	N	O
G	Q	Q	G	Z	T	Y	A	O	U	F	Ț	Â	Y	G
S	Y	Ă	G	L	O	P	Z	F	Î	N	P	N	W	Â
L	Z	Y	F	X	R	T	O	V	Ț	J	U	P	Ă	N

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: BREȘĂ Expunerea neautorizată a unei baze de date. (5 litere)

4 orizontal: MULTIFACTOR Verificare de autentificare cu mai mulți factori. (11 litere)

7 orizontal: PHISHING Inginerie socială pentru a fura datele de autentificare. (8 litere)

8 orizontal: SALTING Adăugarea unui salt aleatoriu la hash-ul parolei. (7 litere)

VERTICAL

1 vertical: BCRYPT Algoritm lent de hash pentru parole. (6 litere)

3 vertical: STUFFING Testarea credențialelor scurse. (8 litere)

5 vertical: RAINBOW Tabel precalculat de hash-uri de parole. (7 litere)

6 vertical: MANAGER Instrument de stocare a credențialelor. (7 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. NFFSITGU — **STUFFING**
2. BĂȘER — **BREȘĂ**
3. AMGRNEA — **MANAGER**
4. WABNORI — **RAINBOW**
5. YRTBPC — **BCRYPT**
6. NLISTGA — **SALTING**
7. CIMUARTOLFT — **MULTIFACTOR**
8. SHHGPNII — **PHISHING**

BAREMUL PROVOCĂRII CU CODUL SECRET

"PROTEJEAZĂ PAROLELE SCURSE CU LOGARE MULTIFACTOR"

Barem pentru studiile de caz

A Studiu de caz 1: Remedierea scurgerii de credențiale într-o organizație

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un serviciu de monitorizare a dark web-ului avertizează o organizație că un dump de bază de date care conține parolele administratorilor de sistem corporativi a fost publicat online.
- Strategie și soluție recomandată: Revocă toate sesiunile active de administrator și resetează credențialele cu un generator de entropie ridicată. Impune MFA rezistent la phishing pe portalurile de administrare [6], schimbă cheile API afectate, examinează jurnalele de autentificare, găsește expunerea inițială și verifică celelalte conturi privilegiate.

B Studiu de caz 2: Implementarea standardelor de hashing pentru parole

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O bază de date a unei companii stochează în prezent parolele utilizatorilor folosind hash-uri MD5 depășite, fără salt criptografic, ceea ce le face vulnerabile la extragere rapidă.
- Strategie și soluție recomandate: Adoptă Argon2id (sau bcrypt pe sistemele vechi) cu un salt unic pentru fiecare utilizator [2]. Învelește acum hash-urile MD5 existente în noul algoritm, rehashuiește direct la următoarea autentificare a fiecărui utilizator și forțează resetarea pentru conturile inactive de mult timp.