Emri: _____ Data: _____ Pikët: _____

Rrjedhjet e fjalëkalimeve dhe siguria e kredencialeve

Credential stuffing, shkeljet e të dhënave, algoritmet hash, autentikimi me shumë faktorë dhe siguria e fjalëkalimeve.

PËRMBLEDHJE MËSIMORE PËR RRJEDHJET E FJALËKALIMEVE

I SIGURUAR
ENKRIPTIMI I TË DHËNAVE
Standardi AES 256-bit

I PËRPUTHSHËM
STANDARDET GLOBALE
Kornizat GDPR dhe CCPA

ZERO-TRUST
POLITIKA E QASJES
Autentikim me shumë faktorë

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes rrjedhjeve të fjalëkalimeve dhe sigurisë së kredencialeve. Do të eksplorosh credential stuffing, shkeljet e të dhënave, algoritmet e hash-it, autentikimin me shumë faktorë dhe menaxherët e fjalëkalimeve.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro sigurinë kibernetike dhe parandalimin e kërcënimeve.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për sigurinë kibernetike

URL: https://www.vpn.com/sq/siguria-kibernetike/fjalekalimet-rrjedhin/

Udhërrëfyesi yt mësimor për sigurinë e fjalëkalimeve

- Kupto rreziqet e ekspozimit të kredencialeve në forumet e uebit të errët.
- Zbato autentikimin me shumë faktorë (MFA) dhe monitorimin e kredencialeve të kompromentuara.
- Harto mbrojtje sigurie për korporatat kundër mashtrimeve të synuara të inxhinierisë sociale.

UDHËZIME PËR UDHËZUESIN E RRJEDHJEVE TË FJALËKALIMEVE

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për mbrojtjen e kredencialeve. Përfundo me aktivitetin bonus Mendo shpejt.

RRJEDHJET E FJALËKALIMEVE DHE SIGURIA E KREDENCIALEVE (HYRJE)

Rrjedhjet e fjalëkalimeve ekspozojnë kredencialet e përdoruesve në sajte publike dhe në dark web. Fjalëkalimet unike nga një menaxher fjalëkalimesh, kontrolli i fjalëkalimeve të komprometuara dhe vërtetimi me shumë faktorë (MFA) zvogëlojnë rrezikun e credential stuffing, ndërsa hashimi i ngadaltë me salt i fjalëkalimeve kufizon dëmin nëse vidhet një bazë të dhënash fjalëkalimesh.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Çfarë është credential stuffing?

- A. Përdorimi i automatizimit për të testuar kombinime të rrjedhura emër përdoruesi/fjalëkalim nëpër faqe të shumta
- B. Enkriptimi i skedarëve lokalë të ruajtjes së bazës së të dhënave
- C. Mbingarkimi i serverëve të uebit me kërkesa trafiku rrjeti
- D. Monitorimi i fshehtë i hyrjeve të tastierës

2. Cilin algoritëm e rendit OWASP si zgjedhjen e parë për ruajtjen e fjalëkalimeve sot?

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

3. Si e zbut autentikimi me shumë faktorë (MFA) rrezikun e rrjedhjeve të fjalëkalimeve?

- A. Kërkon një faktor shtesë verifikimi, ndaj një fjalëkalim i vjedhur vetëm nuk mjafton
- B. E ndryshon automatikisht fjalëkalimin çdo orë
- C. E enkripton emrin e përdoruesit gjatë transmetimit
- D. E njofton byronë e kredisë për kërkesa mashtruese

4. Çfarë është një dump i shkeljes së të dhënave?

- A. Një koleksion kredencialesh të përdoruesve të rrjedhura, të publikuara online ose të shitura në forume hakerësh
- B. Një kopje rezervë e skedarëve të bazës së të dhënave e ruajtur jashtë vendit
- C. Një cache e përkohshme e logjeve të serverit të uebit
- D. Një mjet administrativ i përdorur për të rivendosur fjalëkalimet e përdoruesve

5. Cili është roli i një menaxheri fjalëkalimesh?

- A. Gjenerimi dhe ruajtja e fjalëkalimeve unike e të forta për çdo llogari
- B. Monitorimi i trafikut të rrjetit për rrjedhje fjalëkalimesh
- C. Bllokimi i sulmeve të automatizuara brute-force në gateway
- D. Skanimi i blloqeve të ruajtjes së bazës së të dhënave për fjalëkalime të paenkriptuara

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Ripërdorimi i fjalëkalimeve nëpër llogari të shumta rrit rrezikun e credential stuffing.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. SHA-1 është një funksion hash i rekomanduar për ruajtjen moderne të fjalëkalimeve.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. Zbatimi vetëm i kompleksitetit të fjalëkalimit (pa MFA) e ndalon plotësisht credential stuffing.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. Mjetet e monitorimit të web-it të errët skanojnë internetin për kredencialet e kompromentuara të korporatave.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. Hash-et me salt shtojnë të dhëna të rastësishme unike te fjalëkalimet përpara hash-imit për të mundur sulmet me rainbow table.

- ○ E vërtetë
- ○ E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Testimi i kredencialeve të rrjedhura në shumë aplikacione uebi është _____ kredencialesh.

2. Një algoritëm i ngadaltë dhe adaptiv i hashimit të fjalëkalimeve, ende i pranuar nga OWASP, është _____ .

3. Ekspozimi i skedarëve konfidencialë të bazës së të dhënave në internet është një _____ e të dhënave.

4. Shtimi i vlerave të rastësishme te fjalëkalimet para hashimit quhet _____ .

5. Një bazë e dhënash lokale e sigurt për kredencialet e përdoruesve është një _____ fjalëkalimesh.

6. Shtimi i një hapi të dytë verifikimi në hyrje përdor _____ .

BANKA E FJALËVE TË LEKSIKUT

AUTENTIKIM MFA BCRYPT MBUSHJE MENAXHER PHISHING SALTIM SHKELJE TABELË YLBERI

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

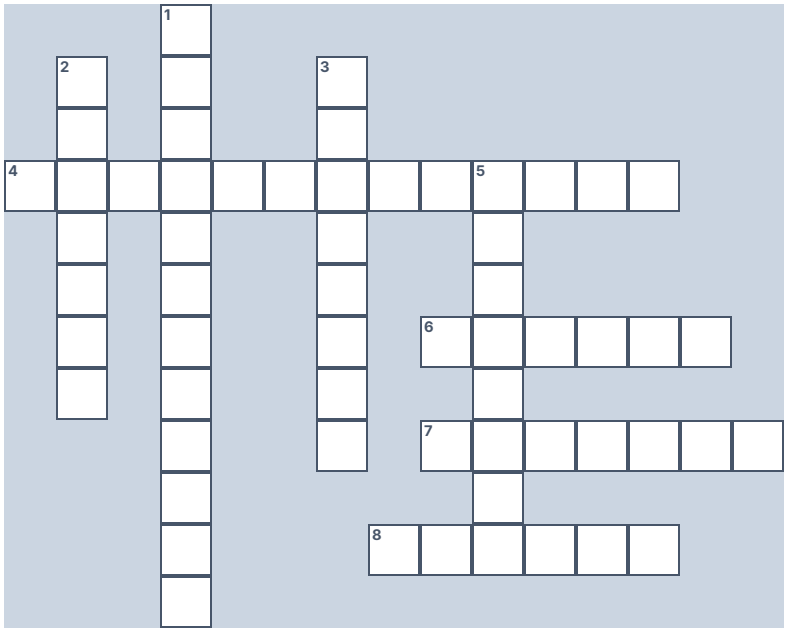
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. STUFFING	A	Tabelë e para-llogaritur e hash-eve të fjalëkalimeve.
☐	2. BCRYPT	B	Kontroll hyrjeje me shumë faktorë.
☐	3. SHKELJE	C	Mjet për ruajtjen e kredencialeve.
☐	4. SHTIM I SALT	D	Ekspozimi i paautorizuar i bazës së të dhënave.
☐	5. MENAXHUES	E	Inxhinieri sociale për të vjedhur hyrjet.
☐	6. MFA	F	Testimi i kredencialeve të rrjedhura.
☐	7. YLBER	G	Shtimi i salt të rastësishëm te hash-i i fjalëkalimit.
☐	8. PHISHING	H	Algoritëm i ngadaltë hash-imi i fjalëkalimeve.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

4. Kontroll hyrjeje me shumë faktorë. (13)

6. Shtimi i një vlere të rastësishme (salt) te hashi i fjalëkalimit. (6)

7. Ekspozim i paautorizuar i bazës së të dhënave. (7)

8. Algoritëm i ngadaltë hashimi për fjalëkalime. (6)

VERTIKALISHT

1. Tabelë e para-llogaritur e hasheve të fjalëkalimeve. (12)

2. Testimi i kredencialeve të rrjedhura. (7)

3. Inxhinieri sociale për të vjedhur kredencialet e hyrjes. (8)

5. Mjet për ruajtjen e kredencialeve. (8)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

4 horizontalisht: Kontroll hyrjeje me shumë faktorë. (13 shkronja):

6 horizontalisht: Shtimi i një vlere të rastësishme (salt) te hashi i fjalëkalimit. (6 shkronja):

7 horizontalisht: Ekspozim i paautorizuar i bazës së të dhënave. (7 shkronja):

8 horizontalisht: Algoritëm i ngadaltë hashimi për fjalëkalime. (6 shkronja):

VERTIKALISHT

1 vertikalisht: Tabelë e para-llogaritur e hasheve të fjalëkalimeve. (12 shkronja):

2 vertikalisht: Testimi i kredencialeve të rrjedhura. (7 shkronja):

3 vertikalisht: Inxhinieri sociale për të vjedhur kredencialet e hyrjes. (8 shkronja):

5 vertikalisht: Mjet për ruajtjen e kredencialeve. (8 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

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

LISTA E FJALËVE TË LEKSIKUT

MBUSHJE BCRYPT SHKELJE SALTIM MENAXHER AUTENTIKIMMFA TABELËYLBERI PHISHING

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. MBUSHJE**
- **B. BCRYPT**
- **C. SHKELJE**
- **D. SALTIM**
- **E. MENAXHER**
- **F. AUTENTIKIMMFA**
- **G. TABELËYLBERI**
- **H. PHISHING**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Inxhinieri sociale për të vjedhur kredencialet e hyrjes.
2. Ekspozim i paautorizuar i bazës së të dhënave.
3. Algoritëm i ngadaltë hashimi për fjalëkalime.
4. Tabelë e para-llogaritur e hasheve të fjalëkalimeve.
5. Testimi i kredencialeve të rrjedhura.
6. Shtimi i një vlere të rastësishme (salt) te hashi i fjalëkalimit.
7. Mjet për ruajtjen e kredencialeve.
8. Kontroll hyrjeje me shumë faktorë.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të sigurisë kibernetike. Shkruaji përgjigjet në kutitë e dhëna.

1. SJMHEUB
2. SKEJLEH
3. AEMXHREN
4. RLLBYIËEBTAE
5. YRTBPC
6. ITSLMA
7. MMKTAUINAFTIE
8. SHHGPNII

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Zakone të sigurta që mund t'i fillosh sot			
2	Rregulla për një fjalëkalim të fortë			
3	Menaxherë fjalëkalimesh që njeh			
4	Mjete sigurie që njeh			
5	Shenja paralajmëruese në një email			
6	Fjalë argëtuese për një frazëkalim të gjatë			
7	Mënyra për t'u identifikuar pa fjalëkalim			
8	Informacione që nuk duhet t'i ndash kurrë			
9	Arsye për të përditësuar softuerin			
10	Gjëra që bëhen kur rrjedh një fjalëkalim			
11	Llogari që kanë nevojë për MFA			
12	Vende ku fjalëkalimet nuk duhet të ruhen kurrë			
13	Shenja që një kompjuter është i infektuar			
14	Fjalëkalime të këqija që përdorin njerëzit			
15	Gjëra që ruan si kopje rezervë			

Pika e kontrollit 8: Studime rasti për sigurinë kibernetike

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: RIPARIMI I RRJEDHJES SË KREDENCIALEVE TË NDËRMARRJES

👷

Skenari: Një shërbim monitorimi i dark web-it njofton një organizatë se një dump i bazës së të dhënave që përmban fjalëkalimet e administratorëve të sistemit të kompanisë është publikuar online.

Pyetje për diskutim: Analizo rreziqet e rrjedhjes së kredencialeve dhe propozo një strategji administrative rivendosjeje.

STUDIMI I RASTIT 2: ZBATIMI I STANDARDEVE TË HASHIMIT TË FJALËKALIMEVE

👷

Skenari: Një bazë të dhënash enterprise aktualisht i ruan fjalëkalimet e përdoruesve duke përdorur hash të vjetruar MD5 pa kripë kriptografike, gjë që i bën të cenueshme ndaj nxjerrjes së shpejtë.

Pyetje për diskutim: Harto një strategji migrimi për përmirësimin e algoritmit të hash-it të bazës së të dhënave.

Pika e kontrollit 9: Deshifrimi i kodit

Një profesionist i sigurisë kibernetike mbron asetet e rrjetit nga aktorët e kërcënimeve online. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

15 2 20 17 12 8 12 1 14 7 13 1 14 11 15 6 22 6

20 20 12 6 5 10 23 20 1 15 6

1 23 22 6 16 22 11 13 11 15 15 8 1

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa A)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q1: Çfarë është një rrjedhje fjalëkalimi?

Një rrjedhje fjalëkalimesh ndodh kur kredencialet e hyrjes së përdoruesit ekspozohen përmes shkeljeve të të dhënave ose konfigurimeve të gabuara të serverit.

Q2: Si i gjejnë hakerët fjalëkalimet e rrjedhura?

Hakerët skanojnë forumet e dark web-it, shkarkimet publike të bazave të të dhënave dhe faqet paste ku publikohen të dhënat e shkeljeve [8].

Q3: A është i rrezikshëm ripërdorimi i fjalëkalimeve?

Po, sepse nëse një faqe kompromentohet, hakerët mund t'i testojnë të njëjtat kredenciale në mijëra platforma të tjera [3].

Q4: Çfarë është një kripë kriptografike (salt)?

Një salt është e dhënë e rastësishme e shtuar te një fjalëkalim para hash-imit, që i bën joefektive sulmet me kërkim të parallogaritur [2].

Q5: Pse është MD5 i vjetruar?

MD5 është një hash i shpejtë, i vjetruar, për qëllime të përgjithshme, ndaj sulmuesit mund t'i testojnë hamendësimet e fjalëkalimeve jashtëzakonisht shpejt, sidomos kur hash-et janë pa kripë [2].

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa B)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q6: Si i mbron përdoruesit një menaxher fjalëkalimesh?

Gjeneron automatikisht kredenciale komplekse dhe unike për çdo faqe, duke zvogëluar gabimet e kujtesës njerëzore dhe ripërdorimin.

Q7: Çfarë është një sulm me forcë brutale (brute force)?

Një sulm që teston sistematikisht çdo kombinim të mundshëm karakteresh derisa të gjendet fjalëkalimi i saktë [4].

Q8: Si ndihmon bllokimi i llogarisë pas përpjekjeve të pasuksesshme?

Bllokimi i llogarisë ose kufizimi i shpejtësisë ngadalëson hamendësimet e përsëritura në internet dhe, së bashku me monitorimin dhe MFA-në, zvogëlon rrezikun e forcës brutale [4].

Q9: A janë të sigurt fjalëkalimet kryesore?

Janë të sigurta nëse janë fraza kalimi me entropi të lartë që nuk ripërdoren kurrë në sisteme të tjera të uebit.

Q10: A duhet të ndryshohen fjalëkalimet rregullisht?

NIST thotë të mos detyrohen ndryshime periodike; ndryshoji kur ka dëshmi kompromentimi dhe jep përparësi gjatësisë, listave të bllokimit dhe MFA-së [1].

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa C)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q1: Si krahasohet Argon2 me bcrypt?

OWASP e rendit Argon2id si zgjedhjen e parë; cilësimet e tij që kërkojnë shumë memorie i rezistojnë më mirë thyerjes me GPU dhe ASIC sesa bcrypt [2].

Q2: Çfarë është zgjatja e çelësave (key stretching)?

Një teknikë që përsërit një algoritëm hash mijëra herë për të ngadalësuar procesin e verifikimit të fjalëkalimit, duke e bërë thyerjen të kushtueshme [2].

Q3: Si funksionojnë tabelat rainbow?

Janë tabela të para-llogaritura kërkimi që lidhin fjalëkalimet e thjeshta me hash-et e tyre, të përdorura për të kthyer shpejt hash-et pa salt [2].

Q4: Çfarë është riciklimi i kredencialeve?

Ripërdorimi i çifteve të vjedhura emër përdoruesi/fjalëkalim nga një shkelje për të provuar qasje në shërbime të tjera, sidomos kur njerëzit kanë ripërdorur fjalëkalimet [3].

Q5: A mund të hakohen menaxherët e fjalëkalimeve?

Po. Shumë përdorin enkriptim zero-knowledge, kështu që një shkelje e serverit ekspozon vetëm kasafortat e enkriptuara, por fjalëkalimet e dobëta kryesore mund të thyhen prapë jashtë linje.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa D)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q6: Çfarë është një sulm me fjalor (dictionary attack)?

Një variant i forcës brutale (brute-force) që teston fjalë të zakonshme, fraza dhe fjalëkalime të rrjedhura historikisht në vend të shkronjave të rastësishme.

Q7: Pse parapëlqehen frazat-fjalëkalim (passphrases)?

Frazëkalimet përdorin disa fjalë të rastësishme, duke krijuar entropi të lartë që është e lehtë për t'u mbajtur mend nga njerëzit, por kërkon shumë llogaritje për t'u thyer [1].

Q8: Si ndikon hyrja e vetme (SSO) në rrjedhjet e fjalëkalimeve?

SSO zvogëlon shumëzimin e fjalëkalimeve, por ofruesi i identitetit bëhet objektiv me vlerë të lartë që kërkon MFA të fortë, mundësisht rezistent ndaj phishing-ut [6].

Q9: Çfarë është rrëmbimi i seancës (session hijacking)?

Një sulmues merr ose abuzon me një token të vlefshëm sesioni për të imituar një përdorues të identifikuar pa pasur nevojë përsëri për fjalëkalimin [5].

Q10: Si ta zbulosh password spraying?

Duke kërkuar të njëjtat pak fjalëkalime të provuara në shumë llogari, shpesh ngadalë për të qëndruar nën pragjet e kyçjes [7].

Pjesa 11: 10 fakte dhe njohuri nga bota reale për sigurinë kibernetike

Rishiko fakte reale për shkeljet e sigurisë, mekanizmat e mbrojtjes dhe standardet e pajtueshmërisë.

1. PERSPEKTIVË PËR SIGURINË

NIST SP 800-63B kërkon që fjalëkalimet e reja të kontrollohen kundrejt listave të bllokimit të fjalëkalimeve të zakonshme dhe të kompromentuara [1].

2. PERSPEKTIVË PËR SIGURINË

Dump-i 'Collection #1' i vitit 2019 bashkoi të dhëna nga shumë cenime të mëparshme në një skedar të vetëm gjigant me çifte email-i dhe fjalëkalimi [8].

3. PERSPEKTIVË PËR SIGURINË

NIST tani kërkon që fjalëkalimet e përdorura si i vetmi faktor autentikimi të jenë të paktën 15 karaktere të gjata [1].

4. PERSPEKTIVË PËR SIGURINË

Hardueri ASIC mund të llogarisë miliarda hash SHA-256 në sekondë, duke e bërë hash-imin e papërpunuar SHA të pasigurt për fjalëkalimet e përdoruesve [2].

5. PERSPEKTIVË PËR SIGURINË

Salt-et unike nënkuptojnë që dy përdorues me fjalëkalimin e njëjtë të saktë marrin hash të ndryshëm në bazën e të dhënave [2].

6. PERSPEKTIVË PËR SIGURINË

Shumë menaxherë fjalëkalimesh e enkriptojnë lokalisht vault-in e të dhënave me kriptografi të fortë të nxjerrë nga fjalëkalimi kryesor i përdoruesit.

7. NJOHURI PËR SIGURINË

Credential stuffing funksionon sepse shumë njerëz e ripërdorin të njëjtin fjalëkalim në llogaritë e e-commerce, bankave dhe email-it [3].

8. NJOHURI PËR SIGURINË

NIST SP 800-63B thotë se verifikuesit nuk duhet të kërkojnë ndryshime periodike të fjalëkalimeve, vetëm ndryshime pas dëshmisë së kompromentimit [1].

9. NJOHURI PËR SIGURINË

Shtimi i një shkronje të madhe dhe një simboli te një fjalëkalim i shkurtër nuk i ndalon sulmet moderne automatike të fjalorit me GPU [1].

10. PERSPEKTIVË PËR SIGURINË

MFA mund të bllokojë shumë tentativa credential stuffing edhe pasi një fjalëkalim rrjedh; MFA rezistente ndaj phishing-ut është më e fortë se kodet SMS [3].

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet globale të NIST, OWASP dhe të pajtueshmërisë me privatësinë e të dhënave.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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/

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Pyetja 1** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Credential stuffing përdor automatizim për të provuar çifte emër përdoruesi/fjalëkalim të rrjedhura në faqe të tjera [3].

2 **Pyetja 2** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

OWASP rekomandon së pari Argon2id; bcrypt është kryesisht për sisteme të vjetra ku Argon2id ose scrypt nuk disponohen [2].

3 **Pyetja 3** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

MFA kërkon një faktor shtesë, ndaj një fjalëkalim i vjedhur vetëm nuk mund ta shkyçë llogarinë [3].

4 **Pyetja 4** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Dump-et e shkeljeve janë koleksione kredencialesh të rrjedhura, si përmbledhja Collection #1 e vitit 2019 [8].

5 **Pyetja 5** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Një menaxher fjalëkalimesh gjeneron dhe ruan një fjalëkalim unik e të fortë për çdo llogari, duke parandaluar ripërdorimin [3].

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Pyetja 6** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

E vërtetë: fjalëkalimet e ripërdorura u lejojnë sulmuesve t'i riprodhojnë kredencialet e rrjedhura nga një faqe në faqe të tjera [3].

7 **Pyetja 7** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: SHA-1 është hash i shpejtë; OWASP rekomandon në vend të tij Argon2id, scrypt, bcrypt ose PBKDF2 [2].

8 **Pyetja 8** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: rregullat e kompleksitetit vetëm nuk e ndalojnë stuffing-un me fjalëkalime të rrjedhura të ripërdorura; nevojitet MFA [3].

9 **Pyetja 9** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

E vërtetë: shërbimet e monitorimit kërkojnë në dump-et e shkeljeve dhe burimet e dark web-it për kredenciale të ekspozuara [8].

10 **Pyetja 10** **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

E vërtetë: një kripë unike për çdo fjalëkalim i bën joefektive tabelat rainbow të para-llogaritura [2].

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

F 1. STUFFING	H 2. BCRYPT	D 3. SHKELJE	G 4. SHTIM I SALT
C 5. MENAXHUES	B 6. MFA	A 7. YLBER	E 8. PHISHING

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 MBUSHJE	2 BCRYPT	3 SHKELJE	4 SALTIM
5 MENAXHER	6 AUTENTIKIM MFA		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 H – PHISHING	2 C – SHKELJE	3 B – BCRYPT	4 G – TABELËYLBERI
5 A – MBUSHJE	6 D – SALTIM	7 E – MENAXHER	8 F – AUTENTIKIMMFA

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë STUFFING, BCRYPT dhe SHKELJE me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

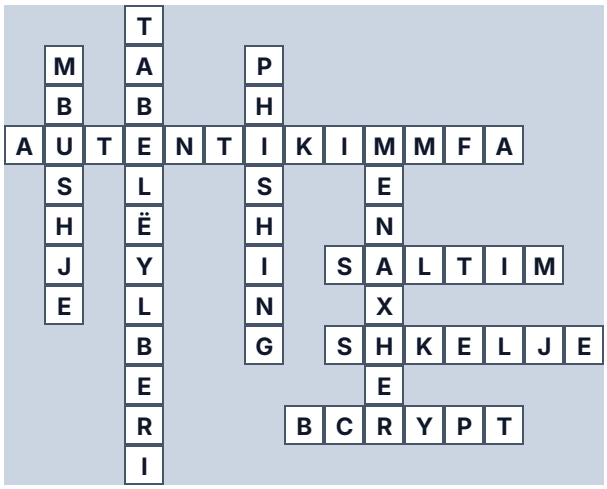
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

4 horizontalisht: AUTENTIKIMMFA Kontroll hyrjeje me shumë faktorë. (13 shkronja)

6 horizontalisht: SALTIM Shtimi i një vlere të rastësishme (salt) te hashi i fjalëkalimit. (6 shkronja)

7 horizontalisht: SHKELJE Ekspozim i paautorizuar i bazës së të dhënave. (7 shkronja)

8 horizontalisht: BCRYPT Algoritëm i ngadaltë hashimi për fjalëkalime. (6 shkronja)

VERTIKALISHT

1 vertikalisht: TABELËYLBERI Tabelë e para-llogaritur e hasheve të fjalëkalimeve. (12 shkronja)

2 vertikalisht: MBUSHJE Testimi i kredencialeve të rrjedhura. (7 shkronja)

3 vertikalisht: PHISHING Inxhinieri sociale për të vjedhur kredencialet e hyrjes. (8 shkronja)

5 vertikalisht: MENAXHER Mjet për ruajtjen e kredencialeve. (8 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. SJMHEUB — **MBUSHJE**
2. SKEJLEH — **SHKELJE**
3. AEMXHREN — **MENAXHER**
4. RLLBYIËEBTAE — **TABELËYLBERI**
5. YRTBPC — **BCRYPT**
6. ITSLMA — **SALTIM**
7. MMKTAUINAFTIE — **AUTENTIKIMMFA**
8. SHHGPNII — **PHISHING**

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"MBROJ FJALËKALIMET E RRJEDHURA ME AUTENTIKIM MFA"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Riparimi i rrjedhjes së kredencialeve të ndërmarrjes

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një shërbim monitorimi i dark web e njofton një organizatë se një depozitim i bazës së të dhënave që përmban fjalëkalimet e administratorëve të sistemit të korporatës është publikuar online.
- Strategjia dhe zgjidhja e rekomanduar: Shfuqizo të gjitha seancat aktive të administratorit dhe rivendos kredencialet me një gjenerator me entropi të lartë. Zbato MFA rezistente ndaj phishing-ut në portalet e administratorit [6], ndrysho çelësat e prekur të API-së, rishiko regjistrat e hyrjes, gjej ekspozimin fillestar dhe kontrollo llogaritë e tjera me privilegje.

B Studimi i rastit 2: Zbatimi i standardeve të hashimit të fjalëkalimeve

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një bazë të dhënash e ndërmarrjes i ruan aktualisht fjalëkalimet e përdoruesve me hash-e të vjetruara MD5 pa kripë kriptografike, duke i bërë ato të cenueshme ndaj nxjerrjes së shpejtë.
- Strategjia dhe zgjidhja e rekomanduar: Përvetëso Argon2id (ose bcrypt në sistemet e vjetra) me kripë (salt) unike për çdo përdorues [2]. Mbështill tani hash-et ekzistuese MD5 në algoritmin e ri, rihash-o drejtpërdrejt gjatë hyrjes së radhës të secilit përdorues dhe detyro rivendosjen për llogaritë joaktive prej kohësh.