Nafn: _____ Dagsetning: _____ Stig: _____

Lykilorðaleki og öryggi auðkennisupplýsinga

Innskráningarfylling, gagnalekar, tætireiknirit, fjölþátta auðkenning og lykilorðaöryggi.

YFIRLIT UM NÁMSEFNI UM LYKILORÐALEKA

VARIÐ

GAGNADULKÓÐUN

256-bita AES staðall

UPPFYLLIR KRÖFUR

ALÞJÓÐLEGIR STAÐLAR

Rammar GDPR og CCPA

ZERO-TRUST

AÐGANGSSTEFNA

Fjölþátta auðkenning

Velkomin! Þetta verkefnahefti leiðir þig í gegnum lykilorðaleka og öryggi skilríkja. Þú munt kynnast credential stuffing, gagnabrotum, kjötkássareikniritum, fjölþátta auðkenningu og lykilorðastjórum.

ÁFANGAR VERKEFNABLAÐSINS

- [ ] **Hluti 1-4: Náðu tökum á netöryggi og varnir gegn ógnum.**
- [ ] **Hluti 5-7: Leystu krossgátur og orðaleitarþrautir.**
- [ ] **Hluti 8-9: Leystu dæmisögur og dulmálsáskorun.**
- [ ] **Hluti 10: Farðu yfir síður með algengum spurningum, grunnstig og framhaldsstig.**
- [ ] **Hluti 11: Kannaðu 10 áhugaverðar staðreyndir úr raunheimum.**
- [ ] **Auka: áskorunin Hugsaðu hratt.**

Opnaðu netöryggisleiðarvísi VPN.com

URL: https://www.vpn.com/is/netoryggd/lykilord-lektu/

Námsvegvísir þinn: lykilorðaöryggi

- Skildu hættuna á að auðkenni afhjúpist á spjallborðum dökka vefsins.
- Innleiddu fjölþátta auðkenningu (MFA) og vöktun á afhjúpuðum innskráningarupplýsingum.
- Hannaðu varnir fyrirtækis gegn markvissum svikum með mannlegri blekkingu.

LEIÐBEININGAR UM LYKILORÐALEKA

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á vernd auðkenna og innskráningarupplýsinga. Ljúktu með aukaverkefninu Hugsaðu hratt.

LYKILORÐALEKAR OG ÖRYGGI AUÐKENNISUPPLÝSINGA (INNGANGUR)

Lykilorðaleki afhjúpar auðkennisupplýsingar notenda á opinberum vefsíðum og á hulduvefnum. Einstök lykilorð úr lykilorðastjóra, skimun fyrir lekum lykilorðum og fjölþátta auðkenning (MFA) draga úr hættu á endurnotkun stolinna auðkenna, en söltuð og hæg lykilorðadreifing takmarkar tjónið ef lykilorðagagnagrunni er stolið.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hvað er credential stuffing?**

- A. Að nota sjálfvirkni til að prófa lekin notendanafna- og lykilorðapör á mörgum vefsvæðum
- B. Að dulkóða gagnagrunnsskrár á staðnum
- C. Að yfirkeyra vefþjóna með umferðarbeiðnum
- D. Að fylgjast leynilega með lyklaborðsinnslætti

2 **2. Hvaða reiknirit setur OWASP í fyrsta val fyrir geymslu lykilorða í dag?**

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

3 **3. Hvernig dregur fjölþátta auðkenning (MFA) úr hættu á leka lykilorða?**

- A. Hún krefst viðbótarstaðfestingarþáttar og því nægir stolið lykilorð eitt og sér ekki
- B. Hún breytir lykilorðinu sjálfkrafa á klukkustundar fresti
- C. Hún dulkóðar notandanafnið við sendingu
- D. Hún lætur lánshæfisstofnun vita af sviksamlegum beiðnum

4 **4. Hvað er gagnaleki sem dreift er í heilu lagi (data breach dump)?**

- A. Safn lekinna notendaauðkenna sem birt eru á netinu eða seld á spjallborðum tölvuþrjóta
- B. Afrit af gagnagrunnsskrám sem er geymt á öðrum stað
- C. Tímabundið skyndiminni skráa vefþjóns
- D. Stjórnunartól til að endurstilla lykilorð notenda

5 **5. Hvert er hlutverk lykilorðastjóra?**

- A. Að búa til og geyma einkvæm, sterk lykilorð fyrir hvern reikning
- B. Að vakta netumferð vegna leka lykilorða
- C. Að loka á sjálfvirkar kerfisbundnar vélmennaárásir (brute-force) á gáttinni
- D. Að skanna geymslublokkir gagnagrunns eftir ódulkóðuðum lykilorðum

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Endurnotkun lykilorða á mörgum aðgöngum eykur hættuna á innskráningarfyllingu (credential stuffing).

○ Satt ○ Ósatt

7 Spurning 7

7. SHA-1 er ráðlögð tætifall fyrir geymslu lykilorða í nútímanum.

○ Satt ○ Ósatt

8 Spurning 8

8. Að framfylgja flækjustigi lykilorða eingöngu (án MFA) stöðvar algjörlega prófanir á stolnum lykilorðum (credential stuffing).

○ Satt ○ Ósatt

9 Spurning 9

9. Vöktunarverkfæri fyrir myrkravefinn skanna netið eftir uppljóstruðum innskráningarupplýsingum fyrirtækja.

○ Satt ○ Ósatt

10 Spurning 10

10. Saltað tætigildi bæta einstökum slembigögnum við lykilorð áður en þau eru tætt til að sigrast á árásum með regnbogatöflum.

○ Satt ○ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

Lestu hverja setningu hér að neðan og fylltu í eyðuna með réttu hugtaki úr orðabankanum.

1. Aðferðin þar sem lekin skilríki eru prófuð á mörgum vefforritum kallast _____ .

2. Hægvirkt, aðlögunarhæft reiknirit til að hasha lykilorð, sem OWASP viðurkennir enn, er _____ .

3. Birting trúnaðarskráa úr gagnagrunnum á netinu er _____ .

4. Að bæta slembigildum við lykilorð áður en þau eru hösuð kallast _____ .

5. Öruggur staðbundinn gagnagrunnur fyrir skilríki notenda er _____ .

6. Viðbótarskref til að staðfesta innskráningu notar fjölþátta _____ .

ORÐABANKI

BCRYPT FYLLINGARÁRÁS GAGNABROT LYKILORÐASAFN REGNBOGATAFLA SALTUN STAÐFESTING VEFVEIÐAR

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um öryggi

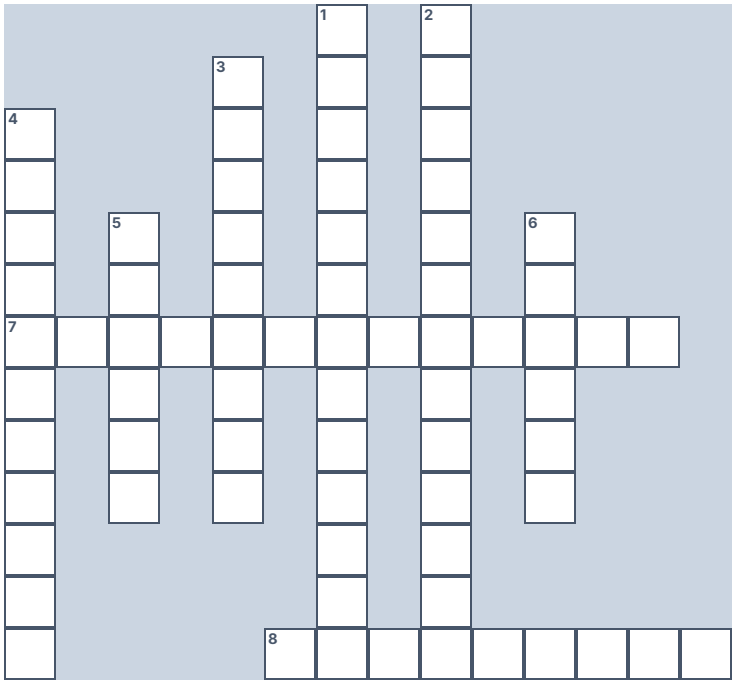
PÖRUN SKILGREININGA

Paraðu hvert hugtak til vinstri við rétta skilgreiningu til hægri með því að skrifa samsvarandi bókstaf (A-H) í útfyllanlega reitinn.

☐	1. FYLLING	A	Forreiknuð tafla yfir lykilorðatætigildi.
☐	2. BCRYPT	B	Fjölþátta innskráningarathugun.
☐	3. GAGNALEKI	C	Tól til að geyma innskráningarupplýsingar.
☐	4. SALTUN	D	Óheimil afhjúpun gagnagrunns.
☐	5. STJÓRNANDI	E	Félagsleg hagræðing til að stela innskráningarupplýsingum.
☐	6. MFA	F	Prófun á lekum innskráningarupplýsingum.
☐	7. REGNBOGI	G	Tilviljanakenndu salti bætt við lykilorðshakk.
☐	8. VEFVEIÐAR	H	Hægt kjötkássualgrím fyrir lykilorð.

Áfangi 5: Krossgáta

Leystu krossgátuna með því að slá stafi inn í virku hvítu reitina. Tölurnar vísa til vísbendinganna hér að neðan.



LÁRÉTT

7. Að prófa lekin skilríki (13)

8. Óheimil birting gagnagrunns (9)

LÓÐRÉTT

1. Fyrirframreiknuð tafla yfir hash lykilorða (13)

2. Tól til að geyma skilríki (13)

3. Félagsleg verkfræði til að stela innskráningum (9)

4. Fjölþátta athugun við innskráningu (11)

5. Slembigildi bætt við hash lykilorðs (6)

6. Hægvirkt reiknirit til að hasha lykilorð (6)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

Notendur skjálesara og lyklaborðs geta slegið svör krossgátunnar beint inn í textareitina hér að neðan.

LÁRÉTT

7 lárétt: Að prófa lekin skilríki (13 stafir):

8 lárétt: Óheimil birting gagnagrunns (9 stafir):

LÓÐRÉTT

1 lóðrétt: Fyrirframreiknuð tafla yfir hash lykilorða (13 stafir):

2 lóðrétt: Tól til að geyma skilríki (13 stafir):

3 lóðrétt: Félagsleg verkfræði til að stela innskráningum (9 stafir):

4 lóðrétt: Fjölþátta athugun við innskráningu (11 stafir):

5 lóðrétt: Slembigildi bætt við hash lykilorðs (6 stafir):

6 lóðrétt: Hægvirkt reiknirit til að hasha lykilorð (6 stafir):

Áfangi 6: Falið orð í orðaleit

Finndu 8 lykilhugtök sem eru falin í reitnum hér að neðan. Orð geta verið lárétt, lóðrétt eða á ská.

N K U T Y S Ö E H É T D A L P

F G N I T S E F Đ A T S B B Ö

A M J X S A L T U N S V C A T

S Ý J M M G H N H S F R K U L

A S Ý H B V É Þ O Æ Y Ý T H Ú

Đ Ý A P V N O Æ Ó P I P U H Ó

R X Ú Ó V Ú J A T E Ó M K Á O

O X F G P R A Đ I E V F E V R

L Ý Æ Í J V Í Æ Y Þ Ó J I Ö I

I Í N T O R B A N G A G A E I

K F Y L L I N G A R Á R Á S Á

Y U A Í É Y E J Ö J E K R N Í

L A R E G N B O G A T A F L A

F Ó J O D N B Đ G I Á Á Ó S L

P Y Ú I Æ F Æ T G Þ Y H É S Ú

ORÐALISTI

FYLLINGARÁRÁS BCRYPT GAGNABROT SALTUN LYKILORÐASAFN STAÐFESTING REGNBOGATAFLA VEFVEIÐAR

Áfangi 6, valkostur: Aðgengileg orðaforðapörun

Paraðu hvert af hugtökunum 8 úr orðaleitinni við rétta skilgreiningu með því að skrifa bókstafinn (A-H) í eyðuna.

HUGTÖK
A. FYLLINGARÁRÁS
B. BCRYPT
C. GAGNABROT
D. SALTUN
E. LYKILORÐASAFN
F. STAÐFESTING
G. REGNBOGATAFLA
H. VEFVEIÐAR

SKILGREININGAR OG PÖRUNARREITIR

____ 1. Félagsleg verkfræði til að stela innskráningum.

____ 2. Óheimil birting gagnagrunns.

____ 3. Hægvirkt reiknirit til að hasha lykilorð.

____ 4. Fyrirframreiknuð tafla yfir hash lykilorða.

____ 5. Að prófa lekin skilríki.

____ 6. Slembigildi bætt við hash lykilorðs.

____ 7. Tól til að geyma skilríki.

____ 8. Fjölþátta athugun við innskráningu.

Áfangi 7: Áskorun með ruglaðum orðum

Raðaðu stöfunum hér að neðan í rétta röð til að afhjúpa lykilhugtök um netöryggi. Skrifaðu svörin þín í reitina sem fylgja.

1. GLRÁNYAÁFRSIL

2. TGONABRAG

3. YLÐSAFNKRLOAI

4. OLTGABAGFAREN

5. YRTBPC

6. UTSLNA

7. TFSTSGINAEÐ

8. REAVVEIÐF

Aukaverkefni: Hugsaðu hratt

3 SVÖR Í HVERJUM FLOKKI. SÁ VINNUR SEM FYLLIR FYRST ÚT LISTANN.

1	Öruggar venjur sem þú getur byrjað á í dag			
2	Reglur fyrir sterkt lykilorð			
3	Lykilorðastjórar sem þú þekkir			
4	Öryggisverkfæri sem þú þekkir			
5	Viðvörunarmerki í tölvupósti			
6	Skemmtileg orð í langa lykilsetningu			
7	Leiðir til að skrá sig inn án lykilorðs			
8	Upplýsingar sem þú ættir aldrei að deila			
9	Ástæður fyrir því að uppfæra hugbúnað			
10	Hlutir til að gera þegar lykilorði er lekið			
11	Reikningar sem þurfa MFA			
12	Staðir þar sem lykilorð ætti aldrei að geyma			
13	Merki þess að tölva sé sýkt			
14	Slæm lykilorð sem fólk notar			
15	Hlutir sem þú afritar			

Áfangi 8: Dæmisögur um netöryggi

Nýttu hugtökin sem þú hefur lært til að leysa raunveruleg dæmi hér að neðan.

DÆMISAGA 1: LAGFÆRING Á LEKA INNSKRÁNINGARUPPLÝSINGA Í FYRIRTÆKI

👷

Aðstæður: Vöktunarþjónusta á myrkvefnum lætur stofnun vita að gagnagrunnsdump með lykilorðum kerfisstjóra fyrirtækisins hafi verið birtur á netinu.

Umræðuspurning: Greindu áhættu af leka auðkenna og leggðu til stjórnunarlega endurstillingaráætlun.

DÆMISAGA 2: INNLEIÐING STAÐLA FYRIR TÆTIGILDI LYKILORÐA

👷

Aðstæður: Gagnagrunnur stórfyrirtækis geymir nú lykilorð notenda með úreltum MD5-tætigildum án dulritunarsalts, sem gerir þau berskjölduð fyrir hraðri útdrætti.

Umræðuspurning: Hannaðu flutningsáætlun til að uppfæra tætireikniritið í gagnagrunninum.

Áfangi 9: Leystu dulmálið

Netöryggissérfræðingur ver netkerfiseignir gegn ógnaraðilum á netinu. Notaðu lykilinn „bókstafur í tölu“ hér að neðan til að afkóða skilaboðin með því að skrifa samsvarandi bókstafi í auðu reitina.

DULMÁLSLYKILL: STAFIR Í TÖLUR

A=1 Á=2 B=3 C=4 D=5 Đ=6 E=7 É=8 F=9 G=10 H=11 I=12

Í=13 J=14 K=15 L=16 M=17 N=18 O=19 Ó=20 P=21 Q=22 R=23 S=24

T=25 U=26 Ú=27 V=28 W=29 X=30 Y=31 Ý=32 Z=33 Þ=34 Æ=35 Ö=36

28	7	23	18	5	1	6	26		16	7	15	12	18
	16	31	15	12	16	19	23	6		17	7	6	
9	14	36	16	34	2	25	25	1		36	23	31	10	10	12

Afkóðuð skilaboð:

ÁBENDING: HVER TALA STENDUR FYRIR STÖÐU STAFSINS Í STAFRÓFINU (T.D. 1 = A, 2 = B, 36 = Ö).

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti A)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q1: Hvað er lykilorðaleki?

Lykilorðaleki verður þegar innskráningarupplýsingar notenda verða berskjaldaðar vegna gagnaleka eða rangra stillinga netþjóna.

Q2: Hvernig finna tölvuþrjótar lekin lykilorð?

Tölvuþrjótar skanna spjallborð á myrkvefnum, opinber gagnasöfn sem hefur verið lekið og afritunarsíður þar sem gögnum úr öryggisbrotum er dreift [8].

Q3: Er hættulegt að nota sama lykilorð aftur?

Já, því ef eitt vefsvæði verður fyrir broti geta tölvuþrjótar prófað sömu innskráningargögn á þúsundum annarra vettvanga [3].

Q4: Hvað er dulritunarsalt (cryptographic salt)?

Salt er tilviljanakennd gögn sem bætt er við lykilorð áður en það er hakkað, sem gerir fyrirfram reiknaðar uppflettiárásir gagnslausar [2].

Q5: Hvers vegna er MD5 úrelt?

MD5 er hröð, úrelt almenn tætifall, svo að árásaraðilar geta prófað lykilorðaágiskanir afar hratt, sérstaklega þegar tætigildin eru ósöltuð [2].

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti B)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvernig ver lykilorðastjóri notendur?

Það býr sjálfkrafa til flókin, einstök lykilorð fyrir hverja vefsíðu, sem dregur úr minnisvillum og endurnotkun.

Q7: Hvað er þrautaárás (brute force attack)?

Árás sem prófar kerfisbundið allar mögulegar stafasamsetningar þar til rétt lykilorð finnst [4].

Q8: Hvernig hjálpar reikningslæsing?

Útilokun eða hraðatakmörkun hægir á ítrekuðum nettilraunum til að giska og dregur, ásamt vöktun og fjölþátta auðkenningu, úr hættu á ágiskunarárásum [4].

Q9: Eru aðallykilorð örugg?

Þau eru örugg ef þau eru lykilsetningar með mikilli óreiðu (entropy) sem eru aldrei endurnotaðar á öðrum vefkerfum.

Q10: Ætti að skipta reglulega um lykilorð?

NIST segir að ekki eigi að þvinga fram reglubundnar breytingar; breyta skuli lykilorðum þegar sannanir um öryggisbrest koma fram og setja lengd, bannlista og MFA í forgang [1].

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti C)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig ber Argon2 sig saman við bcrypt?

OWASP setur Argon2id í fyrsta sæti; minnisfrekar stillingar þess standast betur GPU- og ASIC-dulráðningar en bcrypt [2].

Q2: Hvað er lyklateygja (key stretching)?

Tækni sem keyrir hakkaralgrím þúsundir sinnum í lykkju til að hægja á sannprófun lykilorðs og gera brot dýr [2].

Q3: Hvernig virka regnbogatöflur (rainbow tables)?

Þær eru forreiknaðar uppflettitöflur sem tengja textalykilorð við kjötkássur þeirra og eru notaðar til að snúa hratt við ósöltuðum kjötkássum [2].

Q4: Hvað er endurnotkun innskráningarupplýsinga (credential recycling)?

Að endurnota stolin pör notandanafns og lykilorðs úr einum gagnaleka til að reyna að komast inn í aðra þjónustu, sérstaklega þar sem fólk endurnotaði lykilorð [3].

Q5: Er hægt að brjótast inn í lykilorðastjóra?

Já. Mörg nota dulkóðun án þekkingar (zero-knowledge), svo innbrot í netþjón afhjúpar aðeins dulkóðaðar hirslur, en veik aðallykilorð er samt hægt að brjóta án nettengingar.

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti D)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvað er orðabókarárás (dictionary attack)?

Afbrigði af árás með ítrekuðum tilraunum sem prófar algeng orð, frasa og áður lekin lykilorð frekar en tilviljanakennda stafi.

Q7: Hvers vegna eru lykilsetningar (passphrases) frekar valdar?

Lykilsetningar nota mörg handahófskennd orð, sem skapar mikla óreiðu (entropy) sem auðvelt er fyrir fólk að muna en kostar mikla reikniorku að brjóta [1].

Q8: Hvernig hefur samþætt innskráning (SSO) áhrif á leka lykilorða?

SSO dregur úr útbreiðslu lykilorða, en auðkennisveitan verður verðmætt skotmark sem þarfnast sterkrar, helst vefveiðaþolinnar MFA [6].

Q9: Hvað er lotuarán (session hijacking)?

Árásaraðili nær í eða misnotar gilt lotutákn til að þykjast vera innskráður notandi án þess að þurfa lykilorðið aftur [5].

Q10: Hvernig greinir þú lykilorðaúðun (password spraying)?

Með því að leita að sömu fáu lykilorðunum sem eru prófuð á mörgum reikningum, oft hægt til að haldast undir lokunarmörkum [7].

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

NIST SP 800-63B krefst þess að ný lykilorð séu borin saman við bannlista yfir algeng og afhjúpuð lykilorð [1].

2. INNSÝN Í ÖRYGGI

Lekinn árið 2019, „Collection #1“, sameinaði gögn úr mörgum eldri gagnalekum í eina risastóra skrá með pörum netfanga og lykilorða [8].

3. INNSÝN Í ÖRYGGI

NIST krefst þess nú að lykilorð sem eru eini auðkenningarþátturinn séu að minnsta kosti 15 stafir að lengd [1].

4. INNSÝN Í ÖRYGGI

ASIC-vélbúnaður getur reiknað milljarða SHA-256 hakkgilda á sekúndu, sem gerir hrátt SHA-hakk óöruggt fyrir lykilorð notenda [2].

5. INNSÝN Í ÖRYGGI

Einkvæm sölt þýða að tveir notendur með nákvæmlega sama lykilorð fá ólíkar kjötkássur í gagnagrunninum [2].

6. INNSÝN Í ÖRYGGI

Margir lykilorðastjórar dulkóða hirslugögn staðbundið með sterkri dulritun sem er leidd af aðallykilorði notandans.

7. ÖRYGGISINNSÝN

Innskráningarfylling virkar vegna þess að margir endurnota sama lykilorð í netverslunum, bönkum og tölvupóstreikningum [3].

8. ÖRYGGISINNSÝN

NIST SP 800-63B segir að sannvottarar skuli ekki krefjast reglubundinna lykilorðaskipta, aðeins breytinga eftir að sannanir um öryggisbrest koma fram [1].

9. ÖRYGGISINNSÝN

Að bæta einum stórum staf og tákni við stutt lykilorð stöðvar ekki nútímalegar sjálfvirkar orðabókarárásir með skjákortum [1].

10. INNSÝN Í ÖRYGGI

MFA getur stöðvað margar tilraunir til lykilorðafyllingar (credential stuffing) jafnvel eftir að lykilorði hefur verið lekið; MFA sem stenst vefveiðar er sterkara en SMS-kóðar [3].

Tæknilegar heimildir og tilvísanir

Námsleiðbeiningarnar og gagnvirku þrautirnar eru unnar úr alþjóðlegum stöðlum NIST og OWASP og kröfum um persónuverndarsamræmi.

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[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/

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Lykilorðafylling (credential stuffing) notar sjálfvirkni til að prófa lekin pör notandanafns og lykilorðs á öðrum vefsvæðum [3].

2 **Spurning 2** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

OWASP mælir fyrst með Argon2id; bcrypt er aðallega fyrir eldri kerfi þar sem Argon2id eða scrypt eru ekki tiltæk [2].

3 **Spurning 3** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

MFA krefst viðbótarþáttar og því getur stolið lykilorð eitt og sér ekki opnað reikninginn [3].

4 **Spurning 4** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Gagnaleka-safnskrár eru safn lekinna auðkenna, svo sem Collection #1 safnið frá 2019 [8].

5 **Spurning 5** — **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Lykilorðastjóri býr til og geymir einstakt, sterkt lykilorð fyrir hvern reikning og kemur í veg fyrir endurnotkun [3].

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Satt: endurnotuð lykilorð leyfa árásaraðilum að endurspila auðkenni sem láku frá einu vefsvæði á öðrum vefsvæðum [3].

7 **Spurning 7** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: SHA-1 er hraðvirk tætifall; OWASP mælir með Argon2id, scrypt, bcrypt eða PBKDF2 í staðinn [2].

8 **Spurning 8** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: flækjureglur einar og sér stöðva ekki lykilorðafyllingu með endurnotuðum lekum lykilorðum; MFA þarf til [3].

9 **Spurning 9** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Satt: vöktunarþjónustur leita í gagnaleka-safnskrám og heimildum á dökka vefnum að berskjölduðum auðkennum [8].

10 **Spurning 10** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Satt: einstakt salt fyrir hvert lykilorð gerir fyrirfram reiknaðar regnbogatöflur gagnslausar [2].

Orðalyklar og matskvarði

Einkunnaviðmið kennara: Gefðu 1 stig fyrir hverja rétta pörun (alls 8 stig) og hvert samhengishugtak (alls 6 stig).

ÁFANGI 4: LAUSNIR – PÖRUN HUGTAKA

F 1. FYLLING	H 2. BCRYPT	D 3. GAGNALEKI	G 4. SALTUN
C 5. STJÓRNANDI	B 6. MFA	A 7. REGNBOGI	E 8. VEFVEIÐAR

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 FYLLINGARÁRÁS	2 BCRYPT	3 GAGNABROT	4 SALTUN
5 LYKILORÐASAFN	6 STAÐFESTING		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 H – VEFVEIÐAR	2 C – GAGNABROT	3 B – BCRYPT	4 G – REGNBOGATAFLA
5 A – FYLLINGARÁRÁS	6 D – SALTUN	7 E – LYKILORÐASAFN	8 F – STAÐFESTING

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt FYLLING, BCRYPT og GAGNALEKI með eigin orðum og gefið dæmi um hvert hugtak.

Dæmisögur:
Biddu nemendur að styðja tillögur sínar með staðreyndum úr verkefnablaðinu en ekki ágiskunum.

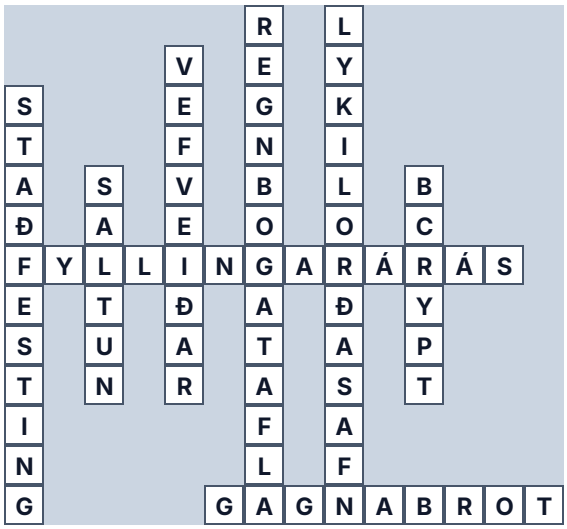
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

N	K	U	T	Y	S	Ö	E	H	É	T	D	A	L	P
F	G	N	I	T	S	E	F	Ð	A	T	S	B	B	Ö
A	M	J	X	S	A	L	T	U	N	S	V	C	A	T
S	Ý	J	M	M	G	H	N	H	S	F	R	K	U	L
A	S	Ý	H	B	V	É	Þ	O	Æ	Y	Ý	T	H	Ú
Ð	Ý	A	P	V	N	O	Æ	Ó	P	I	P	U	H	Ó
R	X	Ú	Ó	V	Ú	J	A	T	E	Ó	M	K	Á	O
O	X	F	G	P	R	A	Ð	I	E	V	F	E	V	R
L	Ý	Æ	Í	J	V	Í	Æ	Y	Þ	Ó	J	I	Ö	I
I	Í	N	T	O	R	B	A	N	G	A	G	A	E	I
K	F	Y	L	L	I	N	G	A	R	Á	R	Á	S	Á
Y	U	A	Í	É	Y	E	J	Ö	J	E	K	R	N	Í
L	A	R	E	G	N	B	O	G	A	T	A	F	L	A
F	Ó	J	O	D	N	B	Ð	G	I	Á	Á	Ó	S	L
P	Y	Ú	I	Æ	F	Æ	T	G	Þ	Y	H	É	S	Ú

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

7 lárétt: FYLLINGARÁRÁS Að prófa lekin skilríki (13 stafir)

8 lárétt: GAGNABROT Óheimil birting gagnagrunns (9 stafir)

LÓÐRÉTT

1 lóðrétt: REGNBOGATAFLA Fyrirframreiknuð tafla yfir hash lykilorða (13 stafir)

2 lóðrétt: LYKILORÐASAFN Tól til að geyma skilríki (13 stafir)

3 lóðrétt: VEFVEIÐAR Félagsleg verkfræði til að stela innskráningum (9 stafir)

4 lóðrétt: STAÐFESTING Fjölþátta athugun við innskráningu (11 stafir)

5 lóðrétt: SALTUN Slembigildi bætt við hash lykilorðs (6 stafir)

6 lóðrétt: BCRYPT Hægvirkt reiknirit til að hasha lykilorð (6 stafir)

Lausnir: Stafaruglingur og dulmál

Lausnalykill fyrir virkni um að raða orðaforða og Secret Cipher Challenge.

LYKILL ORÐARAÐAR

1. GLRÁNYAÁFRSIL — **FYLLINGARÁRÁS**
2. TGONABRAG — **GAGNABROT**
3. YLÐSAFNKRLOAI — **LYKILORÐASAFN**
4. OLTGABAGFAREN — **REGNBOGATAFLA**
5. YRTBPC — **BCRYPT**
6. UTSLNA — **SALTUN**
7. TFSTSGINAEÐ — **STAÐFESTING**
8. REAVVEIÐF — **VEFVEIÐAR**

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"VERNDAÐU LEKIN LYKILORÐ MEÐ FJÖLÞÁTTA ÖRYGGI"

Lausnir dæmisagna

A Dæmisaga 1: Lagfæring á leka innskráningarupplýsinga í fyrirtæki

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Vöktunarþjónusta á myrkravefnum lætur stofnun vita að gagnahrúga með lykilorðum kerfisstjóra fyrirtækisins hafi verið birt á netinu.
- Ráðlögð aðferð og lausn: Afturkallaðu allar virkar stjórnendalotur og endurstilltu auðkenni með kynni sem býr til lykilorð með mikilli óreiðu. Framfylgdu MFA sem þolir vefveiðar á stjórnendagáttum [6], skiptu um viðkomandi API-lykla, farðu yfir innskráningarskrár, finndu upphaflegu berskjöldunina og athugaðu aðra aðganga með sérréttindi.

B Dæmisaga 2: Innleiðing staðla fyrir tætigildi lykilorða

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Aðstæður til greiningar: Gagnagrunnur fyrirtækis geymir lykilorð notenda með úreltum MD5-kjötkássum án dulmálssalts, sem gerir þau berskjölduð fyrir hraðri útdrætti.
- Ráðlögð aðferð og lausn: Taktu upp Argon2id (eða bcrypt á eldri kerfum) með einstöku salti fyrir hvern notanda [2]. Vefðu núverandi MD5-tætigildi inn í nýja reikniritið núna, endurtættu beint við næstu innskráningu hvers notanda og krefstu endurstillingar fyrir reikninga sem hafa lengi verið óvirkir.