Ainm: _____ Dáta: _____ Scór: _____

Sceitheadh pasfhocal agus slándáil dintiúr

Credential stuffing, sáruithe sonraí, halgartaim hashála, fíordheimhniú il-fhachtóra, agus slándáil pasfhocal.

SCEITHEADH PASFHOCAL: FORBHREATHNÚ FOGHLAMA

SLÁNAITHE

CRIPTIÚ SONRAÍ

Caighdeán AES 256-giotán

COMHLÍONTACH

CAIGHDEÁIN DHOMHANDA

Creataí GDPR agus CCPA

IONTAOBHAS NIALASACH

POLASAÍ ROCHTANA

Fíordheimhniú ilfhachtóra

Fáilte! Treoraíonn an paca gníomhaíochtaí seo thú trí sceitheadh pasfhocal agus slándáil dintiúr. Déanfaidh tú iniúchadh ar líonadh dintiúr, sáruithe sonraí, algartaim hashála, fíordheimhniú il-fhachtóra, agus bainisteoirí pasfhocal.

SEICPHOINTÍ NA BILEOGE OIBRE

- [ ] **Cuid 1-4: Máistrigh cibearshlándáil agus cosc bagairtí.**
- [ ] **Cuid 5-7: Réitigh tras-fhocail agus puzail cuardaigh focal.**
- [ ] **Cuid 8-9: Réitigh cás-staidéir agus dúshlán cód.**
- [ ] **Cuid 10: Déan athbhreithniú ar leathanaigh Ceisteanna Coitianta bunúsacha agus ardleibhéil.**
- [ ] **Cuid 11: Féach ar 10 bhfíric spéisiúla ón domhan fíor.**
- [ ] **Breis: dúshlán Smaoinigh go tapa.**

Oscail Treoir VPN.com ar Chibearshlándáil

URL: https://www.vpn.com/ga/slandail-dhigiteach/sceithleadh-pasfhocal/

Do threoirmhapa foghlama: slándáil pasfhocal

- Tuig na rioscaí a bhaineann le nochtadh dintiúr ar fhóraim ghréasáin dhorcha.
- Fíordheimhniú ilfhachtóra (MFA) agus monatóireacht ar dhintiúir chomhréitithe a chur i bhfeidhm.
- Dear cosaintí slándála corparáideacha i gcoinne calaoisí innealtóireachta sóisialta spriocdhírithe.

TREOIR AR SCEITHEADH PASFHOCAL: TREOIRACHA

Freagair na ceisteanna ilrogha agus fíor/bréagach, comhlánaigh na habairtí le bearnaí leis an mbanc focal, meaitseáil sainmhínithe, agus réitigh an crosfhocal agus an cuardach focal. Cuir do chuid eolais i bhfeidhm ar chosaint dintiúir. Críochnaigh leis an ngníomhaíocht bhreise Smaoinigh go tapa.

SCEITHEADH PASFHOCAL AGUS SLÁNDÁIL DINTIÚR (RÉAMHRÁ)

Nochtann sceitheadh pasfhocal dintiúir úsáideoirí ar shuíomhanna poiblí agus ar an ngréasán dorcha. Laghdaíonn pasfhocail uathúla ó bhainisteoir pasfhocal, scagadh pasfhocal sáraithe agus fíordheimhniú ilfhachtóra (MFA) an baol atá ann do stuáil dintiúr, agus cuireann hashadh pasfhocal salannach, mall teorainn leis an damáiste má ghoidtear bunachar sonraí pasfhocal.

LÉIGH GACH SEICPHOINTE GO CÚRAMACH AGUS ROGHNAIGH NÓ SCRÍOBH AN FREAGRA CEART.

Seicphointe 1: Dúshlán ilrogha

1. **1. Cad is líonadh dintiúr ann?**
   - A. Uathoibriú a úsáid chun teaglaim sceite ainm úsáideora/pasfhocal a thástáil thar iliomad suíomh
   - B. Comhaid stórála bunachair sonraí áitiúla a chriptiú
   - C. Freastalaithe gréasáin a ró-ualú le hiarratais tráchta líonra
   - D. Ionchuir mhéarchláir a mhonatóiriú faoi rún

2. **2. Cén algartam a liostaíonn OWASP mar chéad rogha le haghaidh pasfhocail a stóráil inniu?**
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. **3. Conas a mhaolaíonn fíordheimhniú ilfhachtóra (MFA) an riosca go sceithfeadh pasfhocail?**
   - A. Éilíonn sé fachtóir fíorúcháin breise, mar sin ní leor pasfhocal goidte amháin
   - B. Athraíonn sé an pasfhocal go huathoibríoch gach uair an chloig
   - C. Criptíonn sé an t-ainm úsáideora le linn tarchuir
   - D. Tugann sé rabhadh don oifig chreidmheasa faoi iarratais chalaoiseacha

4. **4. Cad is dumpa sáraithe sonraí ann?**
   - A. Bailiúchán dintiúr úsáideoirí sceite a foilsíodh ar líne nó a díoladh ar fóraim hackeálaithe
   - B. Cóip chúltaca de chomhaid bunachair sonraí stóráilte lasmuigh den suíomh
   - C. Taisce shealadach de logaí freastalaí gréasáin
   - D. Uirlis riaracháin a úsáidtear chun pasfhocail úsáideoirí a athshocrú

5. **5. Cad é ról bainisteora pasfhocal?**
   - A. Pasfhocail uathúla láidre a ghiniúint agus a stóráil do gach cuntas
   - B. Trácht líonra a mhonatóiriú le haghaidh sceitheadh pasfhocal
   - C. Ionsaithe fórsa bruidiúil uathoibrithe a bhlocáil ag an ngeata
   - D. Bloic stórála bunachair sonraí a scanadh le haghaidh pasfhocal gan chriptiú

Seicphointe 2: Dúshlán Fíor nó Bréagach

6 Ceist 6

6. Méadaíonn athúsáid pasfhocal ar fud cuntas iolracha an baol líonadh dintiúr.

○ Fíor ○ Bréagach

7 Ceist 7

7. Is feidhm hashála mholta é SHA-1 do stóráil nua-aimseartha pasfhocal.

○ Fíor ○ Bréagach

8 Ceist 8

8. Stopann castacht pasfhocail a chur i bhfeidhm léi féin (gan MFA) líonadh dintiúir go hiomlán.

○ Fíor ○ Bréagach

9 Ceist 9

9. Scanann uirlisí monatóireachta an ghréasáin dhorcha an t-idirlíon do dhintiúir chorparáideacha atá i gcontúirt.

○ Fíor ○ Bréagach

10 Ceist 10

10. Cuireann hais-chodanna salannaithe sonraí randamacha uathúla le pasfhocail sula ndéantar hasháil orthu chun ionsaithe tábla bogha báistí a chloí.

○ Fíor ○ Bréagach

Seicphointe 3: Príomhthéarmaí a chur isteach

Léigh gach abairt thíos agus líon isteach an bhearna leis an téarma ceart ón mBanc Focal.

1. Is é an t-ainm ar dhintiúir sceite a thástáil thar go leor feidhmchlár gréasáin ná: _____ .

2. Is é _____ algartam mall hashála pasfhocal atá in-oiriúnaithe agus a nglacann OWASP leis fós.

3. Is é nochtadh comhad príobháideach bunachair sonraí ar an idirlíon ná _____ sonraí.

4. Tugtar _____ ar luachanna randamacha a chur le pasfhocail sula ndéantar hashadh orthu.

5. Is é bunachar sonraí áitiúil slán le haghaidh dintiúr úsáideora ná _____ pasfhocal.

6. Baineann céim fíorúcháin logála isteach eile a chur leis úsáid as fíordheimhniú _____ .

BANC FOCAL FOCLÓIRE

BAINISTEOIR BCRYPT CRAMADH DINTIÚR FIOSCAIREACHT ILFHACHTÓRA SALANNÚ SÁRÚ TUAR CEATHA

Scríobh do fhreagraí anseo:

1. **2.**

3. **4.**

5. **6.**

Seicphointe 4: Meaitseáil coincheapa slándála

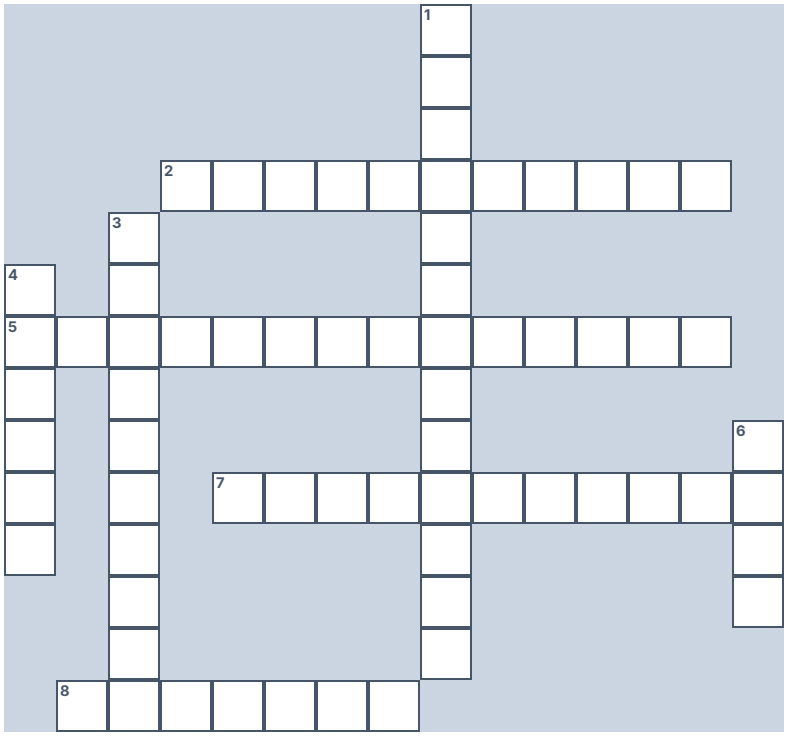
MEAITSEÁIL SAINMHÍNITHE

Meaitseáil gach téarma foclóra ar chlé lena shainmhíniú ceart ar dheis trí scríobh na litreach comhfhreagraí (A-H) sa bhosca ionchuir inlíonta.

☐	1. LÍONADH	A	Tábla réamhríofa de hashanna pasfhocal.
☐	2. BCRYPT	B	Seiceáil logála isteach ilfhachtóra.
☐	3. SÁRÚ	C	Uirlis stórála dintiúr.
☐	4. SALTÚ	D	Nochtadh neamhúdaraithe bunachair sonraí.
☐	5. BAINISTEOIR	E	Innealtóireacht shóisialta chun logálacha isteach a ghoid.
☐	6. MFA	F	Dintiúir sceite a thástáil.
☐	7. TUAR CEATHA	G	Salann randamach a chur le hash an phasfhocail.
☐	8. FIOSCAIREACHT	H	Algartam mall hashála pasfhocal.

Seicphointe 5: Crosfhocal

Réitigh an crosfhocal trí litreacha a chlóscríobh sna boscaí bána gníomhacha. Freagraíonn na huimhreacha do na leideanna thíos.



TRASNA

2. Uirlis stórála dintiúr (11)

5. Dintiúir a sceitheadh a thástáil (14)

7. Seiceáil logála isteach ilfhachtóra (11)

8. Salann randamach a chur le hash pasfhocail (7)

SÍOS

1. Innealtóireacht shóisialta chun logálacha isteach a ghoid (13)

3. Tábla réamhríofa de hashanna pasfhocal (10)

4. Algartam mall hashála pasfhocal (6)

6. Nochtadh neamhúdaraithe bunachair sonraí (4)

Seicphointe 5, rogha eile: Leideanna crosfhocail inrochtana

Is féidir le húsáideoirí léitheora scáileáin agus méarchláir freagraí na crosfhocal a chlóscríobh go díreach sna réimsí téacs thíos.

TRASNA

2 trasna: Uirlis stórála dintiúr (11 litir):

5 trasna: Dintiúir a sceitheadh a thástáil (14 litir):

7 trasna: Seiceáil logála isteach ilfhachtóra (11 litir):

8 trasna: Salann randamach a chur le hash pasfhocail (7 litir):

SÍOS

1 síos: Innealtóireacht shóisialta chun logálacha isteach a ghoid (13 litir):

3 síos: Tábla réamhríofa de hashanna pasfhocal (10 litir):

4 síos: Algartam mall hashála pasfhocal (6 litir):

6 síos: Nochtadh neamhúdaraithe bunachair sonraí (4 litir):

Seicphointe 6: Cuardach focal i bhfolach

Aimsigh na 8 dtéarma eochair-fhoclóra atá i bhfolach san eangach thíos. Is féidir focail a bheith cothrománach, ingearach, nó trasnánach.

T T H G B E I K T S V R Z E H

H A R O T H C A H F L I E B S

C S C A L Q C U Z M K V C A R

A U A S W J R M M H H R L N H

E R F K T A L R W H Y A B U F

R Y O Y S W S H T P N X A P U

I N N Z O I Q T T N I P V U O

A U U K A E P M U K A N V G G

C P Q X Y J K V J Y W Y P J I

S Z A H T A E C R A U T I J N

O C R A M A D H D I N T I U R

I A E I A S A J F W E K Z K E

F K B A I N I S T E O I R Q N

J A F O K N D N C D H I B A P

R L P W T I Y F Y S G X W H F

LIOSTA FOCAL FOCLÓIRE

CRAMADHDINTIUR BCRYPT SARU SALANNU BAINISTEOIR ILFHACHTORA TUARCEATHA FIOSCAIREACHT

Seicphointe 6, rogha eile: Meaitseáil foclóra inrochtana

Meaitseáil gach ceann de na 8 dtéarma foclóra ón Cuardach Focal lena sainmhíniú ceart trí scríobh na litreach (A-H) sa spás folamh.

TÉARMAÍ FOCLÓIRE

A. CRAMADHDINTIUR

B. BCRYPT

C. SARU

D. SALANNU

E. BAINISTEOIR

F. ILFHACHTORA

G. TUARCEATHA

H. FIOSCAIREACHT

SAINMHÍNITHE AGUS GLEANNTA MEAITSEÁLA

____ 1. Innealtóireacht shóisialta chun logálacha isteach a ghoid.

____ 2. Nochtadh neamhúdaraithe bunachair sonraí.

____ 3. Algartam mall hashála pasfhocal.

____ 4. Tábla réamhríofa de hashanna pasfhocal.

____ 5. Dintiúir a sceitheadh a thástáil.

____ 6. Salann randamach a chur le hash pasfhocail.

____ 7. Uirlis stórála dintiúr.

____ 8. Seiceáil logála isteach ilfhachtóra.

Seicphointe 7: Dúshlán focal measctha

Dí-mheascaigh na litreacha thíos chun príomhchoincheapa agus téarmaí cibearshlándála a nochtadh. Scríobh do chuid freagraí sna boscaí ionchuir a sholáthraítear.

1. TDDNHARIICURAM
2. SRUA
3. BTSEIAIRION
4. EHCARTATUA
5. YRTBPC
6. NLNSAUA
7. TAILHAORFCH
8. EOCACRTFIIHAS

Gníomhaíocht bhreise: Smaoinigh go tapa

3 FHREAGRA DO GACH CATAGÓIR. BUAILEANN AN CHÉAD DUINE A LÍONANN AN LIOSTA.

1	Nósanna sábháilte is féidir leat a thosú inniu			
2	Rialacha le haghaidh pasfhocal láidir			
3	Bainisteoirí pasfhocal a bhfuil aithne agat orthu			
4	Uirlisí slándála a bhfuil aithne agat orthu			
5	Comharthaí rabhaidh i ríomhphost			
6	Focail spraiúla le haghaidh frása faire fada			
7	Bealaí le logáil isteach gan pasfhocal			
8	Faisnéis nár cheart duit a roinnt choíche			
9	Cúiseanna le bogearraí a nuashonrú			
10	Rudaí le déanamh nuair a sceitheann pasfhocal			
11	Cuntais a dteastaíonn MFA uathu			
12	Áiteanna nár cheart pasfhocail a stóráil choíche			
13	Comharthaí go bhfuil ríomhaire ionfhabhtaithe			
14	Drochphasfhocail a úsáideann daoine			
15	Rudaí a dhéanann tú cúltaca díobh			

Seicphointe 8: Cás-staidéir ar chibearshlándáil

Cuir na coincheapa a d'fhoghlaim tú i bhfeidhm chun na cásanna fíorshaoil thíos a réiteach.

CÁS-STAIDÉAR 1: ATHCHÓIRIÚ AR SCEITHEADH DINTIÚR FIONTAIR



Cás: Cuireann seirbhís monatóireachta ghréasán dorcha in iúl d'eagraíocht go bhfuil dump bunachair sonraí ina bhfuil pasfhocail riarthóirí córais chorparáideacha foilsithe ar líne.

Ceist phlé: Déan anailís ar na rioscaí sceite dintiúr, agus mol straitéis athshocraithe riaracháin.

CÁS-STAIDÉAR 2: CAIGHDEÁIN HASHÁLA PASFHOCAIL A IMPLEMENTÁIL



Cás: Stórálann bunachar sonraí fiontair pasfhocail úsáideoirí faoi láthair ag baint úsáide as hashanna MD5 as dáta gan salann cripteagrafach, rud a fhágann go bhfuil siad leochaileach d'eastóscadh tapa.

Ceist phlé: Dear straitéis imirce chun halgartam hashála an bhunachair sonraí a uasghrádú.

Seicphointe 9: Díchódaigh an cód

Cosnaíonn gairmí cibearshlándála sócmhainní líonra ó aisteoirí bagartha ar líne. Úsáid an eochair Litir-go-Uimhir thíos chun an teachtaireacht a dhíchódú trí na litreacha comhfhreagracha a scríobh sna spásanna folmha.

EOCHAIR CHRIPTITHE LITIR-GO-UIMHIR

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

3	15	19	1	9	14		16	1	19	6	8	15	3	1	9	12

19	3	5	9	20	5		12	5		9	12	6	8	1	3	8	20	15	18	1

Teachtaireacht díchódaithe:

COMHAIRLE: FREAGRAÍONN GACH UIMHIR DO SHUÍOMH NA LITRE SIN SAN AIBÍTIR (M.SH. 1 = A, 2 = B, 26 = Z).

Seicphointe 10: Ceisteanna coitianta faoi chibearshlándáil – bunleibhéal (Cuid A)

Athbhreithnigh ceisteanna agus freagraí coitianta maidir le laghdú bagairtí ar líne.

Q1: Cad is sceitheadh pasfhocail ann?

Tarlaíonn sceitheadh pasfhocail nuair a nochtar dintiúir logála isteach úsáideoirí trí sháruithe sonraí nó mícumraíochtaí freastalaí.

Q2: Conas a aimsíonn hackers pasfhocail sceite?

Scanann hackers fóraim dhorchghréasáin, dumpaí poiblí bunachar sonraí agus suíomhanna greamaithe ina bhfoilsítear sonraí sáraithe [8].

Q3: An bhfuil athúsáid pasfhocal contúirteach?

Sea, mar má dhéantar suíomh amháin a chomhbhrú, is féidir le hackálaithe na dintiúir chéanna a thástáil ar na mílte ardán eile [3].

Q4: Cad é salann cripteagrafach?

Is éard is salann ann ná sonraí randamacha a chuirtear le pasfhocal sula ndéantar hasháil air, rud a fhágann go bhfuil ionsaithe cuardaigh réamhríofa neamhéifeachtach [2].

Q5: Cén fáth a bhfuil MD5 as feidhm?

Is haise ghinearálta thapa, atá as dáta é MD5, mar sin is féidir le hionsaitheoirí tomhaiseanna pasfhocail a thástáil go han-tapa, go háirithe nuair nach bhfuil na haiseanna saillte [2].

Seicphointe 10: Ceisteanna coitianta faoi chibearshlándáil – bunleibhéal (Cuid B)

Athbhreithnigh ceisteanna agus freagraí coitianta maidir le laghdú bagairtí ar líne.

Q6: Conas a chosnaíonn bainisteoir pasfhocal úsáideoirí?

Gineann sé dintiúir chasta uathúla do gach suíomh go huathoibríoch, ag laghdú earráidí cuimhne daonna agus athúsáide.

Q7: Cad é ionsaí fórsa bruite?

Ionsaí a thástálann gach teaglaim carachtar féideartha go córasach go dtí go bhfaightear an pasfhocal ceart [4].

Q8: Conas a chabhraíonn glasáil chuntais?

Moillíonn glasáil amach nó teorannú ráta iarrachtaí buailte ar líne arís agus arís eile agus, in éineacht le monatóireacht agus MFA, laghdaíonn sé baol fórsa bruidiúil [4].

Q9: An bhfuil máistirphasfhocail slán?

Tá siad slán má tá siad ina bhfrásaí pasfhocail ard-eantrópachta nach n-athúsáidtear riamh ar chórais ghréasáin eile.

Q10: Ar cheart pasfhocail a athrú go rialta?

Deir NIST gan athruithe tréimhsiúla a chur d'iallach; athraigh iad ar fhianaise comhréitigh agus tabhair tosaíocht d'fhad, do liostaí blocála agus do MFA [1].

Seicphointe 10: Ceisteanna coitianta faoi shlándáil – ardleibhéal (Cuid C)

Déan iniúchadh ar ghnéithe teicniúla ardleibhéil de chreataí slándála, anailís bogearraí mailíseacha, agus comhlíonadh sonraí.

Q1: Conas a chuirtear Argon2 i gcomparáid le bcrypt?

Liostaíonn OWASP Argon2id mar a chéad rogha; seasann a shocruithe cuimhne-dhian in aghaidh scoilteadh GPU agus ASIC níos fearr ná bcrypt [2].

Q2: Cad is síneadh eochrach ann?

Teicníc a lúbann algartam hashála na mílte uair chun moill a chur ar phróiseas fíorú pasfhocail, rud a fhágann go bhfuil briseadh costasach [2].

Q3: Conas a oibríonn táblaí tuar ceatha?

Is táblaí cuardaigh réamhríofa iad a nascann pasfhocail téacs simplí lena hashanna, a úsáidtear chun hashanna gan salann a aisiompú go tapa [2].

Q4: Cad é athchúrsáil dintiúr?

Péirí ainm úsáideora/pasfhocail goidte ó shárú amháin a athúsáid chun iarracht a dhéanamh rochtain a fháil ar sheirbhísí eile, go háirithe nuair a d'athúsáid daoine pasfhocail [3].

Q5: An féidir bainisteoirí pasfhocal a hackáil?

Tá. Úsáideann go leor criptiú nialais-eolais, mar sin ní nochtann sárú freastalaí ach cuaillí criptithe, ach is féidir príomhphasfhocail laga a bhriseadh as líne fós.

Seicphointe 10: Ceisteanna coitianta faoi shlándáil – ardleibhéal (Cuid D)

Déan iniúchadh ar ghnéithe teicniúla ardleibhéil de chreataí slándála, anailís bogearraí mailíseacha, agus comhlíonadh sonraí.

Q6: Cad é ionsaí foclóra?

Leagan d'fhórsa brúidiúil a thástálann focail choitianta, frásaí agus pasfhocail a sceitheadh roimhe seo seachas litreacha randamacha.

Q7: Cén fáth a bhfuil pasfhrásaí i bhfabhar?

Úsáideann frásaí pasfhocail go leor focal randamacha, rud a chruthaíonn eantrópacht ard atá furasta do dhaoine cuimhneamh air ach costasach ó thaobh ríomhaireachta de a bhriseadh [1].

Q8: Conas a théann síniú aonair (SSO) i bhfeidhm ar sceitheadh pasfhocal?

Laghdaíonn SSO scaipeadh pasfhocal, ach éiríonn an soláthraí aitheantais ina sprioc ard-luacha a theastaíonn MFA láidir uaidh, atá frithsheasmhach in aghaidh fioscaireachta de réir mar is fearr [6].

Q9: Cad é fuadach seisiúin?

Faigheann ionsaitheoir comhartha seisiúin bailí nó déanann sé mí-úsáid air chun aithris a dhéanamh ar úsáideoir logáilte isteach gan an pasfhocal a bheith de dhíth arís [5].

Q10: Conas a bhraitheann tú spraeáil pasfhocal?

Trí cuardach a dhéanamh ar na pasfhocail bheagacha chéanna a triaileadh thar go leor cuntas, go minic go mall chun fanacht faoi bhun tairseacha glasála [7].

Cuid 11: 10 bhFíric agus Léargas Cibearshlándála ón Domhan Fíor

Athbhreithnigh fíricí fíordhomhanda maidir le sáruithe slándála, sásraí cosanta, agus caighdeáin chomhlíonta.

1. EOLAS SLÁNDÁLA

Éilíonn NIST SP 800-63B go seiceálfar pasfhocail nua i gcoinne liostaí blocála de phasfhocail choitianta agus chomhréitigh [1].

2. EOLAS SLÁNDÁLA

Chomhcheangail dumpa 'Collection #1' 2019 sonraí ó go leor sáruithe níos luaithe in aon chomhad ollmhór amháin de phéirí ríomhphoist agus pasfhocal [8].

3. EOLAS SLÁNDÁLA

Éilíonn NIST anois go mbeadh pasfhocail a úsáidtear mar an t-aon fhachtóir fíordheimhnithe 15 charachtar ar a laghad [1].

4. EOLAS SLÁNDÁLA

Is féidir le crua-earraí ASIC billiúin hash SHA-256 a ríomh in aghaidh an tsoicind, rud a fhágann nach bhfuil hashháil amh SHA sábháilte do phasfhocail úsáideoirí [2].

5. EOLAS SLÁNDÁLA

Ciallaíonn salainn uathúla go bhfaigheann beirt úsáideoirí a bhfuil an pasfhocal céanna acu hashanna bunachair sonraí éagsúla [2].

6. EOLAS SLÁNDÁLA

Criptíonn go leor bainisteoirí pasfhocal sonraí taisceadáin go háitiúil le cripteagrafaíocht láidir díorthaithe ó phríomhphasfhocal an úsáideora.

7. EOLAS SLÁNDÁLA

Oibríonn credential stuffing toisc go n-athúsáideann a lán daoine an pasfhocal céanna ar chuntais e-tráchtála, baincéireachta agus ríomhphoist [3].

8. EOLAS SLÁNDÁLA

Deir NIST SP 800-63B nár cheart d'fhíoraitheoirí athruithe tréimhsiúla pasfhocail a éileamh, ach athruithe tar éis fianaise ar chomhréiteach amháin [1].

9. EOLAS SLÁNDÁLA

Ní stopann litir mhór agus siombail amháin a chur le pasfhocal gearr ionsaithe foclóra GPU uathoibrithe nua-aimseartha [1].

10. EOLAS SLÁNDÁLA

Is féidir le MFA go leor iarrachtaí líonta dintiúr a bhlocáil fiú tar éis pasfhocal a sceitheadh; tá MFA atá frithsheasmhach in aghaidh fioscaireachta níos láidre ná cóid SMS [3].

Tagairtí teicniúla agus foinsí

Tá an treoirleabhar staidéir agus na mearaithe idirghníomhacha curtha le chéile ó chaighdeáin dhomhanda NIST, OWASP agus chomhlíonta príobháideachta sonraí.

TAGAIRTÍ ACADÚLA AGUS TIONSCAIL

[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/

Freagraí: Seicphointe 1 – Ilrogha

1 **Ceist 1** **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Úsáideann líonadh dintiúr uathoibriú chun péirí ainm úsáideora/pasfhocal sceite a thriail ar shuíomhanna eile [3].

2 **Ceist 2** **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Molann OWASP Argon2id ar dtús; úsáidtear bcrypt go príomha le haghaidh córais oidhreachta nuair nach bhfuil Argon2id ná scrypt ar fáil [2].

3 **Ceist 3** **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Éilíonn MFA fachtóir breise, mar sin ní féidir le pasfhocal goidte amháin an cuntas a dhíghlasáil [3].

4 **Ceist 4** **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Is bailiúcháin dintiúr sceite iad dumpaí sáraithe, mar thiomsú Collection #1 2019 [8].

5 **Ceist 5** **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Gintear agus stórálann bainisteoir pasfhocal pasfhocal láidir uathúil do gach cuntas, ag cosc athúsáide [3].

Freagraí: Seicphointe 2 – Fíor nó Bréagach

6 **Ceist 6** **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Fíor: ligeann pasfhocail athúsáidte d'ionsaitheoirí dintiúir a sceitheadh ó shuíomh amháin a athsheinm ar shuíomhanna eile [3].

7 **Ceist 7** **Freagra ceart: Bréagach**

NÓTA DON MHÚINTEOIR

Bréagach: is hais thapa é SHA-1; molann OWASP Argon2id, scrypt, bcrypt nó PBKDF2 ina ionad [2].

8 **Ceist 8** **Freagra ceart: Bréagach**

NÓTA DON MHÚINTEOIR

Bréagach: ní féidir le rialacha castachta amháin líonadh le pasfhocail sceite athúsáidte a stopadh; teastaíonn MFA [3].

9 **Ceist 9** **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Fíor: cuardaíonn seirbhísí monatóireachta dumpaí sáraithe agus foinsí gréasáin dhorcha le haghaidh dintiúir nochta [8].

10 **Ceist 10** **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Fíor: déanann salann uathúil in aghaidh an phasfhocail boird réamhríofa bogha báistí neamhéifeachtach [2].

Eochracha foclóra agus rúibric mharcála

Rúbraic ghrádaithe don mhúinteoir: Bronn 1 phointe do gach meaitseáil cheart (8 pointe san iomlán) agus téarma comhthéacs (6 pointe san iomlán).

SEICPHOINTE 4: FREAGRAÍ – MEAITSEÁIL COINCHEAPA

F 1. LÍONADH	H 2. BCRYPT	D 3. SÁRÚ	G 4. SALTÚ
C 5. BAINISTEOIR	B 6. MFA	A 7. TUAR CEATHA	E 8. FIOSCAIREACHT

SEICPHOINTE 3: FREAGRAÍ – PRÍOMHTHÉARMAÍ

1 CRAMADH DINTIÚR	2 BCRYPT	3 SÁRÚ	4 SALANNÚ
5 BAINISTEOIR	6 ILFHACHTÓRA		

SEICPHOINTE 6, ROGHA EILE: FREAGRAÍ – MEAITSEÁIL FOCAL

1 H – FIOSCAIREACHT	2 C – SARU	3 B – BCRYPT	4 G – TUARCEATHA
5 A – CRAMADHDINTIUR	6 D – SALANNU	7 E – BAINISTEOIR	8 F – ILFHACHTORA

NÓTAÍ PLÉ DO MHÚINTEOIRÍ

Príomhthéarmaí:
Seiceáil an féidir leis na daltaí LÍONADH, BCRYPT agus SÁRÚ a mhíniú ina bhfocail féin agus sampla a thabhairt de gach ceann.

Cás-staidéir:
Iarr ar na daltaí a moltaí a bhunú ar fhíricí ón mbileog oibre, ní ar thuairimí.

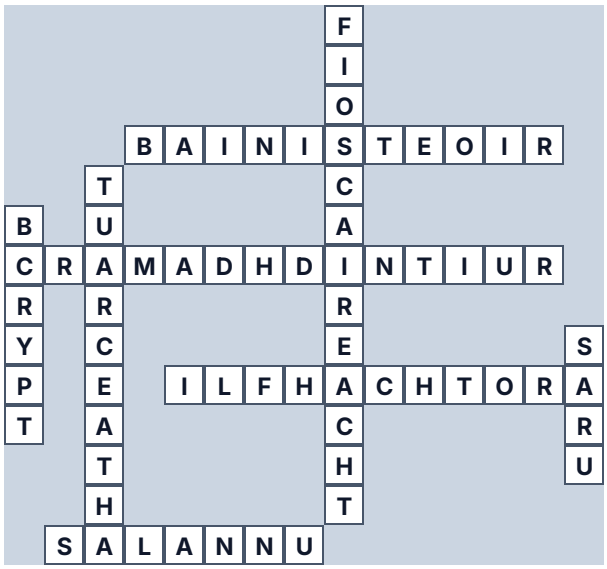
Measúnú foinsí:
Iarr ar na daltaí ráiteas amháin ar a laghad a fhíorú i bhfoinsí na bileoige agus pléigí cén fáth a bhféadfadh figiúirí, praghsanna agus rialacha athrú le himeacht ama.

Eochracha Puzal agus Nótaí don Mhúinteoir

CUR CHUN CINN FOCLÓIR CUARDAIGH

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

TUAIRISC CROSSWORD



TREOIR DON MHÚINTEOIR AR FHREAGRAÍ CROSFHOCAIL

TRASNA

2 trasna: BAINISTEOIR Uirlis stórála dintiúr (11 litir)

5 trasna: CRAMADHDINTIUR Dintiúir a sceitheadh a thástáil (14 litir)

7 trasna: ILFHACHTORA Seiceáil logála isteach ilfhachtóra (11 litir)

8 trasna: SALANNU Salann randamach a chur le hash pasfhocail (7 litir)

SÍOS

1 síos: FIOSCAIREACHT Innealtóireacht shóisialta chun logálacha isteach a ghoid (13 litir)

3 síos: TUARCEATHA Tábla réamhríofa de hashanna pasfhocal (10 litir)

4 síos: BCRYPT Algartam mall hashála pasfhocal (6 litir)

6 síos: SARU Nochtadh neamhúdaraithe bunachair sonraí (4 litir)

Eochair na bhfocal measctha agus réiteach an chóid

Eochair ghrádaithe don ghníomhaíocht dhíchuachta foclóra agus don Dúshlán Cód Rúnda.

EOCHAIR NA bhFOCAL DÍSCRAMBLAITHE

1. TDDNHARIICURAM — CRAMADHDINTIUR
2. SRUA — SARU
3. BTSEIAIRION — BAINISTEOIR
4. EHCARTATUA — TUARCEATHA
5. YRTBPC — BCRYPT
6. NLNSAUA — SALANNU
7. TAILHAORFCH — ILFHACHTORA
8. EOCACRTFIIHAS — FIOSCAIREACHT

EOCHAIR DHÚSHLÁN AN CHÓID RÚNDA

"COSAIN PASFHOCAIL SCEITE LE ILFHACHTORA"

Freagraí na gcás-staidéar

A Cás-staidéar 1: Athchóiriú ar sceitheadh dintiúr fiontair

Réiteach don mhúinteoir

TREOIRLÍNE GRÁDÚ

Ba cheart do fhreagraí na mac léinn na pointí seo a leanas a chlúdach:

- Anailís cháis: Tugann seirbhís monatóireachta ar an ngréasán dorcha rabhadh d'eagraíocht go bhfuil dump bunachair sonraí ina bhfuil pasfhocail riarthóirí córais chorparáideacha foilsithe ar líne.
- Straitéis agus réiteach molta: Cúlghairm gach seisiún riarthóra gníomhach agus athshocraigh na dintiúir le gineadóir ard-eantrópachta. Cuir MFA atá frithsheasmhach in aghaidh fioscaireachta i bhfeidhm ar thairseacha riarthóra [6], rothlaigh eochracha API atá buailte, athbhreithnigh logaí logála isteach, aimsigh an nochtadh tosaigh agus seiceáil cuntais phribhléideacha eile.

B Cás-staidéar 2: Caighdeáin hashála pasfhocail a implementáil

Réiteach don mhúinteoir

TREOIRLÍNE GRÁDÚ

Ba cheart do fhreagraí na mac léinn na pointí seo a leanas a chlúdach:

- Anailís cháis: Stórálann bunachar sonraí fiontair pasfhocail úsáideoirí faoi láthair le hais MD5 atá as dáta gan salann cripteagrafach, rud a fhágann go bhfuil siad leochaileach do bhaint amach go tapa.
- Straitéis mholta agus réiteach: Glac Argon2id (nó bcrypt ar chórais oidhreachta) le salann uathúil in aghaidh an úsáideora [2]. Cuir na hashanna MD5 atá ann cheana faoi chlúdach an algartaim nua anois, athhasháil go díreach ag logáil isteach eile gach úsáideora, agus cuir athshocrú iallach ar chuntais atá neamhghníomhach le fada.