Enw: _____ Dyddiad: _____ Sgôr: _____

Gollyngiadau Cyfrineiriau a Diogelwch Manylion Mewngofnodi

Stwffio manylion mewngofnodi, tor-data, algorithmau stwnsio, dilysu aml-ffactor, a diogelwch cyfrineiriau.

TROSOLWG DYSGU GOLLYNGIADAU CYFRINEIRIAU

WEDI'I DDIOGELU
AMGRYPTIO DATA
Safon AES 256-did

YN CYDYMFFURFIO
SAFONAU BYD-EANG
Fframweithiau GDPR a CCPA

DIM YMDDIRIEDAETH
POLISI MYNEDIAD
Dilysu Aml-ffactor

Croeso! Mae'r pecyn gweithgareddau hwn yn eich tywys drwy ollyngiadau cyfrineiriau a diogelwch manylion mewngofnodi. Byddwch yn archwilio stwffio manylion mewngofnodi, tor-data, algorithmau stwnsio, dilysu aml-ffactor a rheolwyr cyfrineiriau.

PWYNTIAU GWIRIO'R DAFLEN WAITH

- [ ] **Rhan 1-4: Meistroli seiberddiogelwch ac atal bygythiadau.**
- [ ] **Rhan 5-7: Datrys posau croesair a chwilair.**
- [ ] **Rhan 8-9: Datrys astudiaethau achos a her y seiffr.**
- [ ] **Rhan 10: Adolygu tudalennau Cwestiynau Cyffredin sylfaenol ac uwch.**
- [ ] **Rhan 11: Archwilio 10 ffaith ddiddorol o'r byd go iawn.**
- [ ] **Bonws: her Meddwl yn Gyflym.**

Agorwch Ganllaw Seiberddiogelwch VPN.com

URL: https://www.vpn.com/cy/diogelwch-seiber/cyfrineiriau-wedi-gollwng/

Eich Map Llwybr Dysgu Diogelwch Cyfrineiriau

- Deall risgiau datgelu manylion mewngofnodi ar fforymau'r we dywyll.
- Gweithredwch ddilysu aml-ffactor (MFA) a monitro manylion mewngofnodi sydd wedi'u peryglu.
- Lluniwch amddiffynfeydd diogelwch corfforaethol yn erbyn sgamiau peirianneg gymdeithasol wedi'u targedu.

CYFARWYDDIADAU'R CANLLAW GOLLYNGIADAU CYFRINEIRIAU

Atebwch y cwestiynau amlddewis a gwir/gau, cwblhewch y brawddegau llenwi bylchau gan ddefnyddio'r banc geiriau, parwch y diffiniadau, a datryswch y posau croesair a chwilair. Cymhwyswch eich gwybodaeth i ddiogelu manylion mewngofnodi. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

GOLLYNGIADAU CYFRINEIRIAU A DIOGELWCH MANYLION MEWNGOFNODI (CYFLWYNIAD)

Mae gollyngiadau cyfrineiriau yn datgelu manylion mewngofnodi defnyddwyr ar wefannau cyhoeddus ac ar y we dywyll. Mae cyfrineiriau unigryw o reolwr cyfrineiriau, sgrinio rhag cyfrineiriau a ddatgelwyd a dilysu aml-ffactor (MFA) yn lleihau'r risg o credential stuffing, tra bo hashio cyfrineiriau araf â halen yn cyfyngu ar y difrod os caiff cronfa ddata cyfrineiriau ei dwyn.

DARLLENWCH BOB PWYNT GWIRIO YN OFALUS A DEWISWCH NEU YSGRIFENNWCH YR YMATEB CYWIR.

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw stwffio manylion mewngofnodi?**
   - A. Defnyddio awtomeiddio i brofi cyfuniadau enw defnyddiwr/cyfrinair a ddatgelwyd ar draws sawl gwefan
   - B. Amgryptio ffeiliau storio cronfa ddata lleol
   - C. Llethu gweinyddion gwe â cheisiadau traffig rhwydwaith
   - D. Monitro mewnbynnau bysellfwrdd yn gyfrinachol

2. **2. Pa algorithm y mae OWASP yn ei restru fel ei ddewis cyntaf ar gyfer storio cyfrineiriau heddiw?**
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. **3. Sut mae dilysu aml-ffactor (MFA) yn lliniaru'r risg o gyfrineiriau'n gollwng?**
   - A. Mae'n gofyn am ffactor dilysu ychwanegol, felly nid yw cyfrinair wedi'i ddwyn ar ei ben ei hun yn ddigon
   - B. Mae'n newid y cyfrinair bob awr yn awtomatig
   - C. Mae'n amgryptio'r enw defnyddiwr wrth ei drosglwyddo
   - D. Mae'n rhybuddio'r ganolfan gredyd am geisiadau twyllodrus

4. **4. Beth yw tomen data o dor-data?**
   - A. Casgliad o fanylion mewngofnodi defnyddwyr a ddatgelwyd ac a gyhoeddwyd ar-lein neu a werthwyd ar fforymau hacwyr
   - B. Copi wrth gefn o ffeiliau cronfa ddata wedi'i storio oddi ar y safle
   - C. Celc dros dro o logiau gweinydd gwe
   - D. Offeryn gweinyddol a ddefnyddir i ailosod cyfrineiriau defnyddwyr

5. **5. Beth yw rôl rheolwr cyfrineiriau?**
   - A. Cynhyrchu a storio cyfrineiriau unigryw, cryf ar gyfer pob cyfrif
   - B. Monitro traffig rhwydwaith am gyfrineiriau sydd wedi gollwng
   - C. Rhwystro ymosodiadau grym brwnt awtomataidd wrth y porth
   - D. Sganio blociau storio cronfa ddata am gyfrineiriau heb eu hamgryptio

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae ailddefnyddio cyfrineiriau ar draws sawl cyfrif yn cynyddu'r risg o stwffio manylion mewngofnodi.

○ Gwir ○ Gau

7 Cwestiwn 7

7. Mae SHA-1 yn swyddogaeth stwnsio a argymhellir ar gyfer storio cyfrineiriau modern.

○ Gwir ○ Gau

8 Cwestiwn 8

8. Mae gorfodi cymhlethdod cyfrineiriau ar ei ben ei hun (heb MFA) yn atal stwffio manylion mewngofnodi yn llwyr.

○ Gwir ○ Gau

9 Cwestiwn 9

9. Mae offer monitro'r we dywyll yn sganio'r rhyngrwyd am fanylion mewngofnodi corfforaethol sydd wedi'u peryglu.

○ Gwir ○ Gau

10 Cwestiwn 10

10. Mae stwnsh gyda halen yn ychwanegu data ar hap unigryw at gyfrineiriau cyn stwnsio i drechu ymosodiadau tablau enfys.

○ Gwir ○ Gau

Pwynt Gwirio 3: Mewnosod Termau Allweddol

Darllenwch bob brawddeg isod a llenwch y bwlch gyda'r term cywir o'r Banc Geiriau.

1. Yr enw ar brofi tystlythyrau a ollyngwyd ar draws llawer o raglenni gwe yw _____ tystlythyrau.

2. Algorithm stwnsio cyfrineiriau araf, addasol sy'n dal i gael ei dderbyn gan OWASP yw _____ .

3. Yr enw ar ddatgelu ffeiliau cronfa ddata cyfrinachol ar y rhyngrwyd yw _____ data.

4. Yr enw ar ychwanegu gwerthoedd ar hap at gyfrineiriau cyn eu stwnsio yw _____ .

5. Cronfa ddata leol ddiogel ar gyfer tystlythyrau defnyddwyr yw _____ cyfrineiriau.

6. Mae ychwanegu ail gam dilysu wrth fewngofnodi yn defnyddio dilysu _____ .

BANC GEIRIAU GEIRFA

AML-FFACTOR | BCRYPT | ENFYS | GWE-RWYDO | HALLTU | RHEOLWR | STWFFIO | TORIAD

Ysgrifennwch eich atebion yma:

1. | **2.**

3. | **4.**

5. | **6.**

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

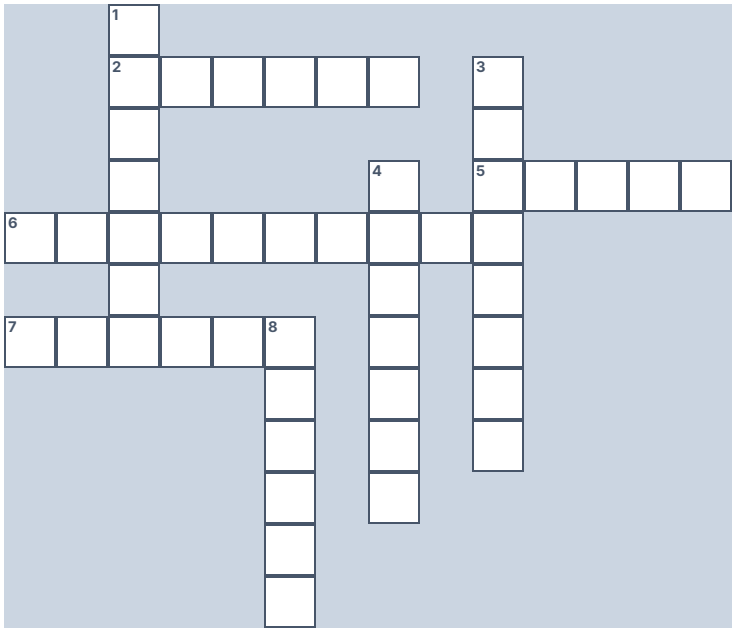
PARU DIFFINIADAU

Parwch bob term geirfa ar y chwith â'i ddiffiniad cywir ar y dde drwy ysgrifennu'r llythyren gyfatebol (A-H) yn y blwch mewnbwn y gellir ei lenwi.

☐	1. STWFFIO	A	Tabl o stwnshis cyfrineiriau wedi'u cyfrifo ymlaen llaw.
☐	2. BCRYPT	B	Gwiriad mewngofnodi aml-ffactor.
☐	3. TORRI DIOGELWCH	C	Offeryn storio manylion mewngofnodi.
☐	4. HALLTU	D	Datgelu cronfa ddata heb awdurdod.
☐	5. RHEOLWR	E	Peirianneg gymdeithasol i ddwyn manylion mewngofnodi.
☐	6. MFA	F	Profi manylion mewngofnodi a ollyngwyd.
☐	7. ENFYS	G	Ychwanegu halen ar hap at stwnsh cyfrinair.
☐	8. GWE-RWYDO	H	Algorithm stwnsio cyfrineiriau araf.

Pwynt Gwirio 5: Pos Croesair

Datryswch y croesair drwy deipio llythrennau yn y blychau gwyn gweithredol. Mae'r rhifau'n cyfateb i'r cliwiau isod.



CLIWIAU AR DRAWS

2. Ychwanegu halen ar hap at stwnsh cyfrinair. (6)

5. Tabl o stwnshau cyfrineiriau wedi'u cyfrifo ymlaen llaw. (5)

6. Gwiriad mewngofnodi â mwy nag un ffactor. (10)

7. Algorithm stwnsio cyfrineiriau araf. (6)

CLIWIAU I LAWR

1. Offeryn storio tystlythyrau. (7)

3. Peirianneg gymdeithasol i ddwyn manylion mewngofnodi. (8)

4. Profi tystlythyrau a ollyngwyd. (7)

8. Datgelu cronfa ddata heb awdurdod. (6)

Pwynt Gwirio 5, dewis arall: Cliwiau Croesair Hygyrch

Gall defnyddwyr darllenwyr sgrin a bysellfwrdd deipio atebion y croesair yn uniongyrchol yn y meysydd testun isod.

CLIWIAU AR DRAWS

2 ar draws: Ychwanegu halen ar hap at stwnsh cyfrinair. (6 llythyren):

5 ar draws: Tabl o stwnshau cyfrineiriau wedi'u cyfrifo ymlaen llaw. (5 llythyren):

6 ar draws: Gwiriad mewngofnodi â mwy nag un ffactor. (10 llythyren):

7 ar draws: Algorithm stwnsio cyfrineiriau araf. (6 llythyren):

CLIWIAU I LAWR

1 i lawr: Offeryn storio tystlythyrau. (7 llythyren):

3 i lawr: Peirianneg gymdeithasol i ddwyn manylion mewngofnodi. (8 llythyren):

4 i lawr: Profi tystlythyrau a ollyngwyd. (7 llythyren):

8 i lawr: Datgelu cronfa ddata heb awdurdod. (6 llythyren):

Pwynt Gwirio 6: Chwilair Geiriau Cudd

Dewch o hyd i'r 8 term geirfa allweddol sydd wedi'u cuddio yn y grid isod. Gall geiriau fod yn llorweddol, yn fertigol neu'n groeslinol.

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

RHESTR GEIRIAU GEIRFA

STWFFIO BCRYPT TORIAD HALLTU RHEOLWR AMLFFACTOR ENFYS GWERWYDO

Pwynt Gwirio 6, dewis arall: Paru Geirfa Hygyrch

Parwch bob un o'r 8 term geirfa o'r Chwilair â'i ddiffiniad cywir drwy ysgrifennu'r llythyren (A-H) yn y bwlch.

TERMAU GEIRFA
A. STWFFIO
B. BCRYPT
C. TORIAD
D. HALLTU
E. RHEOLWR
F. AMLFFACTOR
G. ENFYS
H. GWERWYDO

	DIFFINIADAU A MEYSYDD PARU
	1. Peirianneg gymdeithasol i ddwyn manylion mewngofnodi.
	2. Datgelu cronfa ddata heb awdurdod.
	3. Algorithm stwnsio cyfrineiriau araf.
	4. Tabl o stwnshau cyfrineiriau wedi'u cyfrifo ymlaen llaw.
	5. Profi tystlythyrau a ollyngwyd.
	6. Ychwanegu halen ar hap at stwnsh cyfrinair.
	7. Offeryn storio tystlythyrau.
	8. Gwiriad mewngofnodi â mwy nag un ffactor.

Pwynt Gwirio 7: Her Geiriau Cymysg

Dad-sgramblwch y llythrennau isod i ddatgelu cysyniadau a thermau allweddol seiberddiogelwch. Ysgrifennwch eich atebion yn y blychau mewnbwn a ddarperir.

1. **FISFOWT** _____
2. **DTRAIO** _____
3. **ORLREWH** _____
4. **FSYEN** _____
5. **YRTBPC** _____
6. **TLHLUA** _____
7. **MFACATORFL** _____
8. **RWWOGDYE** _____

Gweithgaredd Bonws: Meddwl yn Gyflym

3 ATEB YM MHOB CATEGORI. Y PERSON CYNTAF I GWBLHAU'R RHESTR SY'N ENNILL.

1	Arferion diogel y gallwch eu dechrau heddiw			
2	Rheolau ar gyfer cyfrinair cryf			
3	Rheolwyr cyfrineiriau rydych chi'n eu hadnabod			
4	Offer diogelwch rydych chi'n eu hadnabod			
5	Arwyddion rhybudd mewn e-bost			
6	Geiriau hwyliog ar gyfer cyfrinymadrodd hir			
7	Ffyrdd o fewngofnodi heb gyfrinair			
8	Gwybodaeth na ddylech byth ei rhannu			
9	Rhesymau dros ddiweddaru meddalwedd			
10	Pethau i'w gwneud pan fydd cyfrinair yn gollwng			
11	Cyfrifon sydd angen MFA			
12	Mannau na ddylid byth storio cyfrineiriau ynddynt			
13	Arwyddion bod cyfrifiadur wedi'i heintio			
14	Cyfrineiriau gwael y mae pobl yn eu defnyddio			
15	Pethau rydych chi'n gwneud copi wrth gefn ohonynt			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

Cymhwyswch y cysyniadau rydych wedi'u dysgu i ddatrys y senarios go iawn isod.

ASTUDIAETH ACHOS 1: UNIONI GOLLYNGIAD MANYLION MEWNGOFNODI MENTER

👷

Senario: Mae gwasanaeth monitro'r we dywyll yn rhybuddio sefydliad bod tomen cronfa ddata sy'n cynnwys cyfrineiriau gweinyddwyr systemau corfforaethol wedi'i chyhoeddi ar-lein.

Cwestiwn Trafod: Dadansoddwch risgiau'r gollyngiad manylion mewngofnodi, a chynigiwch strategaeth ailosod weinyddol.

ASTUDIAETH ACHOS 2: GWEITHREDU SAFONAU STWNSIO CYFRINEIRIAU

👷

Senario: Ar hyn o bryd mae cronfa ddata menter yn storio cyfrineiriau defnyddwyr gan ddefnyddio hashys MD5 hen ffasiwn heb halen cryptograffig, sy'n eu gwneud yn agored i'w tynnu'n gyflym.

Cwestiwn Trafod: Dyluniwch strategaeth fudo i uwchraddio algorithm hashio'r gronfa ddata.

Pwynt Gwirio 9: Dadgryptio'r Seiffr

Mae gweithiwr proffesiynol seiberddiogelwch yn diogelu asedau rhwydwaith rhag actorion bygythiad ar-lein. Defnyddiwch yr allwedd Llythyren-i-Rif isod i ddadgryptio'r neges drwy ysgrifennu'r llythrennau cyfatebol yn y bylchau gwag.

ALLWEDD AMGRYPTIO LLYTHRENNAU-I-RIFAU

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

4	9	15	7	5	12	21		3	25	6	18	9	14	5	9	18	9	1	21

1		15	12	12	25	14	7	23	25	4		7	25	4	1		13	6	1

Neges wedi'i datgodio:

AWGRYM: MAE POB RHIF YN CYNRYCHIOLI SAFLE'R LLYTHYREN HONNO YN YR WYDDOR (E.E. 1 = A, 2 = B, 26 = Z).

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan A)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q1: Beth yw gollyngiad cyfrineiriau?

Mae gollyngiad cyfrineiriau yn digwydd pan fydd manylion mewngofnodi defnyddwyr yn cael eu datgelu drwy dor-data neu ffurfweddiadau gweinydd anghywir.

Q2: Sut mae hacwyr yn dod o hyd i gyfrineiriau a ollyngwyd?

Mae hacwyr yn sganio fforymau ar y we dywyll, dympiau cronfeydd data cyhoeddus a safleoedd paste lle cyhoeddir data tor-diogelwch [8].

Q3: A yw ailddefnyddio cyfrineiriau'n beryglus?

Ie, oherwydd os caiff un wefan ei pheryglu, gall hacwyr brofi'r un manylion mewngofnodi ar draws miloedd o lwyfannau eraill [3].

Q4: Beth yw halen cryptograffig?

Halen yw data ar hap a ychwanegir at gyfrinair cyn hashio, gan wneud ymosodiadau tablau chwilio rhag-gyfrifedig yn aneffeithiol [2].

Q5: Pam mae MD5 wedi darfod?

Mae MD5 yn hash cyffredinol cyflym a hen ffasiwn, felly gall ymosodwyr brofi dyfaliadau cyfrinair yn hynod gyflym, yn enwedig pan nad oes halen ar y gwerthoedd hash [2].

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan B)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q6: Sut mae rheolwr cyfrineiriau yn diogelu defnyddwyr?

Mae'n cynhyrchu manylion mewngofnodi cymhleth ac unigryw yn awtomatig ar gyfer pob gwefan, gan leihau gwallau cof dynol ac ailddefnyddio.

Q7: Beth yw ymosodiad grym ysgrublaidd (brute force)?

Ymosodiad sy'n profi pob cyfuniad posibl o nodau'n systematig nes dod o hyd i'r cyfrinair cywir [4].

Q8: Sut mae cloi cyfrif allan yn helpu?

Mae cloi cyfrifon neu gyfyngu ar gyfradd yn arafu dyfalu ar-lein dro ar ôl tro ac, ynghyd â monitro ac MFA, yn lleihau'r risg o ymosodiadau grym ysgrublaidd [4].

Q9: A yw prif gyfrineiriau'n ddiogel?

Maent yn ddiogel os ydynt yn gyfrinymadroddion ag entropi uchel nad ydynt byth yn cael eu hailddefnyddio ar systemau gwe eraill.

Q10: A ddylid newid cyfrineiriau'n rheolaidd?

Mae NIST yn dweud na ddylid gorfodi newidiadau cyfnodol; newidiwch nhw pan fo tystiolaeth o beryglu, a rhowch flaenoriaeth i hyd, rhestrau blocio ac MFA [1].

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan C)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q1: Sut mae Argon2 yn cymharu â bcrypt?

Mae OWASP yn rhestru Argon2id fel ei ddewis cyntaf; mae ei osodiadau cof-ddwys yn gwrthsefyll cracio â GPU ac ASIC yn well na bcrypt [2].

Q2: Beth yw ymestyn allweddi?

Techneg sy'n rhedeg algorithm hashio filoedd o weithiau i arafu'r broses o wirio cyfrinair, gan wneud cracio'n ddrud [2].

Q3: Sut mae tablau enfys yn gweithio?

Tablau chwilio rhag-gyfrifedig sy'n cysylltu cyfrineiriau testun plaen â'u gwerthoedd hash, a ddefnyddir i wrthdroi hash heb halen yn gyflym [2].

Q4: Beth yw ailgylchu manylion mewngofnodi?

Ailddefnyddio parau enw defnyddiwr/cyfrinair wedi'u dwyn o un tor-diogelwch i geisio cyrchu gwasanaethau eraill, yn enwedig lle mae pobl wedi ailddefnyddio cyfrineiriau [3].

Q5: A oes modd hacio rheolwyr cyfrineiriau?

Ie. Mae llawer yn defnyddio amgryptio dim gwybodaeth, felly dim ond claddgelloedd amgryptiedig sy'n cael eu datgelu os torrir i mewn i weinydd, ond gellir dal i gracio prif gyfrineiriau gwan all-lein.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan D)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q6: Beth yw ymosodiad geiriadur?

Amrywiad grym ysgrublaidd sy'n profi geiriau cyffredin, ymadroddion a chyfrineiriau a ddatgelwyd yn y gorffennol yn hytrach na llythrennau ar hap.

Q7: Pam mae cyfrinymadroddion yn cael eu ffafrio?

Mae cyfrinymadroddion yn defnyddio sawl gair ar hap, gan greu entropi uchel sy'n hawdd i bobl ei gofio ond sy'n gostus yn gyfrifiadurol i'w gracio [1].

Q8: Sut mae mewngofnodi sengl (SSO) yn effeithio ar ollyngiadau cyfrineiriau?

Mae SSO yn lleihau lledaeniad cyfrineiriau, ond daw'r darparwr hunaniaeth yn darged gwerthfawr sydd angen MFA cryf, sy'n gwrthsefyll gwe-rwydo os oes modd [6].

Q9: Beth yw herwgipio sesiynau?

Mae ymosodwr yn cael gafael ar docyn sesiwn dilys neu'n ei gamddefnyddio i ddynwared defnyddiwr sydd wedi mewngofnodi heb fod angen y cyfrinair eto [5].

Q10: Sut ydych chi'n canfod chwistrellu cyfrineiriau?

Drwy chwilio am yr un llond llaw o gyfrineiriau sy'n cael eu profi ar draws llawer o gyfrifon, yn aml yn araf er mwyn aros o dan drothwyon cloi [7].

Rhan 11: 10 Ffaith a Mewnwelediad Seiberddiogelwch o'r Byd Go Iawn

Adolygwch ffeithiau o'r byd go iawn am dor-diogelwch, mecanweithiau amddiffyn, a safonau cydymffurfio.

1. CIPOLWG AR DDIOGELWCH

Mae NIST SP 800-63B yn mynnu gwirio cyfrineiriau newydd yn erbyn rhestrau blocio o gyfrineiriau cyffredin a rhai a beryglwyd [1].

2. CIPOLWG AR DDIOGELWCH

Cyfunodd dymp 'Collection #1' yn 2019 ddata o lawer o doriadau diogelwch cynharach mewn un ffeil enfawr o barau e-bost a chyfrinair [8].

3. CIPOLWG AR DDIOGELWCH

Mae NIST bellach yn mynnu bod cyfrineiriau a ddefnyddir fel yr unig ffactor dilysu yn o leiaf 15 nod o hyd [1].

4. CIPOLWG AR DDIOGELWCH

Gall caledwedd ASIC gyfrifo biliynau o werthoedd hash SHA-256 yr eiliad, sy'n gwneud hashio SHA crai yn anniogel ar gyfer cyfrineiriau defnyddwyr [2].

5. CIPOLWG AR DDIOGELWCH

Mae halen unigryw yn golygu bod dau ddefnyddiwr â'r union un cyfrinair yn cael gwerthoedd hash gwahanol yn y gronfa ddata [2].

6. CIPOLWG AR DDIOGELWCH

Mae llawer o reolwyr cyfrineiriau yn amgryptio data'r gladdgell yn lleol â chryptograffeg gref sy'n deillio o brif gyfrinair y defnyddiwr.

7. MEWNWELEDIAD DIOGELWCH

Mae credential stuffing yn gweithio am fod llawer o bobl yn ailddefnyddio'r un cyfrinair ar gyfrifon e-fasnach, bancio ac e-bost [3].

8. MEWNWELEDIAD DIOGELWCH

Mae NIST SP 800-63B yn dweud na chaiff dilyswyr fynnu newidiadau cyfnodol i gyfrineiriau, dim ond newidiadau ar ôl tystiolaeth o beryglu [1].

9. MEWNWELEDIAD DIOGELWCH

Nid yw ychwanegu un briflythyren a symbol at gyfrinair byr yn atal ymosodiadau geiriadur GPU awtomataidd modern [1].

10. CIPOLWG AR DDIOGELWCH

Gall MFA rwystro llawer o ymdrechion credential stuffing hyd yn oed ar ôl i gyfrinair ollwng; mae MFA sy'n gwrthsefyll gwe-rwydo yn gryfach na chodau SMS [3].

Cyfeiriadau a Ffynonellau Technegol

Mae'r canllaw astudio a'r posau rhyngweithiol wedi'u llunio o safonau byd-eang NIST, OWASP a chydymffurfio â phreifatrwydd data.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[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/

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Cwestiwn 1** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae stwffio manylion mewngofnodi yn defnyddio awtomeiddio i roi cynnig ar barau enw defnyddiwr/cyfrinair a ollyngwyd ar wefannau eraill [3].

2 **Cwestiwn 2** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae OWASP yn argymell Argon2id yn gyntaf; mae bcrypt yn bennaf ar gyfer systemau etifeddol lle nad yw Argon2id neu scrypt ar gael [2].

3 **Cwestiwn 3** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae MFA yn gofyn am ffactor ychwanegol, felly ni all cyfrinair wedi'i ddwyn ar ei ben ei hun ddatgloi'r cyfrif [3].

4 **Cwestiwn 4** — **Ateb Cywir: A**

NODYN ADDYSGU

Casgliadau o fanylion mewngofnodi a ollyngwyd yw tomenni torri data, fel casgliad Collection #1 yn 2019 [8].

5 **Cwestiwn 5** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae rheolwr cyfrineiriau yn cynhyrchu ac yn storio cyfrinair cryf ac unigryw ar gyfer pob cyfrif, gan atal ailddefnyddio [3].

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gwir: mae cyfrineiriau a ailddefnyddir yn gadael i ymosodwyr ailchwarae manylion mewngofnodi a ollyngwyd o un wefan ar wefannau eraill [3].

7 **Cwestiwn 7** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: hash cyflym yw SHA-1; mae OWASP yn argymell Argon2id, scrypt, bcrypt neu PBKDF2 yn lle hynny [2].

8 **Cwestiwn 8** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: ni all rheolau cymhlethdod ar eu pen eu hunain atal stwffio â chyfrineiriau a ollyngwyd ac a ailddefnyddir; mae angen MFA [3].

9 **Cwestiwn 9** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gwir: mae gwasanaethau monitro yn chwilio tomenni torri data a ffynonellau'r we dywyll am fanylion mewngofnodi sydd wedi'u datgelu [8].

10 **Cwestiwn 10** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gwir: mae halen unigryw ar gyfer pob cyfrinair yn gwneud tablau enfys a gyfrifwyd ymlaen llaw yn aneffeithiol [2].

Allweddi Geirfa a Chyfarwyddyd Marcio

Cyfarwyddyd Marcio i Athrawon: Rhowch 1 pwynt am bob paru cywir (8 pwynt i gyd) a phob term cyd-destun (6 phwynt i gyd).

PWYNT GWIRIO 4: ALLWEDD PARU CYSYNIADAU

F 1. STWFFIO	H 2. BCRYPT	D 3. TORRI DIOGELWCH	G 4. HALLTU
C 5. RHEOLWR	B 6. MFA	A 7. ENFYS	E 8. GWE-RWYDO

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 STWFFIO	2 BCRYPT	3 TORIAD	4 HALLTU
5 RHEOLWR	6 AML-FFACTOR		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 H – GWERWYDO	2 C – TORIAD	3 B – BCRYPT	4 G – ENFYS
5 A – STWFFIO	6 D – HALLTU	7 E – RHEOLWR	8 F – AMLFFACTOR

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio STWFFIO, BCRYPT a TORRI DIOGELWCH yn eu geiriau eu hunain a rhoi enghraifft o bob un.

Astudiaethau Achos:
Gofynnwch i fyfyrwyr gefnogi eu hargymhellion â ffeithiau o'r daflen waith yn hytrach na thybiaethau.

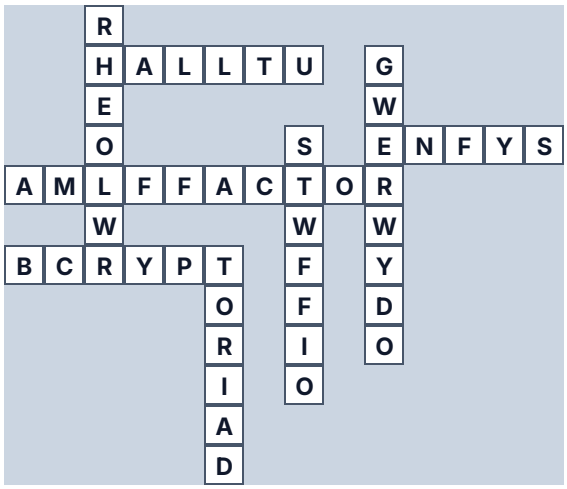
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

2 ar draws: HALLTU Ychwanegu halen ar hap at stwnsh cyfrinair. (6 llythyren)

5 ar draws: ENFYS Tabl o stwnshau cyfrineiriau wedi'u cyfrifo ymlaen llaw. (5 llythyren)

6 ar draws: AMLFFACTOR Gwiriad mewngofnodi â mwy nag un ffactor. (10 llythyren)

7 ar draws: BCRYPT Algorithm stwnsio cyfrineiriau araf. (6 llythyren)

CLIWIAU I LAWR

1 i lawr: RHEOLWR Offeryn storio tystlythyrau. (7 llythyren)

3 i lawr: GWERWYDO Peirianneg gymdeithasol i ddwyn manylion mewngofnodi. (8 llythyren)

4 i lawr: STWFFIO Profi tystlythyrau a ollyngwyd. (7 llythyren)

8 i lawr: TORIAD Datgelu cronfa ddata heb awdurdod. (6 llythyren)

Allwedd Datrys Geiriau Cymysg a Seiffr

Allwedd marcio ar gyfer y gweithgaredd dad-sgramblo geirfa a'r Her Seiffr Gyfrinachol.

ALLWEDD DATRYS GEIRIAU CYMYSG

1. FISFOWT — STWFFIO
2. DTRAIO — TORIAD
3. ORLREWH — RHEOLWR
4. FSYEN — ENFYS
5. YRTBPC — BCRYPT
6. TLHLUA — HALLTU
7. MFACATORFL — AMLFFACTOR
8. RWWOGDYE — GWERWYDO

ALLWEDD HER Y SEIFFR CYFRINACHOL

"DIOGELU CYFRINEIRIAU A OLLYNGWYD GYDA MFA"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Unioni Gollyngiad Manylion Mewngofnodi Menter

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae gwasanaeth monitro'r we dywyll yn rhybuddio sefydliad bod tomen cronfa ddata sy'n cynnwys cyfrineiriau gweinyddwyr systemau corfforaethol wedi'i chyhoeddi ar-lein.
- Strategaeth a Datrysiad a Argymhellir: Dirymwch bob sesiwn weinyddwr weithredol ac ailosodwch y manylion mewngofnodi â generadur entropi uchel. Gorfodwch MFA sy'n gwrthsefyll gwe-rwydo ar byrth gweinyddu [6], cylchdrowch allweddi API yr effeithiwyd arnynt, adolygwch logiau mewngofnodi, dewch o hyd i'r datgeliad cychwynnol a gwiriwch gyfrifon breintiedig eraill.

B Astudiaeth Achos 2: Gweithredu Safonau Stwnsio Cyfrineiriau

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae cronfa ddata menter ar hyn o bryd yn storio cyfrineiriau defnyddwyr gan ddefnyddio stwnshiadau MD5 hen ffasiwn heb halen cryptograffig, sy'n eu gwneud yn agored i gael eu hechdynnu'n gyflym.
- Strategaeth a Datrysiad a Argymhellir: Mabwysiadwch Argon2id (neu bcrypt ar systemau etifeddol) gyda halen unigryw i bob defnyddiwr [2]. Lapiwch werthoedd hash MD5 presennol yn yr algorithm newydd nawr, ail-hashiwch yn uniongyrchol wrth i bob defnyddiwr fewngofnodi nesaf, a gorfodwch ailosod ar gyfrifon sydd wedi bod yn segur ers tro.