Όνομα: _____ **Ημερομηνία:** _____ **Βαθμολογία:** _____

Διαρροές κωδικών πρόσβασης και ασφάλεια διαπιστευτηρίων

Credential stuffing, παραβιάσεις δεδομένων, αλγόριθμοι κατακερματισμού, πολυπαραγοντική ταυτοποίηση και ασφάλεια κωδικών πρόσβασης.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΔΙΑΡΡΟΕΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

ΑΣΦΑΛΙΣΜΕΝΟ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ
Πρότυπο AES 256 bit

ΣΥΜΦΩΝΟ
ΠΑΓΚΟΣΜΙΑ ΠΡΟΤΥΠΑ
Πλαίσια GDPR και CCPA

ZERO-TRUST
ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΗΣ
Έλεγχος ταυτότητας πολλαπλών παραγόντων

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στις διαρροές κωδικών πρόσβασης και την ασφάλεια διαπιστευτηρίων. Θα εξερευνήσεις το credential stuffing, τις παραβιάσεις δεδομένων, τους αλγορίθμους κατακερματισμού, την ταυτοποίηση πολλαπλών παραγόντων και τους διαχειριστές κωδικών πρόσβασης.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Κατάκτησε την κυβερνοασφάλεια και την πρόληψη απειλών.**
- [ ] **Μέρη 5-7: Λύσε γρίφους σταυρολέξου και αναζήτησης λέξεων.**
- [ ] **Μέρη 8-9: Λύσε μελέτες περίπτωσης και πρόκληση κρυπτογραφημένου μηνύματος.**
- [ ] **Μέρος 10: Εξέτασε τις σελίδες συχνών ερωτήσεων βασικού και προχωρημένου επιπέδου.**
- [ ] **Μέρος 11: Εξερεύνησε 10 ενδιαφέροντα πραγματικά στοιχεία.**
- [ ] **Μπόνους: η πρόκληση Σκέψου γρήγορα.**

Άνοιξε τον Οδηγό του VPN.com για την κυβερνοασφάλεια

URL: https://www.vpn.com/el/kiberasfaleia/diasroi-kodikon-prosbasis/

Η πορεία μάθησής σου: ασφάλεια κωδικών πρόσβασης

- Κατανόησε τους κινδύνους έκθεσης διαπιστευτηρίων σε φόρουμ του dark web.
- Εφάρμοσε έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) και παρακολούθηση παραβιασμένων διαπιστευτηρίων.
- Σχεδίασε εταιρικές άμυνες ασφάλειας απέναντι σε στοχευμένες απάτες κοινωνικής μηχανικής.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΟΔΗΓΟ ΔΙΑΡΡΟΩΝ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

Απάντησε στις ερωτήσεις πολλαπλής επιλογής και σωστού/λάθους, συμπλήρωσε τα κενά των προτάσεων με την τράπεζα λέξεων, αντιστοίχισε ορισμούς και λύσε το σταυρόλεξο και τον γρίφο αναζήτησης λέξεων. Εφάρμοσε τις γνώσεις σου στην προστασία των διαπιστευτηρίων. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΔΙΑΡΡΟΕΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΙΑΠΙΣΤΕΥΤΗΡΙΩΝ (ΕΙΣΑΓΩΓΗ)

Οι διαρροές κωδικών πρόσβασης εκθέτουν διαπιστευτήρια χρηστών σε δημόσιους ιστότοπους και στο dark web. Μοναδικοί κωδικοί από διαχειριστή κωδικών, έλεγχος για παραβιασμένους κωδικούς και έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) μειώνουν τον κίνδυνο credential stuffing, ενώ η αργή κατακερματισμένη αποθήκευση κωδικών με salt περιορίζει τη ζημιά αν κλαπεί μια βάση δεδομένων κωδικών.

ΔΙΑΒΑΣΕ ΠΡΟΣΕΚΤΙΚΑ ΚΑΘΕ ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΛΕΞΕ Η ΓΡΑΨΕ ΤΗ ΣΩΣΤΗ ΑΠΑΝΤΗΣΗ.

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **1. Τι είναι το credential stuffing;**
   - A. Χρήση αυτοματισμού για τη δοκιμή διαρρεύσαντων συνδυασμών ονόματος χρήστη/κωδικού πρόσβασης σε πολλούς ιστότοπους
   - B. Κρυπτογράφηση τοπικών αρχείων αποθήκευσης βάσεων δεδομένων
   - C. Υπερφόρτωση διακομιστών ιστού με αιτήματα δικτυακής κίνησης
   - D. Κρυφή παρακολούθηση εισόδων πληκτρολογίου

2. **2. Ποιον αλγόριθμο αναφέρει το OWASP ως πρώτη επιλογή για την αποθήκευση κωδικών πρόσβασης σήμερα;**
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. **3. Πώς περιορίζει η ταυτοποίηση πολλαπλών παραγόντων (MFA) τον κίνδυνο από διαρροές κωδικών πρόσβασης;**
   - A. Απαιτεί έναν πρόσθετο παράγοντα επαλήθευσης, οπότε ένας κλεμμένος κωδικός από μόνος του δεν αρκεί
   - B. Αλλάζει αυτόματα τον κωδικό πρόσβασης κάθε ώρα
   - C. Κρυπτογραφεί το όνομα χρήστη κατά τη μετάδοση
   - D. Ειδοποιεί το γραφείο πίστωσης για παράνομα αιτήματα

4. **4. Τι είναι ένα αρχείο διαρροής δεδομένων (data breach dump);**
   - A. Μια συλλογή διαρρεύσαντων διαπιστευτηρίων χρηστών που δημοσιεύονται στο διαδίκτυο ή πωλούνται σε φόρουμ χάκερ
   - B. Ένα αντίγραφο ασφαλείας των αρχείων της βάσης δεδομένων αποθηκευμένο εκτός χώρου
   - C. Μια προσωρινή μνήμη (cache) αρχείων καταγραφής του διακομιστή ιστού
   - D. Ένα διοικητικό εργαλείο που χρησιμοποιείται για επαναφορά κωδικών πρόσβασης χρηστών

5. **5. Ποιος είναι ο ρόλος ενός διαχειριστή κωδικών πρόσβασης;**
   - A. Δημιουργία και αποθήκευση μοναδικών, ισχυρών κωδικών πρόσβασης για κάθε λογαριασμό
   - B. Παρακολούθηση της κίνησης δικτύου για διαρροές κωδικών πρόσβασης
   - C. Αποκλεισμός αυτοματοποιημένων επιθέσεων ωμής βίας (brute-force) στην πύλη
   - D. Σάρωση μπλοκ αποθήκευσης της βάσης δεδομένων για μη κρυπτογραφημένους κωδικούς πρόσβασης

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Η επαναχρησιμοποίηση κωδικών πρόσβασης σε πολλούς λογαριασμούς αυξάνει τον κίνδυνο credential stuffing.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Το SHA-1 είναι συνιστώμενη συνάρτηση κατακερματισμού για σύγχρονη αποθήκευση κωδικών πρόσβασης.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Η επιβολή πολυπλοκότητας κωδικών πρόσβασης μόνη της (χωρίς MFA) σταματά πλήρως το credential stuffing.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Τα εργαλεία παρακολούθησης του σκοτεινού ιστού σαρώνουν το διαδίκτυο για παραβιασμένα εταιρικά διαπιστευτήρια.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Οι κατακερματισμοί με salt προσθέτουν μοναδικά τυχαία δεδομένα στους κωδικούς πρόσβασης πριν από τον κατακερματισμό, για να αντιμετωπίσουν επιθέσεις με πίνακες rainbow.

○ Σωστό ○ Λάθος

Σημείο ελέγχου 3: Συμπλήρωση βασικών όρων

Διάβασε κάθε πρόταση παρακάτω και συμπλήρωσε το κενό με τον σωστό όρο από την Τράπεζα Λέξεων.

1. Η δοκιμή διαρρεύσαντων διαπιστευτηρίων σε πολλές διαδικτυακές εφαρμογές είναι το _____ διαπιστευτηρίων.

2. Ένας αργός, προσαρμοστικός αλγόριθμος κατακερματισμού κωδικών που εξακολουθεί να γίνεται δεκτός από το OWASP είναι ο _____ .

3. Η έκθεση εμπιστευτικών αρχείων βάσεων δεδομένων στο διαδίκτυο αποτελεί _____ δεδομένων.

4. Η προσθήκη τυχαίων τιμών στους κωδικούς πριν από τον κατακερματισμό ονομάζεται _____ .

5. Μια ασφαλής τοπική βάση δεδομένων για διαπιστευτήρια χρηστών είναι ένας _____ κωδικών πρόσβασης.

6. Η προσθήκη δεύτερου βήματος επαλήθευσης σύνδεσης χρησιμοποιεί την πολυπαραγοντική ταυτοποίηση, δηλαδή _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΛΑΤΙΣΜΑ ΓΕΜΙΣΜΑ ΔΙΑΧΕΙΡΙΣΤΗΣ ΟΥΡΑΝΙΟ ΤΟΞΟ ΠΑΡΑΒΙΑΣΗ ΨΑΡΕΜΑ
BCRYPT MFA

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

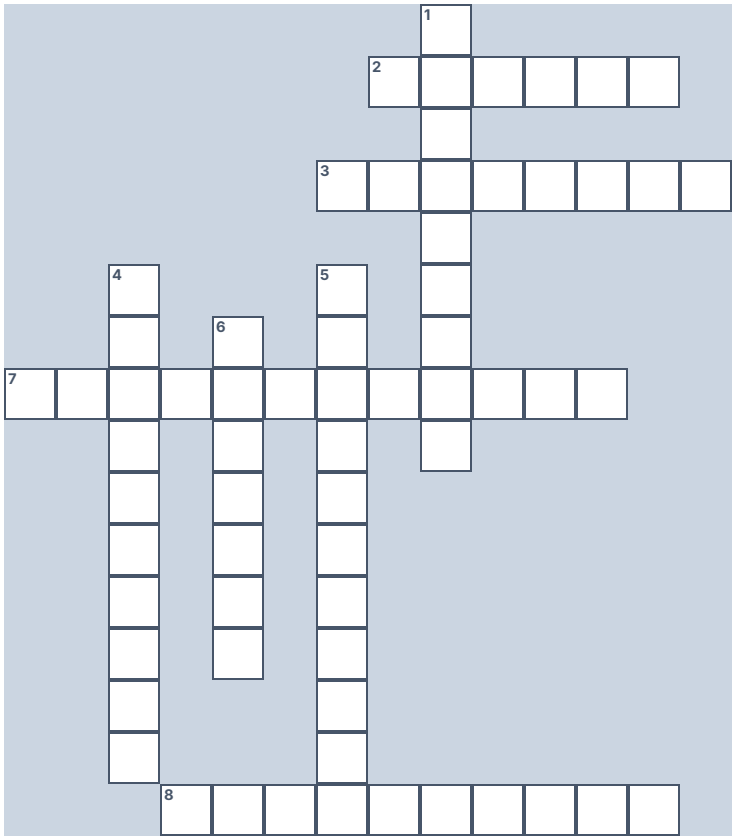
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

Αντιστοίχισε κάθε όρο λεξιλογίου στα αριστερά με τον σωστό ορισμό του στα δεξιά, γράφοντας το αντίστοιχο γράμμα (A-H) στο πλαίσιο εισαγωγής.

☐	1. STUFFING	A	Προϋπολογισμένος πίνακας κατακερματισμών κωδικών πρόσβασης.
☐	2. BCRYPT	B	Έλεγχος σύνδεσης πολλαπλών παραγόντων.
☐	3. ΔΙΑΡΡΗΞΗ	C	Εργαλείο αποθήκευσης διαπιστευτηρίων.
☐	4. ΠΡΟΣΘΗΚΗ SALT	D	Μη εξουσιοδοτημένη έκθεση βάσης δεδομένων.
☐	5. ΔΙΑΧΕΙΡΙΣΤΗΣ	E	Κοινωνική μηχανική για κλοπή διαπιστευτηρίων σύνδεσης.
☐	6. MFA	F	Δοκιμή διαρρεύσαντων διαπιστευτηρίων.
☐	7. ΟΥΡΑΝΙΟ ΤΟΞΟ	G	Προσθήκη τυχαίου salt στον κατακερματισμό (hash) του κωδικού πρόσβασης.
☐	8. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	H	Αργός αλγόριθμος κατακερματισμού κωδικών πρόσβασης.

Σημείο ελέγχου 5: Σταυρόλεξο

Λύσε το σταυρόλεξο πληκτρολογώντας γράμματα στα ενεργά λευκά κουτιά. Οι αριθμοί αντιστοιχούν στις οδηγίες παρακάτω.



ΟΡΙΖΟΝΤΙΑ

2. Κοινωνική μηχανική για την κλοπή στοιχείων σύνδεσης (6)

3. Προσθήκη τυχαίου salt στον κατακερματισμό κωδικού (8)

7. Εργαλείο αποθήκευσης διαπιστευτηρίων (12)

8. Αργή μαθηματική διαδικασία που μετατρέπει τους κωδικούς σε μη αναστρέψιμη τιμή (10)

ΚΑΘΕΤΑ

1. Μη εξουσιοδοτημένη έκθεση βάσης δεδομένων (9)

4. Έλεγχος σύνδεσης πολλαπλών παραγόντων (10)

5. Προϋπολογισμένος πίνακας κατακερματισμών κωδικών (11)

6. Δοκιμή διαρρεύσαντων διαπιστευτηρίων (7)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

Οι χρήστες αναγνώστη οθόνης και πληκτρολογίου μπορούν να πληκτρολογήσουν τις απαντήσεις του σταυρολέξου απευθείας στα πεδία κειμένου παρακάτω.

ΟΡΙΖΟΝΤΙΑ

2 οριζόντια: Κοινωνική μηχανική για την κλοπή στοιχείων σύνδεσης (6 γράμματα):

3 οριζόντια: Προσθήκη τυχαίου salt στον κατακερματισμό κωδικού (8 γράμματα):

7 οριζόντια: Εργαλείο αποθήκευσης διαπιστευτηρίων (12 γράμματα):

8 οριζόντια: Αργή μαθηματική διαδικασία που μετατρέπει τους κωδικούς σε μη αναστρέψιμη τιμή (10 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Μη εξουσιοδοτημένη έκθεση βάσης δεδομένων (9 γράμματα):

4 κάθετα: Έλεγχος σύνδεσης πολλαπλών παραγόντων (10 γράμματα):

5 κάθετα: Προϋπολογισμένος πίνακας κατακερματισμών κωδικών (11 γράμματα):

6 κάθετα: Δοκιμή διαρρεύσαντων διαπιστευτηρίων (7 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

Βρες τους 8 βασικούς όρους λεξιλογίου που κρύβονται στο παρακάτω πλέγμα. Οι λέξεις μπορεί να είναι οριζόντιες, κάθετες ή διαγώνιες.

Γ Ε Μ Ι Σ Μ Α Ε Σ Ω Υ Γ Ω Φ Ζ
Ο Α Κ Η Ω Δ Ν Π Δ Π Π Χ Ο Γ Τ
Ξ Μ Β Α Ω Ν Δ Α Λ Α Α Δ Ξ Δ Ε
Ο Σ Η Θ Δ Ρ Π Λ Μ Ε Ρ Θ Ρ Ω Σ
Τ Ι Ε Π Υ Ε Α Η Α Π Α Ξ Ν Α Ο
Ο Τ Τ Χ Π Κ Ρ Θ Τ Ρ Β Γ Ν Λ Ψ
Ι Α Β Ζ Ρ Χ Φ Ε Ι Α Ι Ρ Ω Γ Ψ
Ν Λ Ψ Λ Ζ Θ Μ Υ Π Κ Α Μ Μ Ο Σ
Α Α Ξ Η Ο Π Η Σ Ω Α Σ Ξ Υ Ρ Ζ
Ρ Υ Β Ψ Ρ Ψ Β Η Η Μ Η Ω Η Ι Κ
Υ Δ Ι Α Χ Ε Ι Ρ Ι Σ Τ Η Σ Θ Ξ
Ο Ο Ν Χ Γ Μ Ω Ψ Ζ Ψ Ξ Φ Υ Μ Λ
Υ Ο Ψ Α Ρ Ε Μ Α Β Ν Φ Τ Μ Ο Η
Υ Γ Ψ Υ Κ Ρ Α Χ Ω Ψ Μ Ρ Π Σ Χ
Θ Ξ Δ Α Γ Κ Π Φ Χ Χ Λ Ι Θ Τ Θ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΓΕΜΙΣΜΑ ΑΛΓΟΡΙΘΜΟΣ ΠΑΡΑΒΙΑΣΗ ΑΛΑΤΙΣΜΑ ΔΙΑΧΕΙΡΙΣΤΗΣ ΕΠΑΛΗΘΕΥΣΗ
ΟΥΡΑΝΙΟΤΟΞΟ ΨΑΡΕΜΑ

Σημείο ελέγχου 6, εναλλακτικά: Προσβάσιμη αντιστοίχιση λεξιλογίου

Αντιστοίχισε καθέναν από τους 8 όρους λεξιλογίου του Word Search με τον σωστό ορισμό του, γράφοντας το γράμμα (A-H) στο κενό.

ΟΡΟΙ ΛΕΞΙΛΟΓΙΟΥ
A. ΓΕΜΙΣΜΑ
B. ΑΛΓΟΡΙΘΜΟΣ
C. ΠΑΡΑΒΙΑΣΗ
D. ΑΛΑΤΙΣΜΑ
E. ΔΙΑΧΕΙΡΙΣΤΗΣ
F. ΕΠΑΛΗΘΕΥΣΗ
G. ΟΥΡΑΝΙΟΤΟΞΟ
H. ΨΑΡΕΜΑ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ	
	1. Κοινωνική μηχανική για την κλοπή στοιχείων σύνδεσης.
	2. Μη εξουσιοδοτημένη έκθεση βάσης δεδομένων.
	3. Αργή μαθηματική διαδικασία που μετατρέπει τους κωδικούς σε μη αναστρέψιμη τιμή.
	4. Προϋπολογισμένος πίνακας κατακερματισμών κωδικών.
	5. Δοκιμή διαρρεύσαντων διαπιστευτηρίων.
	6. Προσθήκη τυχαίου salt στον κατακερματισμό κωδικού.
	7. Εργαλείο αποθήκευσης διαπιστευτηρίων.
	8. Έλεγχος σύνδεσης πολλαπλών παραγόντων.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους της κυβερνοασφάλειας. Γράψε τις απαντήσεις σου στα διαθέσιμα πλαίσια εισαγωγής.

1. ΙΜΓΣΑΜΕ
2. ΗΠΣΑΑΙΑΒΡ
3. ΔΙΙΡΗΣΑΙΣΕΤΧ
4. ΟΞΟΙΡΝΟΤΟΥΑ
5. ΜΙΣΛΟΘΡΑΟΓ
6. ΜΑΤΣΑΙΛΑ
7. ΠΛΕΕΘΥΣΗΗΑ
8. ΡΑΨΜΕΑ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

3 ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ. ΚΕΡΔΙΖΕΙ ΟΠΟΙΟΣ ΣΥΜΠΛΗΡΩΣΕΙ ΠΡΩΤΟΣ ΤΗ ΛΙΣΤΑ.

1	**Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα**			
2	**Κανόνες για έναν ισχυρό κωδικό πρόσβασης**			
3	**Διαχειριστές κωδικών πρόσβασης που γνωρίζεις**			
4	**Εργαλεία ασφαλείας που γνωρίζεις**			
5	**Προειδοποιητικά σημάδια σε ένα email**			
6	**Διασκεδαστικές λέξεις για μια μεγάλη φράση πρόσβασης**			
7	**Τρόποι να συνδεθείς χωρίς κωδικό πρόσβασης**			
8	**Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι**			
9	**Λόγοι για να ενημερώνεις το λογισμικό**			
10	**Πράγματα που κάνεις όταν διαρρεύσει ένας κωδικός πρόσβασης**			
11	**Λογαριασμοί που χρειάζονται MFA**			
12	**Μέρη όπου δεν πρέπει ποτέ να αποθηκεύονται οι κωδικοί πρόσβασης**			
13	**Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί**			
14	**Κακοί κωδικοί πρόσβασης που χρησιμοποιούν οι άνθρωποι**			
15	**Πράγματα που παίρνεις αντίγραφο ασφαλείας**			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

Εφάρμοσε τις έννοιες που έμαθες για να λύσεις τα παρακάτω σενάρια πραγματικού κόσμου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΑΠΟΚΑΤΑΣΤΑΣΗ ΔΙΑΡΡΟΗΣ ΕΤΑΙΡΙΚΩΝ ΔΙΑΠΙΣΤΕΥΤΗΡΙΩΝ

👷

Σενάριο: Μια υπηρεσία παρακολούθησης του dark web ειδοποιεί έναν οργανισμό ότι ένα dump βάσης δεδομένων που περιέχει κωδικούς πρόσβασης διαχειριστών εταιρικών συστημάτων έχει δημοσιευτεί online.

Ερώτηση συζήτησης: Ανάλυσε τους κινδύνους της διαρροής διαπιστευτηρίων και πρότεινε μια στρατηγική διοικητικής επαναφοράς.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΕΦΑΡΜΟΓΗ ΠΡΟΤΥΠΩΝ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

👷

Σενάριο: Μια εταιρική βάση δεδομένων αποθηκεύει προς το παρόν κωδικούς πρόσβασης χρηστών με παρωχημένους κατακερματισμούς MD5 χωρίς κρυπτογραφικό salt, κάτι που τους κάνει ευάλωτους σε γρήγορη εξαγωγή.

Ερώτηση συζήτησης: Σχεδίασε μια στρατηγική μετάβασης για την αναβάθμιση του αλγορίθμου κατακερματισμού της βάσης δεδομένων.

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας επαγγελματίας κυβερνοασφάλειας προστατεύει τα περιουσιακά στοιχεία του δικτύου από διαδικτυακούς φορείς απειλών. Χρησιμοποίησε το παρακάτω κλειδί Γράμμα-Αριθμός για να αποκρυπτογραφήσεις το μήνυμα γράφοντας τα αντίστοιχα γράμματα στα κενά.

ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΓΡΑΜΜΑΤΟΣ ΣΕ ΑΡΙΘΜΟ

Α=1 Β=2 Γ=3 Δ=4 Ε=5 Ζ=6 Η=7 Θ=8

Ι=9 Κ=10 Λ=11 Μ=12 Ν=13 Ξ=14 Ο=15 Π=16

Ρ=17 Σ=18 Τ=19 Υ=20 Φ=21 Χ=22 Ψ=23 Ω=24

16	17	15	18	19	1	19	5	23	5		19	15	20	18

10	24	4	9	10	15	20	18		12	5		16	15	11	11	1	16	11	7

5	16	1	11	7	8	5	20	18	7

Αποκρυπτογραφημένο μήνυμα:

ΣΥΜΒΟΥΛΗ: ΚΑΘΕ ΑΡΙΘΜΟΣ ΕΚΠΡΟΣΩΠΕΙ ΤΗ ΘΕΣΗ ΤΟΥ ΓΡΑΜΜΑΤΟΣ ΣΤΟ ΑΛΦΑΒΗΤΟ (Π.Χ. 1 = Α, 2 = Β, 24 = Ω).

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Α)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q1: Τι είναι μια διαρροή κωδικών πρόσβασης;

Μια διαρροή κωδικών πρόσβασης συμβαίνει όταν τα διαπιστευτήρια σύνδεσης των χρηστών εκτίθενται μέσω παραβιάσεων δεδομένων ή εσφαλμένων ρυθμίσεων διακομιστών.

Q2: Πώς βρίσκουν οι χάκερ διαρρεύσαντες κωδικούς πρόσβασης;

Οι χάκερ σαρώνουν φόρουμ του dark web, δημόσια αρχεία απόρριψης βάσεων δεδομένων και ιστότοπους επικόλλησης (paste sites) όπου δημοσιεύονται δεδομένα παραβιάσεων [8].

Q3: Είναι επικίνδυνη η επαναχρησιμοποίηση κωδικών πρόσβασης;

Ναι, επειδή αν παραβιαστεί ένας ιστότοπος, οι χάκερ μπορούν να δοκιμάσουν τα ίδια διαπιστευτήρια σε χιλιάδες άλλες πλατφόρμες [3].

Q4: Τι είναι το κρυπτογραφικό salt;

Το salt είναι τυχαία δεδομένα που προστίθενται σε έναν κωδικό πρόσβασης πριν από τον κατακερματισμό, καθιστώντας αναποτελεσματικές τις επιθέσεις με προϋπολογισμένους πίνακες αναζήτησης [2].

Q5: Γιατί το MD5 είναι ξεπερασμένο;

Το MD5 είναι μια γρήγορη, ξεπερασμένη συνάρτηση κατακερματισμού γενικής χρήσης, γι' αυτό οι επιτιθέμενοι μπορούν να δοκιμάζουν εικασίες κωδικών πρόσβασης εξαιρετικά γρήγορα, ειδικά όταν οι κατακερματισμοί δεν έχουν salt [2].

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Β)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q6: Πώς προστατεύει τους χρήστες ένας διαχειριστής κωδικών πρόσβασης;

Δημιουργεί αυτόματα σύνθετα, μοναδικά διαπιστευτήρια για κάθε ιστότοπο, μειώνοντας τα ανθρώπινα λάθη μνήμης και την επαναχρησιμοποίηση.

Q7: Τι είναι μια επίθεση ωμής βίας (brute force);

Μια επίθεση που δοκιμάζει συστηματικά κάθε πιθανό συνδυασμό χαρακτήρων μέχρι να βρεθεί ο σωστός κωδικός πρόσβασης [4].

Q8: Πώς βοηθά το κλείδωμα λογαριασμού;

Το κλείδωμα ή ο περιορισμός ρυθμού επιβραδύνει τις επαναλαμβανόμενες διαδικτυακές δοκιμές μαντεψιάς και, σε συνδυασμό με την παρακολούθηση και το MFA, μειώνει τον κίνδυνο επίθεσης ωμής βίας [4].

Q9: Είναι ασφαλείς οι κύριοι κωδικοί πρόσβασης;

Είναι ασφαλείς αν είναι φράσεις πρόσβασης υψηλής εντροπίας που δεν επαναχρησιμοποιούνται ποτέ σε άλλα συστήματα του διαδικτύου.

Q10: Πρέπει να αλλάζουμε τακτικά τους κωδικούς πρόσβασης;

Το NIST λέει να μην επιβάλλονται περιοδικές αλλαγές· να αλλάζουν μόνο με ένδειξη παραβίασης και να δίνεται προτεραιότητα στο μήκος, τις λίστες αποκλεισμού και το MFA [1].

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q1: Πώς συγκρίνεται το Argon2 με το bcrypt;

Το OWASP αναφέρει το Argon2id ως πρώτη επιλογή· οι ρυθμίσεις του που απαιτούν μνήμη αντιστέκονται στην αποκρυπτογράφηση με GPU και ASIC καλύτερα από το bcrypt [2].

Q2: Τι είναι το key stretching;

Μια τεχνική που επαναλαμβάνει έναν αλγόριθμο κατακερματισμού χιλιάδες φορές για να επιβραδύνει τη διαδικασία επαλήθευσης κωδικών πρόσβασης, καθιστώντας το σπάσιμο δαπανηρό [2].

Q3: Πώς λειτουργούν οι rainbow tables;

Είναι προϋπολογισμένοι πίνακες αναζήτησης που συνδέουν κωδικούς πρόσβασης απλού κειμένου με τα hash τους και χρησιμοποιούνται για την ταχεία αντιστροφή hash χωρίς salt [2].

Q4: Τι είναι η ανακύκλωση διαπιστευτηρίων;

Επαναχρησιμοποίηση κλεμμένων ζευγών ονόματος χρήστη/κωδικού από μία παραβίαση για απόπειρα πρόσβασης σε άλλες υπηρεσίες, ειδικά όταν οι άνθρωποι έχουν επαναχρησιμοποιήσει κωδικούς πρόσβασης [3].

Q5: Μπορούν να παραβιαστούν οι διαχειριστές κωδικών πρόσβασης;

Ναι. Πολλοί χρησιμοποιούν κρυπτογράφηση μηδενικής γνώσης, ώστε μια παραβίαση διακομιστή να εκθέτει μόνο κρυπτογραφημένα θησαυροφυλάκια, αλλά οι αδύναμοι κύριοι κωδικοί πρόσβασης μπορούν και πάλι να σπάσουν εκτός σύνδεσης.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q6: Τι είναι μια επίθεση λεξικού;

Μια παραλλαγή brute-force που δοκιμάζει συνηθισμένες λέξεις, φράσεις και κωδικούς πρόσβασης που έχουν διαρρεύσει στο παρελθόν, αντί για τυχαία γράμματα.

Q7: Γιατί προτιμώνται οι φράσεις πρόσβασης (passphrases);

Οι φράσεις πρόσβασης χρησιμοποιούν πολλές τυχαίες λέξεις, δημιουργώντας υψηλή εντροπία που είναι εύκολο να την απομνημονεύσουν οι άνθρωποι αλλά υπολογιστικά δαπανηρή να σπάσει [1].

Q8: Πώς επηρεάζει η ενιαία σύνδεση (SSO) τις διαρροές κωδικών πρόσβασης;

Το SSO μειώνει τον πολλαπλασιασμό των κωδικών πρόσβασης, αλλά ο πάροχος ταυτότητας γίνεται στόχος υψηλής αξίας που χρειάζεται ισχυρό, κατά προτίμηση ανθεκτικό στο ηλεκτρονικό ψάρεμα MFA [6].

Q9: Τι είναι η υφαρπαγή συνεδρίας (session hijacking);

Ένας επιτιθέμενος αποκτά ή καταχράται ένα έγκυρο διακριτικό συνεδρίας για να υποδυθεί έναν συνδεδεμένο χρήστη χωρίς να χρειάζεται ξανά τον κωδικό πρόσβασης [5].

Q10: Πώς εντοπίζεις επιθέσεις password spraying;

Αναζητώντας τους ίδιους λίγους κωδικούς πρόσβασης που δοκιμάζονται σε πολλούς λογαριασμούς, συχνά αργά ώστε να μένουν κάτω από τα όρια κλειδώματος [7].

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για την κυβερνοασφάλεια

Εξέτασε πραγματικά στοιχεία για τις παραβιάσεις ασφαλείας, τους μηχανισμούς άμυνας και τα πρότυπα συμμόρφωσης.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το NIST SP 800-63B απαιτεί οι νέοι κωδικοί πρόσβασης να ελέγχονται έναντι λιστών αποκλεισμού κοινών και παραβιασμένων κωδικών [1].

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το dump του 2019 'Collection #1' συγχώνευσε δεδομένα από πολλές προηγούμενες παραβιάσεις σε ένα τεράστιο αρχείο με ζεύγη email και κωδικών πρόσβασης [8].

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το NIST πλέον απαιτεί οι κωδικοί πρόσβασης που χρησιμοποιούνται ως μοναδικός παράγοντας ταυτοποίησης να έχουν μήκος τουλάχιστον 15 χαρακτήρων [1].

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το υλικό ASIC μπορεί να υπολογίσει δισεκατομμύρια κατακερματισμούς SHA-256 ανά δευτερόλεπτο, καθιστώντας τον απλό κατακερματισμό SHA μη ασφαλή για τους κωδικούς πρόσβασης των χρηστών [2].

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα μοναδικά salts σημαίνουν ότι δύο χρήστες με ακριβώς τον ίδιο κωδικό πρόσβασης έχουν διαφορετικά hash στη βάση δεδομένων [2].

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Πολλοί διαχειριστές κωδικών πρόσβασης κρυπτογραφούν τοπικά τα δεδομένα του θησαυροφυλακίου με ισχυρή κρυπτογραφία που προέρχεται από τον κύριο κωδικό πρόσβασης του χρήστη.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το credential stuffing λειτουργεί επειδή πολλοί άνθρωποι επαναχρησιμοποιούν τον ίδιο κωδικό πρόσβασης σε λογαριασμούς ηλεκτρονικού εμπορίου, τραπεζών και email [3].

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το NIST SP 800-63B αναφέρει ότι οι επαληθευτές δεν πρέπει να απαιτούν περιοδικές αλλαγές κωδικού πρόσβασης, παρά μόνο μετά από ένδειξη παραβίασης [1].

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η προσθήκη ενός κεφαλαίου γράμματος και ενός συμβόλου σε έναν σύντομο κωδικό πρόσβασης δεν σταματά τις σύγχρονες αυτοματοποιημένες επιθέσεις λεξικού με GPU [1].

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το MFA μπορεί να αποκλείσει πολλές απόπειρες credential stuffing ακόμη και μετά από διαρροή κωδικού πρόσβασης· το MFA ανθεκτικό στο ηλεκτρονικό ψάρεμα (phishing) είναι ισχυρότερο από τους κωδικούς SMS [3].

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια πρότυπα NIST, OWASP και συμμόρφωσης με την ιδιωτικότητα των δεδομένων.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[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/

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το credential stuffing χρησιμοποιεί αυτοματισμό για να δοκιμάσει διαρρεύσαντα ζεύγη ονόματος χρήστη/κωδικού πρόσβασης σε άλλους ιστότοπους [3].

2 Ερώτηση 2 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το OWASP συνιστά πρώτα το Argon2id· το bcrypt προορίζεται κυρίως για παλαιά συστήματα όπου δεν είναι διαθέσιμα το Argon2id ή το scrypt [2].

3 Ερώτηση 3 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το MFA απαιτεί έναν πρόσθετο παράγοντα, οπότε ένας κλεμμένος κωδικός πρόσβασης από μόνος του δεν μπορεί να ξεκλειδώσει τον λογαριασμό [3].

4 Ερώτηση 4 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα breach dump είναι συλλογές διαρρεύσαντων διαπιστευτηρίων, όπως η συλλογή Collection #1 του 2019 [8].

5 Ερώτηση 5 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένας διαχειριστής κωδικών πρόσβασης δημιουργεί και αποθηκεύει έναν μοναδικό, ισχυρό κωδικό για κάθε λογαριασμό, αποτρέποντας την επαναχρησιμοποίηση [3].

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Ερώτηση 6

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Σωστό: οι κωδικοί που επαναχρησιμοποιούνται επιτρέπουν στους επιτιθέμενους να επαναλάβουν διαπιστευτήρια που διέρρευσαν από έναν ιστότοπο σε άλλους ιστότοπους [3].

7 Ερώτηση 7

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το SHA-1 είναι γρήγορη συνάρτηση κατακερματισμού· το OWASP συνιστά αντί γι' αυτό Argon2id, scrypt, bcrypt ή PBKDF2 [2].

8 Ερώτηση 8

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: οι κανόνες πολυπλοκότητας από μόνοι τους δεν μπορούν να σταματήσουν το stuffing με διαρρεύσαντες κωδικούς που επαναχρησιμοποιούνται· χρειάζεται MFA [3].

9 Ερώτηση 9

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Σωστό: οι υπηρεσίες παρακολούθησης αναζητούν σε breach dump και πηγές του dark web εκτεθειμένα διαπιστευτήρια [8].

10 Ερώτηση 10

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Σωστό: ένα μοναδικό salt ανά κωδικό καθιστά αναποτελεσματικούς τους προϋπολογισμένους rainbow tables [2].

Λύσεις λεξιλογίου και κριτήρια βαθμολόγησης

Κριτήρια βαθμολόγησης για τον εκπαιδευτικό: Δώσε 1 μονάδα για κάθε σωστή αντιστοίχιση (σύνολο 8 μονάδες) και για κάθε όρο περιεχομένου (σύνολο 6 μονάδες).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΕΝΝΟΙΩΝ

F 1. STUFFING	H 2. BCRYPT	D 3. ΔΙΑΡΡΗΞΗ	G 4. ΠΡΟΣΘΗΚΗ SALT
C 5. ΔΙΑΧΕΙΡΙΣΤΗΣ	B 6. MFA	A 7. ΟΥΡΑΝΙΟ ΤΟΞΟ	E 8. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΓΕΜΙΣΜΑ	2 BCRYPT	3 ΠΑΡΑΒΙΑΣΗ	4 ΑΛΑΤΙΣΜΑ
5 ΔΙΑΧΕΙΡΙΣΤΗΣ	6 MFA		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 H – ΨΑΡΕΜΑ	2 C – ΠΑΡΑΒΙΑΣΗ	3 B – ΑΛΓΟΡΙΘΜΟΣ	4 G – ΟΥΡΑΝΙΟΤΟΞΟ
5 A – ΓΕΜΙΣΜΑ	6 D – ΑΛΑΤΙΣΜΑ	7 E – ΔΙΑΧΕΙΡΙΣΤΗΣ	8 F – ΕΠΑΛΗΘΕΥΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους STUFFING, BCRYPT και ΔΙΑΡΡΗΞΗ και να δώσουν ένα παράδειγμα για τον καθένα.

Μελέτες περίπτωσης:
Ζήτησε από τους μαθητές να στηρίζουν τις προτάσεις τους σε στοιχεία του φύλλου εργασίας και όχι σε υποθέσεις.

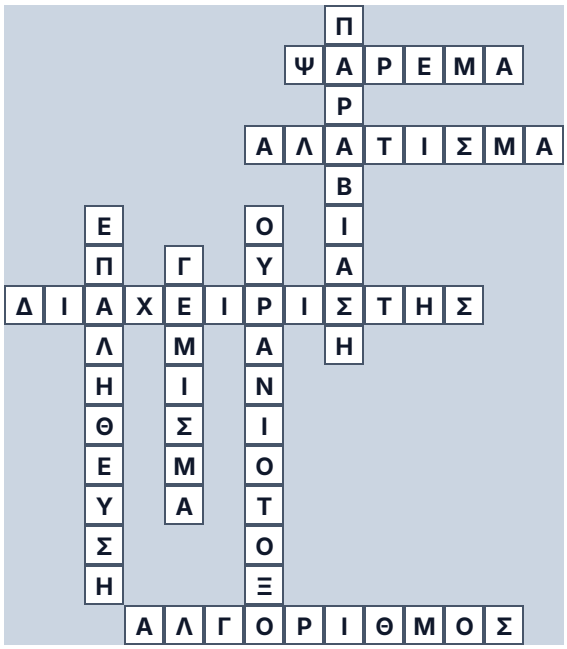
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

Γ	Ε	Μ	Ι	Σ	Μ	Α	Ε	Σ	Ω	Υ	Γ	Ω	Φ	Ζ
Ο	Α	Κ	Η	Ω	Δ	Ν	Π	Δ	Π	Π	Χ	Ο	Γ	Τ
Ξ	Μ	Β	Α	Ω	Ν	Δ	Α	Λ	Α	Α	Δ	Ξ	Δ	Ε
Ο	Σ	Η	Θ	Δ	Ρ	Π	Λ	Μ	Ε	Ρ	Θ	Ρ	Ω	Σ
Τ	Ι	Ε	Π	Υ	Ε	Α	Η	Α	Π	Α	Ξ	Ν	Α	Ο
Ο	Τ	Τ	Χ	Π	Κ	Ρ	Θ	Τ	Ρ	Β	Γ	Ν	Λ	Ψ
Ι	Α	Β	Ζ	Ρ	Χ	Φ	Ε	Ι	Α	Ι	Ρ	Ω	Γ	Ψ
Ν	Λ	Ψ	Λ	Ζ	Θ	Μ	Υ	Π	Κ	Α	Μ	Μ	Ο	Σ
Α	Α	Ξ	Η	Ο	Π	Η	Σ	Ω	Α	Σ	Ξ	Υ	Ρ	Ζ
Ρ	Υ	Β	Ψ	Ρ	Ψ	Β	Η	Η	Μ	Η	Ω	Η	Ι	Κ
Υ	Δ	Ι	Α	Χ	Ε	Ι	Ρ	Ι	Σ	Τ	Η	Σ	Θ	Ξ
Ο	Ο	Ν	Χ	Γ	Μ	Ω	Ψ	Ζ	Ψ	Ξ	Φ	Υ	Μ	Λ
Υ	Ο	Ψ	Α	Ρ	Ε	Μ	Α	Β	Ν	Φ	Τ	Μ	Ο	Η
Υ	Γ	Ψ	Υ	Κ	Ρ	Α	Χ	Ω	Ψ	Μ	Ρ	Π	Σ	Χ
Θ	Ξ	Δ	Α	Γ	Κ	Π	Φ	Χ	Χ	Λ	Ι	Θ	Τ	Θ

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

2 οριζόντια: ΨΑΡΕΜΑ Κοινωνική μηχανική για την κλοπή στοιχείων σύνδεσης (6 γράμματα)

3 οριζόντια: ΑΛΑΤΙΣΜΑ Προσθήκη τυχαίου salt στον κατακερματισμό κωδικού (8 γράμματα)

7 οριζόντια: ΔΙΑΧΕΙΡΙΣΤΗΣ Εργαλείο αποθήκευσης διαπιστευτηρίων (12 γράμματα)

8 οριζόντια: ΑΛΓΟΡΙΘΜΟΣ Αργή μαθηματική διαδικασία που μετατρέπει τους κωδικούς σε μη αναστρέψιμη τιμή (10 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΠΑΡΑΒΙΑΣΗ Μη εξουσιοδοτημένη έκθεση βάσης δεδομένων (9 γράμματα)

4 κάθετα: ΕΠΑΛΗΘΕΥΣΗ Έλεγχος σύνδεσης πολλαπλών παραγόντων (10 γράμματα)

5 κάθετα: ΟΥΡΑΝΙΟΤΟΞΟ Προϋπολογισμένος πίνακας κατακερματισμών κωδικών (11 γράμματα)

6 κάθετα: ΓΕΜΙΣΜΑ Δοκιμή διαρρεύσαντων διαπιστευτηρίων (7 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

Κλειδί βαθμολόγησης για τη δραστηριότητα αποκωδικοποίησης λέξεων λεξιλογίου και την πρόκληση Secret Cipher.

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΙΜΓΣΑΜΕ — **ΓΕΜΙΣΜΑ**
2. ΗΠΣΑΑΙΑΒΡ — **ΠΑΡΑΒΙΑΣΗ**
3. ΔΙΙΡΗΣΑΙΣΕΤΧ — **ΔΙΑΧΕΙΡΙΣΤΗΣ**
4. ΟΞΟΙΡΝΟΤΟΥΑ — **ΟΥΡΑΝΙΟΤΟΞΟ**
5. ΜΙΣΛΟΘΡΑΟΓ — **ΑΛΓΟΡΙΘΜΟΣ**
6. ΜΑΤΣΑΙΛΑ — **ΑΛΑΤΙΣΜΑ**
7. ΠΛΕΕΘΥΣΗΗΑ — **ΕΠΑΛΗΘΕΥΣΗ**
8. ΡΑΨΜΕΑ — **ΨΑΡΕΜΑ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΠΡΟΣΤΑΤΕΨΕ ΤΟΥΣ ΚΩΔΙΚΟΥΣ ΜΕ ΠΟΛΛΑΠΛΗ ΕΠΑΛΗΘΕΥΣΗ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Αποκατάσταση διαρροής εταιρικών διαπιστευτηρίων

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια υπηρεσία παρακολούθησης του dark web ειδοποιεί έναν οργανισμό ότι ένα αρχείο βάσης δεδομένων που περιέχει κωδικούς πρόσβασης εταιρικών διαχειριστών συστήματος έχει δημοσιευτεί στο διαδίκτυο.
- Προτεινόμενη στρατηγική και λύση: Ανακάλεσε όλες τις ενεργές συνεδρίες διαχειριστή και επανέφερε τα διαπιστευτήρια με γεννήτρια υψηλής εντροπίας. Επίβαλε MFA ανθεκτικό στο ηλεκτρονικό ψάρεμα στις πύλες διαχείρισης [6], άλλαξε τα επηρεασμένα κλειδιά API, εξέτασε τα αρχεία καταγραφής συνδέσεων, βρες την αρχική έκθεση και έλεγξε τους άλλους προνομιούχους λογαριασμούς.

B Μελέτη περίπτωσης 2: Εφαρμογή προτύπων κατακερματισμού κωδικών πρόσβασης

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια βάση δεδομένων μιας επιχείρησης αποθηκεύει σήμερα τους κωδικούς πρόσβασης των χρηστών με παρωχημένους κατακερματισμούς MD5 χωρίς κρυπτογραφικό salt, με αποτέλεσμα να είναι ευάλωτοι σε γρήγορη εξαγωγή.
- Προτεινόμενη στρατηγική και λύση: Υιοθέτησε τον Argon2id (ή το bcrypt σε παλαιότερα συστήματα) με μοναδικό salt ανά χρήστη [2]. Τύλιξε τώρα τα υπάρχοντα hash MD5 στον νέο αλγόριθμο, κάνε απευθείας νέο hashing στην επόμενη σύνδεση κάθε χρήστη και επέβαλε επαναφορά κωδικού σε λογαριασμούς που είναι ανενεργοί για μεγάλο διάστημα.