Nom : _____ Date : _____ Note : _____

Fuites de mots de passe et sécurité des identifiants

Credential stuffing, violations de données, algorithmes de hachage, authentification multifacteur et sécurité des mots de passe.

PRÉSENTATION DE L'APPRENTISSAGE : FUITES DE MOTS DE PASSE

SÉCURISÉ
CHIFFREMENT DES DONNÉES
Norme AES 256 bits

CONFORME
NORMES MONDIALES
Cadres RGPD (GDPR) et CCPA

ZERO TRUST
POLITIQUE D'ACCÈS
Authentification multifacteur

Bienvenue ! Ce dossier d'activités vous guide à travers les fuites de mots de passe et la sécurité des identifiants. Vous étudierez le credential stuffing, les violations de données, les algorithmes de hachage, l'authentification multifacteur et les gestionnaires de mots de passe.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la cybersécurité

URL: https://www.vpn.com/fr/cybersecurite/fuite-mots-de-passe/

Votre parcours d'apprentissage : sécurité des mots de passe

- Comprendre les risques d'exposition des identifiants sur les forums du dark web.
- Mettre en place l'authentification multifacteur (MFA) et la surveillance des identifiants compromis.
- Concevoir les défenses de sécurité de l'entreprise contre les arnaques ciblées d'ingénierie sociale.

CONSIGNES DU GUIDE SUR LES FUITES DE MOTS DE PASSE

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à la protection des identifiants. Terminez par l'activité bonus Réflexion rapide.

FUITES DE MOTS DE PASSE ET SÉCURITÉ DES IDENTIFIANTS (INTRODUCTION)

Les fuites de mots de passe exposent les identifiants des utilisateurs sur des sites publics et du dark web. Des mots de passe uniques issus d'un gestionnaire de mots de passe, la vérification des mots de passe divulgués et l'authentification multifacteur (MFA) réduisent le risque de credential stuffing, tandis qu'un hachage lent et salé des mots de passe limite les dégâts si une base de mots de passe est volée.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Qu'est-ce que le credential stuffing (bourrage d'identifiants) ?

- A. Utiliser l'automatisation pour tester des combinaisons nom d'utilisateur/mot de passe ayant fuité sur plusieurs sites
- B. Chiffrer les fichiers de stockage de la base de données locale
- C. Submerger les serveurs web de requêtes de trafic réseau
- D. Surveiller secrètement les frappes au clavier

2. Quel algorithme l'OWASP indique-t-il aujourd'hui comme premier choix pour stocker les mots de passe ?

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

3. Comment l'authentification multifacteur (MFA) atténue-t-elle le risque lié aux fuites de mots de passe ?

- A. Elle exige un facteur de vérification supplémentaire, donc un mot de passe volé ne suffit pas à lui seul
- B. Elle change automatiquement le mot de passe toutes les heures
- C. Elle chiffre le nom d'utilisateur pendant la transmission
- D. Elle signale les demandes frauduleuses au bureau de crédit

4. Qu'est-ce qu'un dump de fuite de données ?

- A. Une collection d'identifiants d'utilisateurs ayant fuité, publiée en ligne ou vendue sur des forums de pirates
- B. Une copie de sauvegarde des fichiers de base de données stockée hors site
- C. Un cache temporaire des journaux du serveur web
- D. Un outil d'administration servant à réinitialiser les mots de passe des utilisateurs

5. Quel est le rôle d'un gestionnaire de mots de passe ?

- A. Générer et conserver des mots de passe uniques et robustes pour chaque compte
- B. Surveiller le trafic réseau pour détecter les fuites de mots de passe
- C. Bloquer les attaques automatisées par force brute au niveau de la passerelle
- D. Analyser les blocs de stockage de la base de données à la recherche de mots de passe non chiffrés

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Réutiliser les mots de passe sur plusieurs comptes augmente le risque de credential stuffing (bourrage d'identifiants).

- ◯ Vrai
- ◯ Faux

7 Question 7

7. SHA-1 est une fonction de hachage recommandée pour le stockage moderne des mots de passe.

- ◯ Vrai
- ◯ Faux

8 Question 8

8. Imposer seulement la complexité des mots de passe (sans MFA) arrête complètement le bourrage d'identifiants.

- ◯ Vrai
- ◯ Faux

9 Question 9

9. Les outils de surveillance du dark web recherchent sur Internet les identifiants d'entreprise compromis.

- ◯ Vrai
- ◯ Faux

10 Question 10

10. Les hachages salés ajoutent des données aléatoires uniques aux mots de passe avant le hachage afin de déjouer les attaques par tables arc-en-ciel.

- ◯ Vrai
- ◯ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Tester des identifiants divulgués sur de nombreuses applications web s'appelle le _____ d'identifiants.

2. Un algorithme de hachage de mots de passe lent et adaptatif, toujours accepté par l'OWASP, est _____ .

3. L'exposition sur Internet de fichiers de bases de données confidentiels est une _____ de données.

4. Ajouter des valeurs aléatoires aux mots de passe avant le hachage s'appelle le _____ .

5. Une base de données locale sécurisée pour les identifiants des utilisateurs est un _____ de mots de passe.

6. Ajouter une seconde étape de vérification à la connexion relève de l'authentification _____ .

BANQUE DE MOTS DE VOCABULAIRE

BCRYPT BOURRAGE GESTIONNAIRE HAMEÇONNAGE MULTIFACTEUR SALAGE TABLE ARC-EN-CIEL VIOLATION

Écrivez vos réponses ici :

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

Point de contrôle 4 : Association de notions sur la sécurité

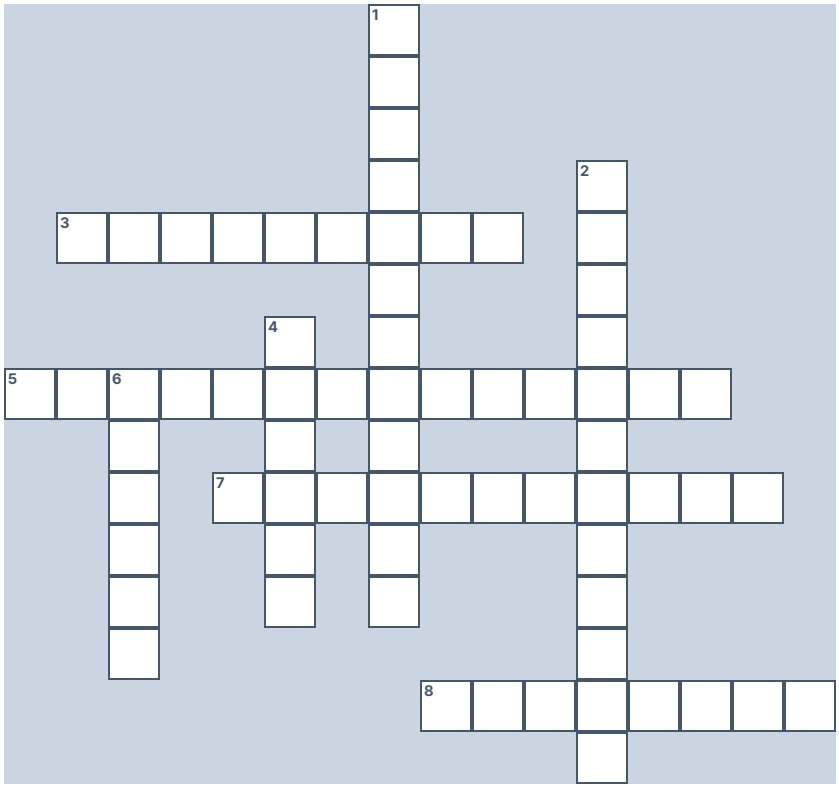
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. BOURRAGE D'IDENTIFIANTS	A	Table précalculée d'empreintes (hashes) de mots de passe.
☐	2. BCRYPT	B	Vérification de connexion multifacteur.
☐	3. VIOLATION DE DONNÉES	C	Outil de stockage des identifiants.
☐	4. SALAGE	D	Exposition non autorisée d'une base de données.
☐	5. GESTIONNAIRE	E	Ingénierie sociale visant à voler des identifiants.
☐	6. MFA	F	Tester des identifiants divulgués.
☐	7. ARC-EN-CIEL	G	Ajout d'un sel aléatoire à l'empreinte du mot de passe.
☐	8. HAMEÇONNAGE	H	Algorithme de hachage de mots de passe lent.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

3. Exposition non autorisée d'une base de données. (9)

5. Table précalculée d'empreintes de mots de passe. (14)

7. Ingénierie sociale visant à voler des identifiants de connexion. (11)

8. Test d'identifiants divulgués. (8)

VERTICALEMENT

1. Contrôle de connexion à plusieurs facteurs (MFA). (12)

2. Outil de stockage des identifiants. (12)

4. Ajout d'un sel aléatoire au hachage d'un mot de passe. (6)

6. Algorithme lent de hachage de mots de passe. (6)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

3 horizontal: Exposition non autorisée d'une base de données. (9 lettres):

5 horizontal: Table précalculée d'empreintes de mots de passe. (14 lettres):

7 horizontal: Ingénierie sociale visant à voler des identifiants de connexion. (11 lettres):

8 horizontal: Test d'identifiants divulgués. (8 lettres):

VERTICALEMENT

1 vertical: Contrôle de connexion à plusieurs facteurs (MFA). (12 lettres):

2 vertical: Outil de stockage des identifiants. (12 lettres):

4 vertical: Ajout d'un sel aléatoire au hachage d'un mot de passe. (6 lettres):

6 vertical: Algorithme lent de hachage de mots de passe. (6 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

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

LISTE DE MOTS DE VOCABULAIRE

BOURRAGE BCRYPT VIOLATION SALAGE GESTIONNAIRE MULTIFACTEUR TABLEARCENCIEL HAMECONNAGE

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. BOURRAGE
B. BCRYPT
C. VIOLATION
D. SALAGE
E. GESTIONNAIRE
F. MULTIFACTEUR
G. TABLEARCENCIEL
H. HAMECONNAGE

	DÉFINITIONS ET CHAMPS D'ASSOCIATION
	1. Ingénierie sociale visant à voler des identifiants de connexion.
	2. Exposition non autorisée d'une base de données.
	3. Algorithme lent de hachage de mots de passe.
	4. Table précalculée d'empreintes de mots de passe.
	5. Test d'identifiants divulgués.
	6. Ajout d'un sel aléatoire au hachage d'un mot de passe.
	7. Outil de stockage des identifiants.
	8. Contrôle de connexion à plusieurs facteurs (MFA).

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. GRRBAOEU
2. NVOLITIAO
3. GENNRASOEIIT
4. ARENLEALCICTBE
5. YRTBPC
6. GASLEA
7. CTIMUAREULFT
8. ANEOMHCAGNE

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Bonnes habitudes de sécurité à adopter dès aujourd'hui			
2	Règles pour un mot de passe robuste			
3	Gestionnaires de mots de passe que vous connaissez			
4	Outils de sécurité que vous connaissez			
5	Signaux d'alerte dans un e-mail			
6	Mots amusants pour une longue phrase de passe			
7	Façons de se connecter sans mot de passe			
8	Informations que vous ne devriez jamais partager			
9	Raisons de mettre à jour les logiciels			
10	Choses à faire quand un mot de passe a fuité			
11	Comptes qui nécessitent la MFA			
12	Endroits où les mots de passe ne devraient jamais être stockés			
13	Signes qu'un ordinateur est infecté			
14	Mauvais mots de passe que les gens utilisent			
15	Choses que vous sauvegardez			

Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : REMÉDIATION D'UNE FUITE D'IDENTIFIANTS EN ENTREPRISE

👷

Scénario : Un service de surveillance du dark web avertit une organisation qu'un dump de base de données contenant les mots de passe des administrateurs système de l'entreprise a été publié en ligne.

Question de discussion : Analysez les risques liés à la fuite d'identifiants et proposez une stratégie de réinitialisation administrative.

ÉTUDE DE CAS 2 : APPLIQUER DES NORMES DE HACHAGE DES MOTS DE PASSE

👷

Scénario : La base de données d'une entreprise stocke actuellement les mots de passe des utilisateurs sous forme de hachages MD5 obsolètes, sans sel cryptographique, ce qui les rend vulnérables à une extraction rapide.

Question de discussion : Concevez une stratégie de migration pour mettre à niveau l'algorithme de hachage de la base de données.

Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

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

16 18 15 20 5 7 5 26 12 5 19 13 15 20 19 4 5

16 1 19 19 5 6 21 9 20 5 19 16 1 18 12 1

13 6 1

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q1: Qu'est-ce qu'une fuite de mot de passe ?

Une fuite de mots de passe se produit lorsque les identifiants de connexion des utilisateurs sont exposés à la suite de violations de données ou de mauvaises configurations de serveurs.

Q2: Comment les pirates trouvent-ils les mots de passe divulgués ?

Les pirates fouillent les forums du dark web, les vidages publics de bases de données et les sites de type « paste » où sont publiées les données issues de violations [8].

Q3: Réutiliser un mot de passe est-il dangereux ?

Oui, car si un site est compromis, les pirates peuvent tester les mêmes identifiants sur des milliers d'autres plateformes [3].

Q4: Qu'est-ce qu'un sel cryptographique ?

Un sel est une donnée aléatoire ajoutée à un mot de passe avant le hachage, ce qui rend inefficaces les attaques par tables précalculées [2].

Q5: Pourquoi MD5 est-il obsolète ?

MD5 est une fonction de hachage généraliste rapide et obsolète : les attaquants peuvent donc tester des mots de passe extrêmement vite, surtout lorsque les hachages ne sont pas salés [2].

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q6: Comment un gestionnaire de mots de passe protège-t-il les utilisateurs ?

Il génère automatiquement des identifiants complexes et uniques pour chaque site, ce qui réduit les erreurs de mémoire et la réutilisation.

Q7: Qu'est-ce qu'une attaque par force brute ?

Une attaque qui teste systématiquement toutes les combinaisons de caractères possibles jusqu'à trouver le bon mot de passe [4].

Q8: En quoi le verrouillage de compte est-il utile ?

Le verrouillage de compte ou la limitation du débit ralentit les tentatives répétées de devinette en ligne et, combiné à la surveillance et à la MFA, réduit le risque d'attaque par force brute [4].

Q9: Les mots de passe maîtres sont-ils sûrs ?

Elles sont sûres s'il s'agit de phrases de passe à forte entropie qui ne sont jamais réutilisées sur d'autres systèmes web.

Q10: Faut-il changer régulièrement ses mots de passe ?

Le NIST recommande de ne pas imposer de changements périodiques : il faut les changer en cas de preuve de compromission et privilégier la longueur, les listes de blocage et la MFA [1].

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q1: Comment Argon2 se compare-t-il à bcrypt ?

L'OWASP place Argon2id en premier choix ; ses paramètres gourmands en mémoire résistent mieux que bcrypt au cassage par GPU et ASIC [2].

Q2: Qu'est-ce que l'étirement de clé (key stretching) ?

Une technique qui répète un algorithme de hachage des milliers de fois pour ralentir la vérification des mots de passe, ce qui rend leur craquage coûteux [2].

Q3: Comment fonctionnent les tables arc-en-ciel ?

Ce sont des tables de correspondance précalculées qui associent des mots de passe en clair à leurs hachages, utilisées pour inverser rapidement des hachages sans sel [2].

Q4: Qu'est-ce que le recyclage d'identifiants ?

Réutilisation de paires nom d'utilisateur/mot de passe volées lors d'une fuite pour tenter d'accéder à d'autres services, en particulier lorsque des personnes ont réutilisé leurs mots de passe [3].

Q5: Les gestionnaires de mots de passe peuvent-ils être piratés ?

Oui. Beaucoup utilisent un chiffrement à connaissance nulle, de sorte qu'une violation du serveur n'expose que des coffres chiffrés, mais des mots de passe maîtres faibles peuvent quand même être craqués hors ligne.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q6: Qu'est-ce qu'une attaque par dictionnaire ?

Une variante de la force brute qui teste des mots courants, des phrases et des mots de passe ayant déjà fuité plutôt que des lettres aléatoires.

Q7: Pourquoi les phrases de passe sont-elles préférées ?

Les phrases de passe utilisent plusieurs mots aléatoires, ce qui crée une forte entropie, facile à mémoriser pour un humain mais coûteuse à casser par calcul [1].

Q8: Quel est l'effet de l'authentification unique (SSO) sur les fuites de mots de passe ?

Le SSO réduit la multiplication des mots de passe, mais le fournisseur d'identité devient une cible de grande valeur qui nécessite une MFA forte, de préférence résistante à l'hameçonnage [6].

Q9: Qu'est-ce que le détournement de session ?

Un attaquant obtient ou détourne un jeton de session valide pour se faire passer pour un utilisateur connecté sans avoir à fournir à nouveau le mot de passe [5].

Q10: Comment détecter une attaque par pulvérisation de mots de passe (password spraying) ?

En repérant les quelques mêmes mots de passe essayés sur de nombreux comptes, souvent lentement pour rester sous les seuils de verrouillage [7].

Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

1. APERÇU SÉCURITÉ

La norme NIST SP 800-63B exige que les nouveaux mots de passe soient comparés à des listes de blocage de mots de passe courants et compromis [1].

2. APERÇU SÉCURITÉ

La fuite 'Collection #1' de 2019 a regroupé les données de nombreuses fuites antérieures en un énorme fichier de paires adresse e-mail/mot de passe [8].

3. APERÇU SÉCURITÉ

Le NIST exige désormais que les mots de passe utilisés comme unique facteur d'authentification comptent au moins 15 caractères [1].

4. APERÇU SÉCURITÉ

Le matériel ASIC peut calculer des milliards d'empreintes SHA-256 par seconde, ce qui rend le simple hachage SHA dangereux pour les mots de passe des utilisateurs [2].

5. APERÇU SÉCURITÉ

Des sels uniques font que deux utilisateurs ayant exactement le même mot de passe obtiennent des hachages différents dans la base de données [2].

6. APERÇU SÉCURITÉ

De nombreux gestionnaires de mots de passe chiffrent localement les données du coffre avec une cryptographie robuste dérivée du mot de passe principal de l'utilisateur.

7. ZOOM SUR LA SÉCURITÉ

Le credential stuffing fonctionne parce que beaucoup de gens réutilisent le même mot de passe pour leurs comptes de sites marchands, de banque et de messagerie [3].

8. ZOOM SUR LA SÉCURITÉ

La norme NIST SP 800-63B indique que les vérificateurs ne doivent pas exiger de changements périodiques de mot de passe, mais seulement des changements en cas de preuve de compromission [1].

9. ZOOM SUR LA SÉCURITÉ

Ajouter une seule majuscule et un symbole à un mot de passe court n'arrête pas les attaques par dictionnaire automatisées modernes menées sur GPU [1].

10. APERÇU SÉCURITÉ

La MFA peut bloquer de nombreuses tentatives de bourrage d'identifiants (credential stuffing), même après la fuite d'un mot de passe ; une MFA résistante à l'hameçonnage est plus robuste que les codes SMS [3].

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[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/

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Le bourrage d'identifiants (credential stuffing) utilise l'automatisation pour essayer des paires nom d'utilisateur/mot de passe divulguées sur d'autres sites [3].

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

L'OWASP recommande Argon2id en premier ; bcrypt est surtout destiné aux anciens systèmes où Argon2id ou scrypt ne sont pas disponibles [2].

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

La MFA exige un facteur supplémentaire : un mot de passe volé ne peut donc pas à lui seul déverrouiller le compte [3].

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

Les dumps de violations sont des collections d'identifiants divulgués, comme la compilation de 2019 « Collection #1 » [8].

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Un gestionnaire de mots de passe génère et stocke un mot de passe unique et robuste pour chaque compte, ce qui évite la réutilisation [3].

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Vrai : les mots de passe réutilisés permettent aux attaquants de rejouer sur d'autres sites des identifiants divulgués par un site [3].

7 Question 7

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : SHA-1 est un hachage rapide ; l'OWASP recommande plutôt Argon2id, scrypt, bcrypt ou PBKDF2 [2].

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : les règles de complexité seules ne peuvent pas arrêter le bourrage avec des mots de passe divulgués réutilisés ; la MFA est nécessaire [3].

9 Question 9

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Vrai : les services de surveillance fouillent les dumps de violations et les sources du dark web à la recherche d'identifiants exposés [8].

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Vrai : un sel unique par mot de passe rend inefficaces les tables arc-en-ciel précalculées [2].

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

F 1. BOURRAGE D'IDENTIFIANTS	H 2. BCRYPT	D 3. VIOLATION DE DONNÉES	G 4. SALAGE
C 5. GESTIONNAIRE	B 6. MFA	A 7. ARC-EN-CIEL	E 8. HAMEÇONNAGE

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 BOURRAGE	2 BCRYPT	3 VIOLATION	4 SALAGE
5 GESTIONNAIRE	6 MULTIFACTEUR		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 H – HAMECONNAGE	2 C – VIOLATION	3 B – BCRYPT	4 G – TABLEARCENCIEL
5 A – BOURRAGE	6 D – SALAGE	7 E – GESTIONNAIRE	8 F – MULTIFACTEUR

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer BOURRAGE D'IDENTIFIANTS, BCRYPT et VIOLATION DE DONNÉES avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

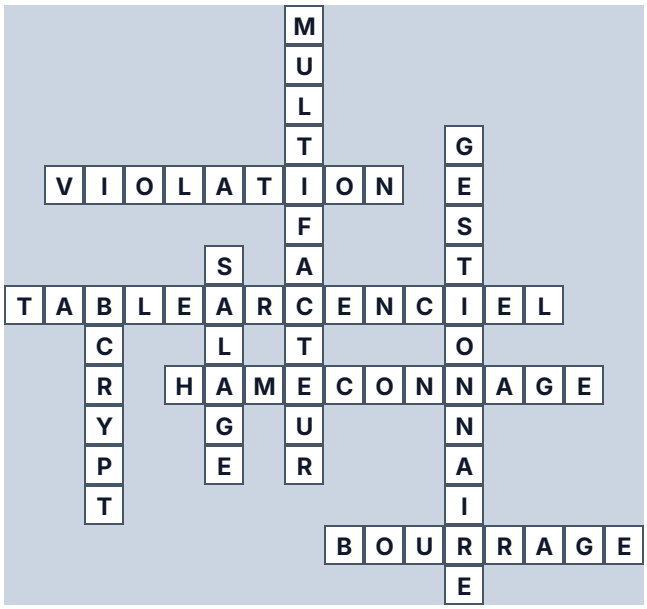
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

3 horizontal: VIOLATION Exposition non autorisée d'une base de données. (9 lettres)

5 horizontal: TABLEARCENCIEL Table précalculée d'empreintes de mots de passe. (14 lettres)

7 horizontal: HAMECONNAGE Ingénierie sociale visant à voler des identifiants de connexion. (11 lettres)

8 horizontal: BOURRAGE Test d'identifiants divulgués. (8 lettres)

VERTICALEMENT

1 vertical: MULTIFACTEUR Contrôle de connexion à plusieurs facteurs (MFA). (12 lettres)

2 vertical: GESTIONNAIRE Outil de stockage des identifiants. (12 lettres)

4 vertical: SALAGE Ajout d'un sel aléatoire au hachage d'un mot de passe. (6 lettres)

6 vertical: BCRYPT Algorithme lent de hachage de mots de passe. (6 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. GRRBAOEU — **BOURRAGE**
2. NVOLITIAO — **VIOLATION**
3. GENNRASOEIIT — **GESTIONNAIRE**
4. ARENLEALCICTBE — **TABLEARCENCIEL**
5. YRTBPC — **BCRYPT**
6. GASLEA — **SALAGE**
7. CTIMUAREULFT — **MULTIFACTEUR**
8. ANEOMHCAGNE — **HAMECONNAGE**

CORRIGÉ DU DÉFI DU CODE SECRET

"PROTEGEZ LES MOTS DE PASSE FUITES PAR LA MFA"

Corrigé des études de cas

A Étude de cas 1 : Remédiation d'une fuite d'identifiants en entreprise

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un service de surveillance du dark web avertit une organisation qu'un vidage de base de données contenant les mots de passe des administrateurs système de l'entreprise a été publié en ligne.
- Stratégie et solution recommandées : révoquez toutes les sessions administrateur actives et réinitialisez les identifiants avec un générateur à haute entropie. Imposez une MFA résistante à l'hameçonnage sur les portails d'administration [6], renouvelez les clés API concernées, examinez les journaux de connexion, trouvez l'exposition initiale et vérifiez les autres comptes à privilèges.

B Étude de cas 2 : Appliquer des normes de hachage des mots de passe

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : la base de données d'une entreprise stocke actuellement les mots de passe des utilisateurs sous forme de hachages MD5 obsolètes sans sel cryptographique, ce qui les rend vulnérables à une extraction rapide.
- Stratégie et solution recommandées : adopter Argon2id (ou bcrypt sur les systèmes anciens) avec un sel unique par utilisateur [2]. Envelopper dès maintenant les hachages MD5 existants dans le nouvel algorithme, refaire directement le hachage à la prochaine connexion de chaque utilisateur et imposer une réinitialisation pour les comptes inactifs depuis longtemps.