Imię i nazwisko: _____ Data: _____ Wynik: _____

Wycieki haseł i bezpieczeństwo danych logowania

Credential stuffing, naruszenia danych, algorytmy skrótu, uwierzytelnianie wieloskładnikowe i bezpieczeństwo haseł.

PRZEGLĄD NAUKI: WYCIEKI HASEŁ

CHRONIONY
SZYFROWANIE DANYCH
Standard AES 256-bitowy

ZGODNY
STANDARDY GLOBALNE
Ramy prawne RODO (GDPR) i CCPA

ZERO TRUST
POLITYKA DOSTĘPU
Uwierzytelnianie wieloskładnikowe

Witaj! Ten pakiet ćwiczeń przeprowadzi cię przez wycieki haseł i bezpieczeństwo poświadczeń. Poznasz credential stuffing, wycieki danych, algorytmy mieszające (hashing), uwierzytelnianie wieloskładnikowe i menedżery haseł.

PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj cyberbezpieczeństwo i zapobieganie zagrożeniom.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

Otwórz przewodnik VPN.com po cyberbezpieczeństwie

URL: https://www.vpn.com/pl/cyberbezpieczenstwo/wyciek-hasel/

Twoja ścieżka nauki: bezpieczeństwo haseł

- Zrozum ryzyko ujawnienia danych logowania na forach dark webu.
- Wdróż uwierzytelnianie wieloskładnikowe (MFA) i monitorowanie przejętych danych logowania.
- Zaprojektuj firmowe zabezpieczenia przed ukierunkowanymi oszustwami opartymi na inżynierii społecznej.

INSTRUKCJE DO PRZEWODNIKA O WYCIEKACH HASEŁ

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu ochrony danych uwierzytelniających. Zakończ zadaniem dodatkowym Myśl szybko.

WYCIEKI HASEŁ I BEZPIECZEŃSTWO DANYCH LOGOWANIA (WPROWADZENIE)

Wycieki haseł ujawniają dane logowania użytkowników w publicznych witrynach i w darknecie. Unikalne hasła z menedżera haseł, sprawdzanie pod kątem ujawnionych haseł i uwierzytelnianie wieloskładnikowe (MFA) zmniejszają ryzyko credential stuffingu, a solone, powolne haszowanie haseł ogranicza szkody w razie kradzieży bazy haseł.

PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ ODPOWIEDŹ.

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Czym jest credential stuffing?

- A. Wykorzystywanie automatyzacji do testowania wyciekłych kombinacji nazwy użytkownika i hasła na wielu stronach
- B. Szyfrowanie lokalnych plików magazynu bazy danych
- C. Przeciążanie serwerów WWW żądaniami ruchu sieciowego
- D. Potajemne monitorowanie danych wprowadzanych z klawiatury

2. Który algorytm OWASP wymienia dziś jako pierwszy wybór do przechowywania haseł?

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

3. W jaki sposób uwierzytelnianie wieloskładnikowe (MFA) zmniejsza ryzyko wycieku haseł?

- A. Wymaga dodatkowego składnika weryfikacji, więc samo skradzione hasło nie wystarcza
- B. Automatycznie zmienia hasło co godzinę
- C. Szyfruje nazwę użytkownika podczas przesyłania
- D. Powiadamia biuro informacji kredytowej o oszukańczych żądaniach

4. Czym jest zrzut danych z wycieku (data breach dump)?

- A. Zbiór wyciekłych danych uwierzytelniających użytkowników opublikowany w internecie lub sprzedawany na forach hakerskich
- B. Kopia zapasowa plików bazy danych przechowywana poza siedzibą
- C. Tymczasowa pamięć podręczna dzienników serwera WWW
- D. Narzędzie administracyjne do resetowania haseł użytkowników

5. Jaką rolę pełni menedżer haseł?

- A. Generowanie i przechowywanie unikalnych, silnych haseł do każdego konta
- B. Monitorowanie ruchu sieciowego pod kątem wycieków haseł
- C. Blokowanie zautomatyzowanych ataków brute-force na bramie
- D. Skanowanie bloków pamięci bazy danych w poszukiwaniu nieszyfrowanych haseł

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Ponowne używanie haseł na wielu kontach zwiększa ryzyko ataku credential stuffing.

Prawda Fałsz

7 Pytanie 7

7. SHA-1 jest zalecaną funkcją skrótu do nowoczesnego przechowywania haseł.

Prawda Fałsz

8 Pytanie 8

8. Samo wymuszanie złożoności haseł (bez MFA) całkowicie zatrzymuje credential stuffing.

Prawda Fałsz

9 Pytanie 9

9. Narzędzia do monitorowania ciemnej sieci skanują internet w poszukiwaniu przejętych firmowych danych uwierzytelniających.

Prawda Fałsz

10 Pytanie 10

10. Solone skróty dodają do haseł unikalne losowe dane przed haszowaniem, aby udaremnić ataki z użyciem tęczowych tablic.

Prawda Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Testowanie wyciekniętych poświadczeń w wielu aplikacjach internetowych nazywa się credential _____ .

2. Powolnym, adaptacyjnym algorytmem haszowania haseł, nadal akceptowanym przez OWASP, jest _____ .

3. Ujawnienie poufnych plików baz danych w internecie to _____ danych.

4. Dodawanie losowych wartości do haseł przed haszowaniem nazywa się _____ .

5. Bezpieczną lokalną bazą danych na poświadczenia użytkowników jest _____ haseł.

6. Dodanie drugiego etapu weryfikacji logowania wykorzystuje _____ .

BANK SŁÓW

BCRYPT MENEDŻER MFA NARUSZENIE PHISHING SOLENIE STUFFING TĘCZOWA TABLICA

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

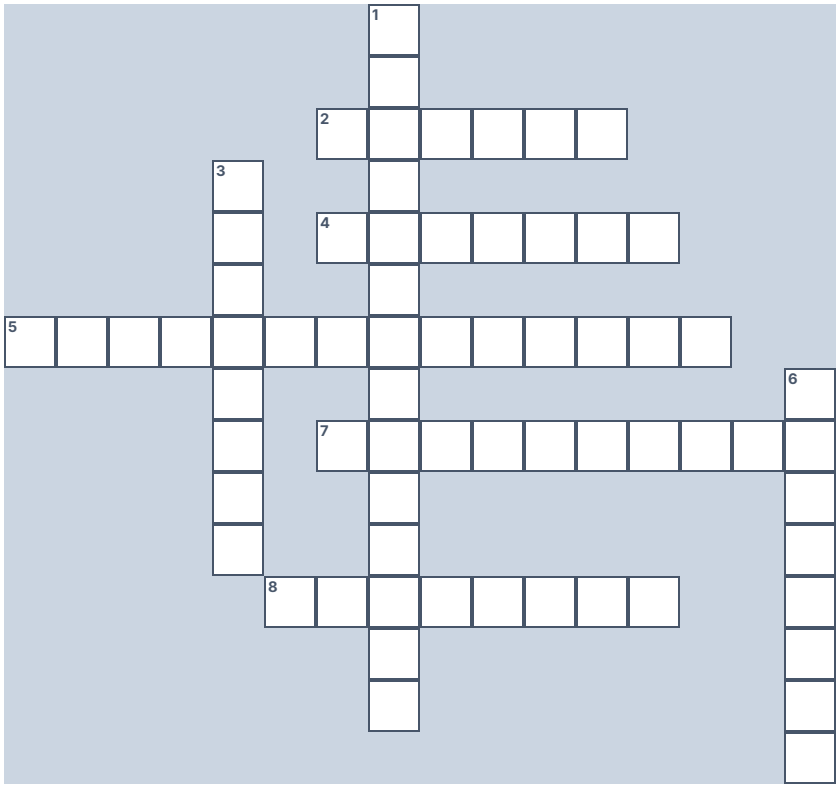
DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

☐	1. STUFFING	A	Wstępnie obliczona tabela skrótów haseł.
☐	2. BCRYPT	B	Wieloskładnikowa kontrola logowania.
☐	3. NARUSZENIE	C	Narzędzie do przechowywania poświadczeń.
☐	4. SOLENIE	D	Nieautoryzowane ujawnienie bazy danych.
☐	5. MENEDŻER	E	Socjotechnika w celu kradzieży danych logowania.
☐	6. MFA	F	Testowanie wyciekłych danych logowania.
☐	7. TĘCZOWE	G	Dodawanie losowej soli do skrótu hasła.
☐	8. PHISHING	H	Powolny algorytm haszowania haseł.

Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.



POZIOMO

2. Powolny algorytm haszowania haseł. (6)

4. Dodawanie losowej soli do skrótu hasła. (7)

5. Wieloskładnikowa kontrola logowania. (14)

7. Nieautoryzowane ujawnienie bazy danych. (10)

8. Socjotechnika służąca do wykradania danych logowania. (8)

PIONOWO

1. Wstępnie obliczona tablica skrótów haseł. (14)

3. Testowanie wyciekniętych poświadczeń. (8)

6. Narzędzie do przechowywania poświadczeń. (8)

Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej.

POZIOMO

2 poziomo: Powolny algorytm haszowania haseł. (6 liter):

4 poziomo: Dodawanie losowej soli do skrótu hasła. (7 liter):

5 poziomo: Wieloskładnikowa kontrola logowania. (14 liter):

7 poziomo: Nieautoryzowane ujawnienie bazy danych. (10 liter):

8 poziomo: Socjotechnika służąca do wykradania danych logowania. (8 liter):

PIONOWO

1 pionowo: Wstępnie obliczona tablica skrótów haseł. (14 liter):

3 pionowo: Testowanie wyciekniętych poświadczeń. (8 liter):

6 pionowo: Narzędzie do przechowywania poświadczeń. (8 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

T Ę C Z O W A T A B L I C A G
M Ż G K R E Ż D E N E M O P S
Ń X C M Ż Ź F Z O X U L V O Ó
B Ń W T M G V Ć Z V L R L Ą Y
Ż E I N E Z S U R A N E Z M S
Q Y I Ó D A Ć K Q W N X X L J
H T H F Ą E I L Ś I S W Q Ź E
H E S C A Ł P C E Ż M L W S U
Ą S X K M M G H N H R Ę L Ś Ł
T R X H G N I H S I H P B U Ę
P W E R Y F I K A C J A M F A
Y Z O Ź X S G T Y A Ó V Ń Ń Ź
R O S T U F F I N G H P T H Ó
C V U O U T K A E Ó N L Ą Ń V
B F F P Q Y Ź J K V K Ź X Z Ó

LISTA SŁÓW

STUFFING BCRYPT NARUSZENIE SOLENIE MENEDŻER WERYFIKACJAMFA TĘCZOWATABLICA PHISHING

Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

TERMINY ZE SŁOWNICZKA

- **A. STUFFING**
- **B. BCRYPT**
- **C. NARUSZENIE**
- **D. SOLENIE**
- **E. MENEDŻER**
- **F. WERYFIKACJAMFA**
- **G. TĘCZOWATABLICA**
- **H. PHISHING**

DEFINICJE I POLA DOPASOWANIA

1. Socjotechnika służąca do wykradania danych logowania. ____
2. Nieautoryzowane ujawnienie bazy danych. ____
3. Powolny algorytm haszowania haseł. ____
4. Wstępnie obliczona tablica skrótów haseł. ____
5. Testowanie wyciekniętych poświadczeń. ____
6. Dodawanie losowej soli do skrótu hasła. ____
7. Narzędzie do przechowywania poświadczeń. ____
8. Wieloskładnikowa kontrola logowania. ____

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z cyberbezpieczeństwem. Wpisz odpowiedzi w przygotowanych polach.

1. NFFSITGU
2. IUNASEENZR
3. EEMDŻREN
4. ĘACBZAWATI LTCO
5. YRTBPC
6. ILNSEEO
7. AFJWCERAIM AYKF
8. SHHGPNII

Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

1	Bezpieczne nawyki, które możesz zacząć już dziś			
2	Zasady silnego hasła			
3	Menedżery haseł, które znasz			
4	Narzędzia bezpieczeństwa, które znasz			
5	Sygnały ostrzegawcze w e-mailu			
6	Zabawne słowa do długiej frazy hasła			
7	Sposoby na logowanie bez hasła			
8	Informacje, których nigdy nie powinieneś udostępniać			
9	Powody, dla których warto aktualizować oprogramowanie			
10	Rzeczy do zrobienia, gdy hasło wycieknie			
11	Konta, które wymagają MFA			
12	Miejsca, w których hasła nigdy nie powinny być przechowywane			
13	Oznaki, że komputer jest zainfekowany			
14	Złe hasła, których używają ludzie			
15	Rzeczy, z których robisz kopie zapasowe			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

STUDIUM PRZYPADKU 1: NAPRAWA WYCIEKU POŚWIADCZEŃ W FIRMIE

👷

Scenariusz: Usługa monitorowania dark webu powiadamia organizację, że w internecie opublikowano zrzut bazy danych zawierający hasła firmowych administratorów systemów.

Pytanie do dyskusji: Przeanalizuj ryzyka wycieku danych uwierzytelniających i zaproponuj administracyjną strategię resetowania.

STUDIUM PRZYPADKU 2: WDRAŻANIE STANDARDÓW HASZOWANIA HASEŁ

👷

Scenariusz: Firmowa baza danych przechowuje obecnie hasła użytkowników przy użyciu przestarzałych skrótów MD5 bez soli kryptograficznej, co czyni je podatnymi na szybkie wydobycie.

Pytanie do dyskusji: Zaprojektuj strategię migracji, aby zaktualizować algorytm haszowania bazy danych.

Punkt kontrolny 9: Odszyfruj szyfr

Specjalista ds. cyberbezpieczeństwa chroni zasoby sieciowe przed cyberprzestępcami. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

KLUCZ SZYFROWANIA LITERA-LICZBA

A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12
J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24
S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35

33	1	3	7	33	22	12	7	4	33		30	32	4	12	7	14	16	7

11	1	25	16	1		22	24	33	7	33		17	9	1

Odszyfrowana wiadomość:

WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część A)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q1: Czym jest wyciek hasła?

Wyciek hasła występuje, gdy dane logowania użytkowników zostają ujawnione w wyniku naruszeń danych lub błędnych konfiguracji serwerów.

Q2: Jak hakerzy znajdują wycieki haseł?

Hakerzy przeszukują fora w dark webie, publiczne zrzuty baz danych i serwisy typu paste, w których publikowane są dane z wycieków [8].

Q3: Czy ponowne używanie haseł jest niebezpieczne?

Tak, ponieważ jeśli jedna witryna zostanie naruszona, hakerzy mogą wypróbować te same dane logowania na tysiącach innych platform [3].

Q4: Czym jest sól kryptograficzna (salt)?

Sól to losowe dane dodawane do hasła przed haszowaniem, co sprawia, że ataki z użyciem wstępnie obliczonych tablic są nieskuteczne [2].

Q5: Dlaczego MD5 jest przestarzały?

MD5 to szybka, przestarzała funkcja skrótu ogólnego przeznaczenia, więc atakujący mogą testować zgadywane hasła bardzo szybko, zwłaszcza gdy skróty nie są solone [2].

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część B)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Jak menedżer haseł chroni użytkowników?

Automatycznie generuje złożone, unikalne dane logowania dla każdej strony, zmniejszając błędy pamięciowe i ponowne używanie haseł.

Q7: Czym jest atak siłowy (brute force)?

Atak, który systematycznie testuje każdą możliwą kombinację znaków, aż zostanie znalezione prawidłowe hasło [4].

Q8: Jak pomaga blokada konta po nieudanych próbach logowania?

Blokada konta lub ograniczanie liczby prób spowalnia wielokrotne zgadywanie online i w połączeniu z monitorowaniem oraz MFA zmniejsza ryzyko ataku siłowego [4].

Q9: Czy hasła główne są bezpieczne?

Są bezpieczne, jeśli są frazami hasłowymi o wysokiej entropii, które nigdy nie są używane ponownie w innych systemach internetowych.

Q10: Czy hasła powinno się zmieniać regularnie?

NIST zaleca, aby nie wymuszać okresowych zmian; zmieniaj hasła po wykryciu oznak naruszenia i stawiaj na długość, listy blokad i MFA [1].

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część C)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q1: Jak Argon2 wypada w porównaniu z bcrypt?

OWASP wymienia Argon2id jako pierwszy wybór; jego ustawienia wymagające dużej ilości pamięci lepiej niż bcrypt opierają się łamaniu z użyciem GPU i ASIC [2].

Q2: Czym jest rozciąganie klucza (key stretching)?

Technika, która zapętla algorytm haszujący tysiące razy, aby spowolnić proces weryfikacji hasła, przez co łamanie staje się kosztowne [2].

Q3: Jak działają tęczowe tablice (rainbow tables)?

To wstępnie obliczone tablice wyszukiwania łączące hasła jawnym tekstem z ich skrótami, służące do szybkiego odwracania skrótów bez soli [2].

Q4: Czym jest recykling danych uwierzytelniających?

Wykorzystywanie skradzionych par nazwa użytkownika/hasło z jednego naruszenia do prób dostępu do innych usług, zwłaszcza tam, gdzie ludzie używali tych samych haseł [3].

Q5: Czy menedżery haseł mogą zostać zhakowane?

Tak. Wiele z nich używa szyfrowania zero-knowledge, więc włamanie na serwer ujawnia tylko zaszyfrowane sejfy, ale słabe hasła główne nadal można złamać offline.

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część D)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q6: Czym jest atak słownikowy?

Odmiana ataku brute-force, która testuje popularne słowa, frazy i historyczne wyciekłe hasła zamiast losowych liter.

Q7: Dlaczego preferuje się frazy hasłowe (passphrases)?

Frazy hasłowe składają się z kilku losowych słów, co tworzy wysoką entropię, którą ludzie łatwo zapamiętują, ale której złamanie jest kosztowne obliczeniowo [1].

Q8: Jak jednokrotne logowanie (SSO) wpływa na wycieki haseł?

SSO zmniejsza rozrost haseł, ale dostawca tożsamości staje się celem o wysokiej wartości, który wymaga silnego, najlepiej odpornego na phishing MFA [6].

Q9: Czym jest przejęcie sesji (session hijacking)?

Atakujący zdobywa lub nadużywa prawidłowego tokena sesji, aby podszyć się pod zalogowanego użytkownika bez ponownej potrzeby podawania hasła [5].

Q10: Jak wykryć password spraying?

Przez wyszukiwanie tych samych kilku haseł wypróbowywanych na wielu kontach, często powoli, aby nie przekroczyć progów blokady [7].

Część 11: 10 faktów o cyberbezpieczeństwie z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące naruszeń bezpieczeństwa, mechanizmów obronnych i standardów zgodności.

1. WGLĄD W BEZPIECZEŃSTWO

NIST SP 800-63B wymaga, aby nowe hasła były sprawdzane z listami blokad popularnych i skompromitowanych haseł [1].

2. WGLĄD W BEZPIECZEŃSTWO

Zrzut „Collection #1" z 2019 roku połączył dane z wielu wcześniejszych naruszeń w jeden ogromny plik z parami e-mail i hasło [8].

3. WGLĄD W BEZPIECZEŃSTWO

NIST wymaga obecnie, aby hasła używane jako jedyny czynnik uwierzytelniania miały co najmniej 15 znaków [1].

4. WGLĄD W BEZPIECZEŃSTWO

Sprzęt ASIC może obliczać miliardy skrótów SHA-256 na sekundę, przez co surowe haszowanie SHA jest niebezpieczne dla haseł użytkowników [2].

5. WGLĄD W BEZPIECZEŃSTWO

Unikalna sól oznacza, że dwóch użytkowników z dokładnie takim samym hasłem otrzymuje różne skróty w bazie danych [2].

6. WGLĄD W BEZPIECZEŃSTWO

Wiele menedżerów haseł szyfruje dane sejfu lokalnie przy użyciu silnej kryptografii opartej na haśle głównym użytkownika.

7. WGLĄD W BEZPIECZEŃSTWO

Credential stuffing działa, ponieważ wiele osób używa tego samego hasła na kontach w sklepach internetowych, bankach i poczty e-mail [3].

8. WGLĄD W BEZPIECZEŃSTWO

NIST SP 800-63B stanowi, że weryfikatorzy nie mogą wymagać okresowej zmiany haseł, a jedynie zmiany po wykryciu oznak naruszenia [1].

9. WGLĄD W BEZPIECZEŃSTWO

Dodanie jednej wielkiej litery i symbolu do krótkiego hasła nie powstrzymuje nowoczesnych zautomatyzowanych ataków słownikowych z użyciem GPU [1].

10. WGLĄD W BEZPIECZEŃSTWO

MFA może zablokować wiele prób credential stuffingu nawet po wycieku hasła; MFA odporne na phishing jest silniejsze niż kody SMS [3].

Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów NIST, OWASP i zgodności z przepisami o ochronie prywatności danych.

PUBLIKACJE NAUKOWE I BRANŻOWE

[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/

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Credential stuffing wykorzystuje automatyzację do wypróbowywania wyciekłych par nazwa użytkownika/hasło w innych witrynach [3].

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

OWASP zaleca najpierw Argon2id; bcrypt jest przeznaczony głównie dla starszych systemów, w których Argon2id lub scrypt są niedostępne [2].

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

MFA wymaga dodatkowego składnika, więc samo skradzione hasło nie może odblokować konta [3].

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Zrzuty wycieków (breach dumps) to zbiory wyciekłych danych uwierzytelniających, takie jak kompilacja z 2019 roku, Collection #1 [8].

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Menedżer haseł generuje i przechowuje unikalne, silne hasło do każdego konta, zapobiegając ich ponownemu użyciu [3].

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 Pytanie 6

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Prawda: ponownie używane hasła pozwalają atakującym odtwarzać dane uwierzytelniające wyciekłe z jednej witryny w innych witrynach [3].

7 Pytanie 7

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: SHA-1 to szybka funkcja skrótu; OWASP zaleca zamiast niej Argon2id, scrypt, bcrypt lub PBKDF2 [2].

8 Pytanie 8

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: same reguły złożoności nie powstrzymają ataku credential stuffing z użyciem ponownie używanych wyciekłych haseł; potrzebne jest MFA [3].

9 Pytanie 9

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Prawda: usługi monitorujące przeszukują zrzuty wycieków i źródła z dark webu pod kątem ujawnionych danych uwierzytelniających [8].

10 Pytanie 10

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Prawda: unikalna sól dla każdego hasła sprawia, że wstępnie obliczone tablice tęczowe są nieskuteczne [2].

Klucze słownictwa i kryteria oceny

Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).

PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

F 1. STUFFING	H 2. BCRYPT	D 3. NARUSZENIE	G 4. SOLENIE
C 5. MENEDŻER	B 6. MFA	A 7. TĘCZOWE	E 8. PHISHING

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 STUFFING	2 BCRYPT	3 NARUSZENIE	4 SOLENIE
5 MENEDŻER	6 MFA		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 H – PHISHING	2 C – NARUSZENIE	3 B – BCRYPT	4 G – TĘCZOWATABLICA
5 A – STUFFING	6 D – SOLENIE	7 E – MENEDŻER	8 F – WERYFIKACJAMFA

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia STUFFING, BCRYPT i NARUSZENIE oraz podać przykład każdego z nich.

Studia przypadków:
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

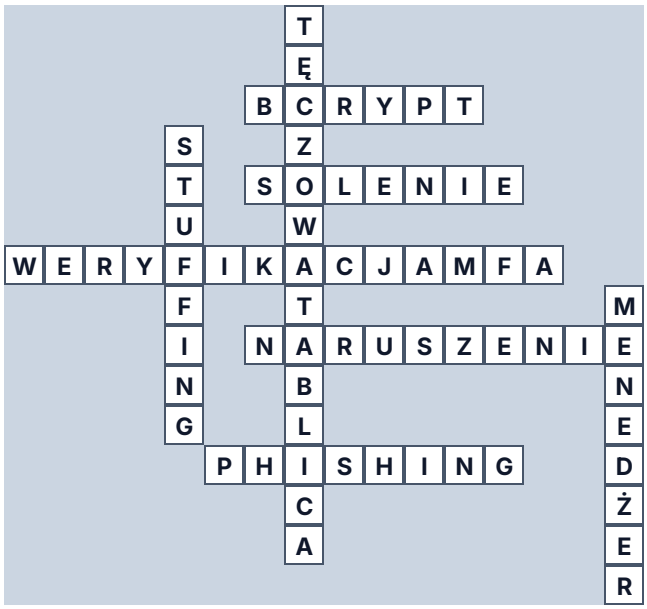
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

T	Ę	C	Z	O	W	A	T	A	B	L	I	C	A	G
M	Ż	G	K	R	E	Ż	D	E	N	E	M	O	P	S
Ń	X	C	M	Ż	Ź	F	Z	O	X	U	L	V	O	Ó
B	Ń	W	T	M	G	V	Ć	Z	V	L	R	L	Ą	Y
Ż	E	I	N	E	Z	S	U	R	A	N	E	Z	M	S
Q	Y	I	Ó	D	A	Ć	K	Q	W	N	X	X	L	J
H	T	H	F	Ą	E	I	L	Ś	I	S	W	Q	Ź	E
H	E	S	C	A	Ł	P	C	E	Ż	M	L	W	S	U
Ą	S	X	K	M	M	G	H	N	H	R	Ę	L	Ś	Ł
T	R	X	H	G	N	I	H	S	I	H	P	B	U	Ę
P	W	E	R	Y	F	I	K	A	C	J	A	M	F	A
Y	Z	O	Ź	X	S	G	T	Y	A	Ó	V	Ń	Ń	Ź
R	O	S	T	U	F	F	I	N	G	H	P	T	H	Ó
C	V	U	O	U	T	K	A	E	Ó	N	L	Ą	Ń	V
B	F	F	P	Q	Y	Ź	J	K	V	K	Ź	X	Z	Ó

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

2 poziomo: BCRYPT Powolny algorytm haszowania haseł. (6 liter)

4 poziomo: SOLENIE Dodawanie losowej soli do skrótu hasła. (7 liter)

5 poziomo: WERYFIKACJAMFA Wieloskładnikowa kontrola logowania. (14 liter)

7 poziomo: NARUSZENIE Nieautoryzowane ujawnienie bazy danych. (10 liter)

8 poziomo: PHISHING Socjotechnika służąca do wykradania danych logowania. (8 liter)

PIONOWO

1 pionowo: TĘCZOWATABLICA Wstępnie obliczona tablica skrótów haseł. (14 liter)

3 pionowo: STUFFING Testowanie wyciekniętych poświadczeń. (8 liter)

6 pionowo: MENEDŻER Narzędzie do przechowywania poświadczeń. (8 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. NFFSITGU — **STUFFING**
2. IUNASEENZR — **NARUSZENIE**
3. EEMDŻREN — **MENEDŻER**
4. ĘACBZAWATILTCO — **TĘCZOWATABLICA**
5. YRTBPC — **BCRYPT**
6. ILNSEEO — **SOLENIE**
7. AFJWCERAIMAYKF — **WERYFIKACJAMFA**
8. SHHGPNII — **PHISHING**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"ZABEZPIECZ WYCIEKŁE HASŁA PRZEZ MFA"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Naprawa wycieku poświadczeń w firmie

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Usługa monitorowania dark webu informuje organizację, że w internecie opublikowano zrzut bazy danych zawierający hasła firmowych administratorów systemów.
- Zalecana strategia i rozwiązanie: Unieważnij wszystkie aktywne sesje administratorów i zresetuj dane uwierzytelniające za pomocą generatora o wysokiej entropii. Wymuś MFA odporne na phishing w portalach administracyjnych [6], zmień dotknięte klucze API, przejrzyj logi logowań, znajdź pierwotne źródło ekspozycji i sprawdź inne konta uprzywilejowane.

B Studium przypadku 2: Wdrażanie standardów haszowania haseł

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Baza danych firmy przechowuje obecnie hasła użytkowników w postaci przestarzałych skrótów MD5 bez soli kryptograficznej, przez co można je szybko wydobyć.
- Zalecana strategia i rozwiązanie: Przyjmij Argon2id (lub bcrypt w starszych systemach) z unikalną solą dla każdego użytkownika [2]. Opakuj istniejące skróty MD5 w nowy algorytm już teraz, przeliczaj je bezpośrednio przy następnym logowaniu każdego użytkownika i wymuś reset haseł dla kont długo nieaktywnych.