**Nome:** _____ **Data:** _____ **Punteggio:** _____

# Fughe di password e sicurezza delle credenziali

Credential stuffing, violazioni dei dati, algoritmi di hash, autenticazione a più fattori e sicurezza delle password.

## PANORAMICA DI APPRENDIMENTO SULLE FUGHE DI PASSWORD

**PROTETTO**
**CRITTOGRAFIA DEI DATI**
Standard AES a 256 bit

**CONFORME**
**STANDARD GLOBALI**
Framework GDPR e CCPA

**ZERO-TRUST**
**POLITICA DI ACCESSO**
Autenticazione a più fattori

**Benvenuto!** Questo pacchetto di attività ti guida attraverso le perdite di password e la sicurezza delle credenziali. Esplorerai il credential stuffing, le violazioni di dati, gli algoritmi di hashing, l'autenticazione a più fattori e i gestori di password.

### PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia la sicurezza informatica e la prevenzione delle minacce.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

**Apri la guida alla sicurezza informatica di VPN.com**

URL: https://www.vpn.com/it/sicurezza-informatica/fuga-password/

# Il tuo percorso di apprendimento sulla sicurezza delle password

- Comprendi i rischi di esposizione delle credenziali sui forum del dark web.
- Implementa l'autenticazione a più fattori (MFA) e il monitoraggio delle credenziali compromesse.
- Progetta difese di sicurezza aziendali contro le truffe mirate di ingegneria sociale.

## ISTRUZIONI DELLA GUIDA SULLE FUGHE DI PASSWORD

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze alla protezione delle credenziali. Concludi con l'attività bonus Pensa veloce.

## FUGHE DI PASSWORD E SICUREZZA DELLE CREDENZIALI (INTRODUZIONE)

Le fughe di password espongono le credenziali degli utenti su siti pubblici e del dark web. Password uniche generate da un gestore di password, il controllo delle password compromesse e l'autenticazione a più fattori (MFA) riducono il rischio di credential stuffing, mentre un hashing delle password con salt e lento limita i danni se un database di password viene rubato.

**LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.**

## Punto di controllo 1: Sfida a scelta multipla

**1. Che cos'è il credential stuffing?**

- A. Usare l'automazione per testare combinazioni di nome utente e password trapelate su più siti
- B. Crittografare i file di archiviazione dei database locali
- C. Sovraccaricare i server web con richieste di traffico di rete
- D. Monitorare di nascosto gli input della tastiera

**2. Quale algoritmo indica OWASP come prima scelta oggi per la memorizzazione delle password?**

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

**3. In che modo l'autenticazione a più fattori (MFA) riduce il rischio di fughe di password?**

- A. Richiede un fattore di verifica aggiuntivo, quindi una password rubata da sola non basta
- B. Cambia automaticamente la password ogni ora
- C. Cifra il nome utente durante la trasmissione
- D. Avvisa l'ufficio di credito delle richieste fraudolente

**4. Che cos'è un dump di dati di una violazione?**

- A. Una raccolta di credenziali utente trapelate, pubblicate online o vendute sui forum di hacker
- B. Una copia di backup dei file del database archiviata fuori sede
- C. Una cache temporanea dei log del server web
- D. Uno strumento amministrativo usato per reimpostare le password degli utenti

**5. Qual è il ruolo di un gestore di password?**

- A. Generare e memorizzare password univoche e robuste per ogni account
- B. Monitorare il traffico di rete alla ricerca di perdite di password
- C. Bloccare al gateway gli attacchi automatizzati di forza bruta
- D. Analizzare i blocchi di archiviazione del database alla ricerca di password non cifrate

## Punto di controllo 2: Sfida Vero o Falso

### 6 Domanda 6

6. Riutilizzare le password su più account aumenta il rischio di credential stuffing.

- ◯ Vero
- ◯ Falso

### 7 Domanda 7

7. SHA-1 è una funzione di hashing consigliata per l'archiviazione moderna delle password.

- ◯ Vero
- ◯ Falso

### 8 Domanda 8

8. Imporre solo la complessità delle password (senza MFA) ferma completamente il credential stuffing.

- ◯ Vero
- ◯ Falso

### 9 Domanda 9

9. Gli strumenti di monitoraggio del dark web analizzano Internet alla ricerca di credenziali aziendali compromesse.

- ◯ Vero
- ◯ Falso

### 10 Domanda 10

10. Gli hash con salt aggiungono dati casuali univoci alle password prima dell'hashing per sconfiggere gli attacchi con rainbow table.

- ◯ Vero
- ◯ Falso

## Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. Testare credenziali trapelate su molte applicazioni web è il credential _____ .
2. Un algoritmo di hashing delle password lento e adattivo, ancora accettato da OWASP, è _____ .
3. L'esposizione di file riservati di un database su internet è una _____ di dati.
4. Aggiungere valori casuali alle password prima dell'hashing si chiama _____ .
5. Un database locale sicuro per le credenziali degli utenti è un _____ di password.
6. Aggiungere un secondo passaggio di verifica dell'accesso richiede l'autenticazione _____ .

**BANCA DELLE PAROLE DEL VOCABOLARIO**

BCRYPT GESTORE MULTIFATTORE PHISHING RAINBOW SALTING STUFFING VIOLAZIONE

**Scrivi qui le tue risposte:**

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

# Punto di controllo 4: Abbinamento di concetti sulla sicurezza

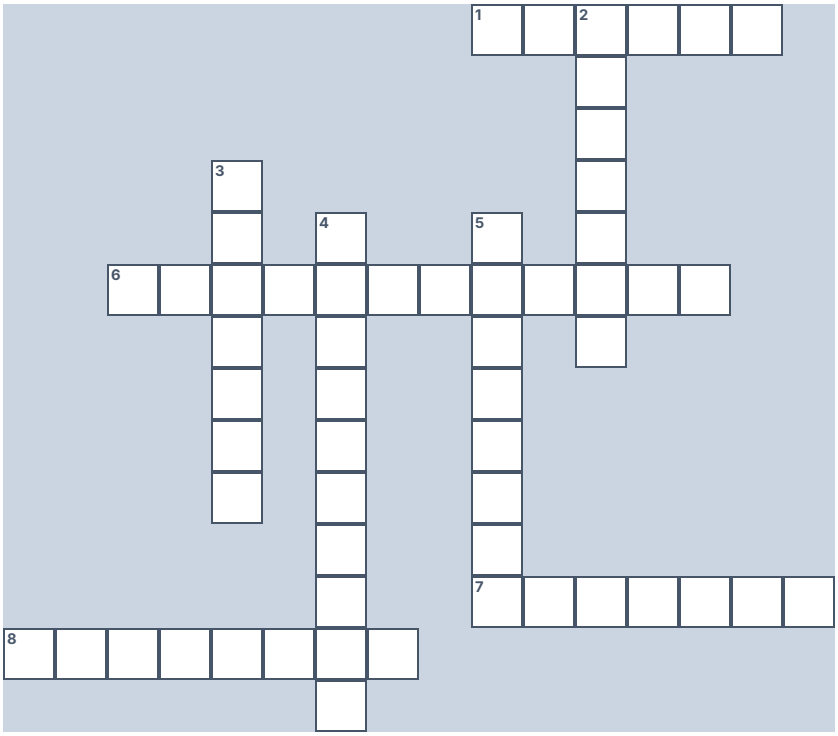
## ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

| | | | |
|---|---|---|---|
| ☐ | 1. STUFFING | A | Tabella precalcolata di hash di password. |
| ☐ | 2. BCRYPT | B | Verifica di accesso a più fattori. |
| ☐ | 3. VIOLAZIONE | C | Strumento per l'archiviazione delle credenziali. |
| ☐ | 4. SALTING | D | Esposizione non autorizzata di un database. |
| ☐ | 5. GESTORE | E | Ingegneria sociale per rubare gli accessi. |
| ☐ | 6. MFA | F | Verifica di credenziali trapelate. |
| ☐ | 7. RAINBOW | G | Aggiungere un salt casuale all'hash della password. |
| ☐ | 8. PHISHING | H | Algoritmo lento di hashing delle password. |

## Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.




### ORIZZONTALI

**1. Algoritmo lento di hashing delle password. (6)**

**6. Controllo di accesso a più fattori. (12)**

**7. Strumento di archiviazione delle credenziali. (7)**

**8. Ingegneria sociale per rubare gli accessi. (8)**

### VERTICALI

**2. Tabella precalcolata di hash di password. (7)**

**3. Aggiunta di un salt casuale all'hash della password. (7)**

**4. Esposizione non autorizzata di database. (10)**

**5. Verifica di credenziali trapelate. (8)**

# Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

## ORIZZONTALI

**1 orizzontale: Algoritmo lento di hashing delle password. (6 lettere):**

**6 orizzontale: Controllo di accesso a più fattori. (12 lettere):**

**7 orizzontale: Strumento di archiviazione delle credenziali. (7 lettere):**

**8 orizzontale: Ingegneria sociale per rubare gli accessi. (8 lettere):**

## VERTICALI

**2 verticale: Tabella precalcolata di hash di password. (7 lettere):**

**3 verticale: Aggiunta di un salt casuale all'hash della password. (7 lettere):**

**4 verticale: Esposizione non autorizzata di database. (10 lettere):**

**5 verticale: Verifica di credenziali trapelate. (8 lettere):**

## Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

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

**ELENCO DELLE PAROLE DEL VOCABOLARIO**

STUFFING BCRYPT VIOLAZIONE SALTING GESTORE MULTIFATTORE RAINBOW PHISHING

# Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

| TERMINI DEL VOCABOLARIO | DEFINIZIONI E CAMPI DI ABBINAMENTO |
|---|---|
| **A. STUFFING** | _____ 1. Ingegneria sociale per rubare gli accessi. |
| **B. BCRYPT** | _____ 2. Esposizione non autorizzata di database. |
| **C. VIOLAZIONE** | _____ 3. Algoritmo lento di hashing delle password. |
| **D. SALTING** | _____ 4. Tabella precalcolata di hash di password. |
| **E. GESTORE** | _____ 5. Verifica di credenziali trapelate. |
| **F. MULTIFATTORE** | _____ 6. Aggiunta di un salt casuale all'hash della password. |
| **G. RAINBOW** | _____ 7. Strumento di archiviazione delle credenziali. |
| **H. PHISHING** | _____ 8. Controllo di accesso a più fattori. |

## Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave della sicurezza informatica. Scrivi le tue risposte nelle caselle fornite.

1. NFFSITGU
2. NLVIAEIOZO
3. TGOESRE
4. WABNORI
5. YRTBPC
6. NLISTGA
7. TTIMUAEORLFT
8. SHHGPNII

# Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

| | | | | |
|---|---|---|---|---|
| 1 | Buone abitudini sicure che puoi iniziare oggi | | | |
| 2 | Regole per una password robusta | | | |
| 3 | Gestori di password che conosci | | | |
| 4 | Strumenti di sicurezza che conosci | | | |
| 5 | Segnali di allarme in un'email | | | |
| 6 | Parole divertenti per una lunga passphrase | | | |
| 7 | Modi per accedere senza password | | | |
| 8 | Informazioni che non dovresti mai condividere | | | |
| 9 | Motivi per aggiornare il software | | | |
| 10 | Cose da fare quando una password viene diffusa | | | |
| 11 | Account che richiedono l'MFA | | | |
| 12 | Luoghi in cui le password non dovrebbero mai essere memorizzate | | | |
| 13 | Segnali che indicano che un computer è infetto | | | |
| 14 | Password scadenti che le persone usano | | | |
| 15 | Cose di cui fai il backup | | | |

# Punto di controllo 8: Casi di studio sulla sicurezza informatica

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

## CASO DI STUDIO 1: RISOLUZIONE DI UNA FUGA DI CREDENZIALI AZIENDALI

👷

**Scenario:** Un servizio di monitoraggio del dark web avvisa un'organizzazione che un dump di un database contenente le password degli amministratori di sistema aziendali è stato pubblicato online.

**Domanda di discussione:** Analizza i rischi della fuga di credenziali e proponi una strategia amministrativa di reimpostazione.

## CASO DI STUDIO 2: IMPLEMENTARE GLI STANDARD DI HASHING DELLE PASSWORD

👷

**Scenario:** Un database aziendale attualmente memorizza le password degli utenti usando hash MD5 obsoleti senza salt crittografico, rendendole vulnerabili a una rapida estrazione.

**Domanda di discussione:** Progetta una strategia di migrazione per aggiornare l'algoritmo di hashing del database.

## Punto di controllo 9: Decifrare il codice

Un professionista della sicurezza informatica protegge le risorse di rete dagli attori delle minacce online. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

**CHIAVE DI CIFRATURA LETTERA-NUMERO**

**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 7 9 16 1 19 19 23 15 18 4

20 18 1 16 5 12 1 20 5 3 15 14

13 21 12 20 9 6 1 20 20 15 18 5

**Messaggio decifrato:**

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

# Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte A)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

### Q1: Che cos'è una fuga di password?

Una fuga di password si verifica quando le credenziali di accesso degli utenti vengono esposte a causa di violazioni dei dati o configurazioni errate dei server.

### Q2: Come trovano gli hacker le password trapelate?

Gli hacker esaminano forum del dark web, dump pubblici di database e siti di paste in cui vengono pubblicati i dati delle violazioni [8].

### Q3: Riutilizzare la stessa password è pericoloso?

Sì, perché se un sito viene compromesso, gli hacker possono provare le stesse credenziali su migliaia di altre piattaforme [3].

### Q4: Cos'è un salt crittografico?

Un salt è un dato casuale aggiunto a una password prima dell'hashing, che rende inefficaci gli attacchi con tabelle precalcolate [2].

### Q5: Perché MD5 è obsoleto?

MD5 è un hash generico veloce e obsoleto, quindi gli attaccanti possono provare tentativi di password estremamente in fretta, soprattutto quando gli hash sono privi di salt [2].

# Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte B)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

### Q6: Come protegge gli utenti un gestore di password?

Genera automaticamente credenziali complesse e uniche per ogni sito, riducendo gli errori di memoria umana e il riutilizzo.

### Q7: Cos'è un attacco a forza bruta?

Un attacco che prova sistematicamente ogni possibile combinazione di caratteri finché non trova la password corretta [4].

### Q8: Come aiuta il blocco dell'account?

Il blocco o la limitazione della frequenza rallenta i tentativi ripetuti di indovinare online la password e, se combinato con monitoraggio e MFA, riduce il rischio di attacchi a forza bruta [4].

### Q9: Le password principali (master password) sono sicure?

Sono sicure se sono passphrase ad alta entropia che non vengono mai riutilizzate su altri sistemi web.

### Q10: Le password vanno cambiate regolarmente?

Il NIST afferma di non imporre cambi periodici; cambiale solo in presenza di prove di compromissione e dai priorità a lunghezza, elenchi di blocco e MFA [1].

# Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte C)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

### Q1: Come si confronta Argon2 con bcrypt?

OWASP indica Argon2id come prima scelta; le sue impostazioni ad alto consumo di memoria resistono al cracking con GPU e ASIC meglio di bcrypt [2].

### Q2: Che cos'è il key stretching?

Una tecnica che ripete un algoritmo di hashing migliaia di volte per rallentare il processo di verifica della password, rendendo costoso il cracking [2].

### Q3: Come funzionano le rainbow table?

Sono tabelle di ricerca precalcolate che collegano le password in chiaro ai loro hash, usate per invertire rapidamente gli hash senza salt [2].

### Q4: Cos'è il riciclo delle credenziali?

Riutilizzare coppie di nome utente e password rubate in una violazione dei dati per tentare di accedere ad altri servizi, soprattutto dove le persone hanno riutilizzato le password [3].

### Q5: I gestori di password possono essere violati?

Sì. Molti usano la crittografia a conoscenza zero, quindi una violazione dei server espone solo casseforti cifrate, ma le master password deboli possono comunque essere decifrate offline.

# Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte D)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

### Q6: Cos'è un attacco a dizionario?

Una variante della forza bruta che prova parole comuni, frasi e password trapelate in passato anziché lettere casuali.

### Q7: Perché si preferiscono le passphrase?

Le passphrase usano più parole casuali, creando un'entropia elevata, facile da ricordare per gli esseri umani ma costosa da violare dal punto di vista computazionale [1].

### Q8: Come influisce il single sign-on (SSO) sulle fughe di password?

L'SSO riduce la proliferazione delle password, ma il provider di identità diventa un bersaglio di grande valore che richiede una MFA forte, preferibilmente resistente al phishing [6].

### Q9: Cos'è il session hijacking?

Un aggressore ottiene o abusa di un token di sessione valido per impersonare un utente connesso senza bisogno di conoscere di nuovo la password [5].

### Q10: Come si rileva il password spraying?

Cercando le stesse poche password provate su molti account, spesso lentamente per restare sotto le soglie di blocco [7].

## Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

Rivedi fatti reali su violazioni della sicurezza, meccanismi di difesa e standard di conformità.

**1. APPROFONDIMENTO SULLA SICUREZZA**

NIST SP 800-63B richiede che le nuove password vengano confrontate con elenchi di blocco di password comuni e compromesse [1].

**2. APPROFONDIMENTO SULLA SICUREZZA**

Il dump «Collection #1» del 2019 ha unito i dati di molte violazioni precedenti in un unico enorme file di coppie email e password [8].

**3. APPROFONDIMENTO SULLA SICUREZZA**

Il NIST ora richiede che le password usate come unico fattore di autenticazione siano lunghe almeno 15 caratteri [1].

**4. APPROFONDIMENTO SULLA SICUREZZA**

L'hardware ASIC può calcolare miliardi di hash SHA-256 al secondo, il che rende l'hashing SHA grezzo non sicuro per le password degli utenti [2].

**5. APPROFONDIMENTO SULLA SICUREZZA**

I salt univoci fanno sì che due utenti con la stessa identica password ottengano hash diversi nel database [2].

**6. APPROFONDIMENTO SULLA SICUREZZA**

Molti gestori di password crittografano i dati del caveau in locale con una crittografia robusta derivata dalla password principale dell'utente.

**7. APPROFONDIMENTO SULLA SICUREZZA**

Il credential stuffing funziona perché molte persone riutilizzano la stessa password su account di e-commerce, banche ed email [3].

**8. APPROFONDIMENTO SULLA SICUREZZA**

NIST SP 800-63B afferma che i verificatori non devono richiedere cambi periodici della password, ma solo cambi dopo prove di compromissione [1].

**9. APPROFONDIMENTO SULLA SICUREZZA**

Aggiungere una sola lettera maiuscola e un simbolo a una password breve non ferma i moderni attacchi automatici a dizionario con GPU [1].

**10. APPROFONDIMENTO SULLA SICUREZZA**

L'MFA può bloccare molti tentativi di credential stuffing anche dopo la fuga di una password; l'MFA resistente al phishing è più robusta dei codici via SMS [3].

# Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire dagli standard globali NIST, OWASP e di conformità alla privacy dei dati.

## RIFERIMENTI ACCADEMICI E DI SETTORE

[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/

## Soluzioni: Punto di controllo 1 – Scelta multipla

**1 Domanda 1** — **Risposta corretta: A**

### NOTA DIDATTICA

Il credential stuffing usa l'automazione per provare coppie di nome utente e password trapelate su altri siti [3].

**2 Domanda 2** — **Risposta corretta: A**

### NOTA DIDATTICA

OWASP raccomanda Argon2id come prima scelta; bcrypt è usato principalmente per i sistemi legacy in cui Argon2id o scrypt non sono disponibili [2].

**3 Domanda 3** — **Risposta corretta: A**

### NOTA DIDATTICA

L'MFA richiede un fattore aggiuntivo, quindi una password rubata da sola non può sbloccare l'account [3].

**4 Domanda 4** — **Risposta corretta: A**

### NOTA DIDATTICA

I breach dump sono raccolte di credenziali trapelate, come la compilazione Collection #1 del 2019 [8].

**5 Domanda 5** — **Risposta corretta: A**

### NOTA DIDATTICA

Un gestore di password genera e memorizza una password unica e robusta per ogni account, evitando il riutilizzo [3].

## Soluzioni: Punto di controllo 2 – Vero o falso

**6** **Domanda 6** — **Risposta corretta: Vero**

### NOTA DIDATTICA

Vero: le password riutilizzate permettono agli aggressori di riutilizzare su altri siti le credenziali trapelate da uno solo [3].

**7** **Domanda 7** — **Risposta corretta: Falso**

### NOTA DIDATTICA

Falso: SHA-1 è un hash veloce; OWASP raccomanda invece Argon2id, scrypt, bcrypt o PBKDF2 [2].

**8** **Domanda 8** — **Risposta corretta: Falso**

### NOTA DIDATTICA

Falso: le sole regole di complessità non possono fermare lo stuffing con password trapelate e riutilizzate; serve l'MFA [3].

**9** **Domanda 9** — **Risposta corretta: Vero**

### NOTA DIDATTICA

Vero: i servizi di monitoraggio cercano nei breach dump e nelle fonti del dark web le credenziali esposte [8].

**10** **Domanda 10** — **Risposta corretta: Vero**

### NOTA DIDATTICA

Vero: un salt unico per ogni password rende inefficaci le rainbow table precalcolate [2].

# Chiavi del vocabolario e griglia di valutazione

**Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).**

## PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

| | | | |
|---|---|---|---|
| F 1. STUFFING | H 2. BCRYPT | D 3. VIOLAZIONE | G 4. SALTING |
| C 5. GESTORE | B 6. MFA | A 7. RAINBOW | E 8. PHISHING |

## PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

| | | | |
|---|---|---|---|
| 1 STUFFING | 2 BCRYPT | 3 VIOLAZIONE | 4 SALTING |
| 5 GESTORE | 6 MULTIFATTORE | | |

## PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

| | | | |
|---|---|---|---|
| 1 H – PHISHING | 2 C – VIOLAZIONE | 3 B – BCRYPT | 4 G – RAINBOW |
| 5 A – STUFFING | 6 D – SALTING | 7 E – GESTORE | 8 F – MULTIFATTORE |

## NOTE DI DISCUSSIONE PER GLI INSEGNANTI

**Termini chiave:**
Verifica che gli studenti sappiano spiegare STUFFING, BCRYPT e VIOLAZIONE con parole proprie e fare un esempio per ciascuno.

**Casi di studio:**
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

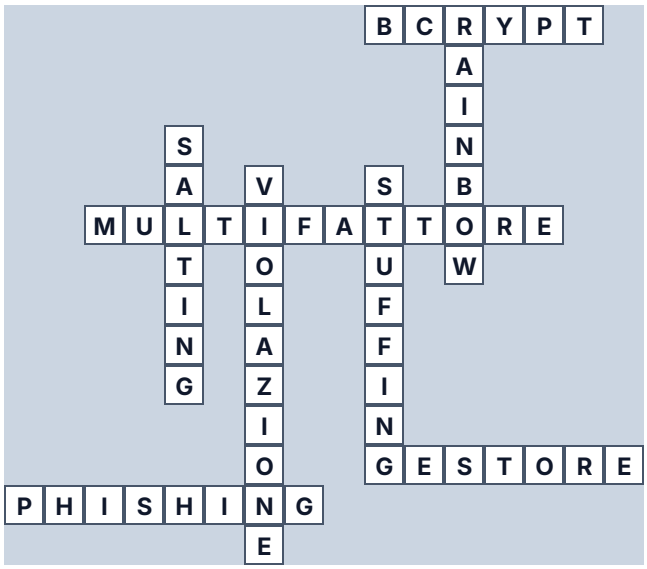
**Valutazione delle fonti:**
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

# Soluzioni dei rompicapi e note per l'insegnante

## SOLUZIONE DELLA RICERCA DELLE PAROLE

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

## SOLUZIONE DEL CRUCIVERBA




## GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

### ORIZZONTALI

**1 orizzontale: BCRYPT** Algoritmo lento di hashing delle password. (6 lettere)

**6 orizzontale: MULTIFATTORE** Controllo di accesso a più fattori. (12 lettere)

**7 orizzontale: GESTORE** Strumento di archiviazione delle credenziali. (7 lettere)

**8 orizzontale: PHISHING** Ingegneria sociale per rubare gli accessi. (8 lettere)

### VERTICALI

**2 verticale: RAINBOW** Tabella precalcolata di hash di password. (7 lettere)

**3 verticale: SALTING** Aggiunta di un salt casuale all'hash della password. (7 lettere)

**4 verticale: VIOLAZIONE** Esposizione non autorizzata di database. (10 lettere)

**5 verticale: STUFFING** Verifica di credenziali trapelate. (8 lettere)

# Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

### CHIAVE DELLE PAROLE DA RIORDINARE

1. NFFSITGU — **STUFFING**
2. NLVIAEIOZO — **VIOLAZIONE**
3. TGOESRE — **GESTORE**
4. WABNORI — **RAINBOW**
5. YRTBPC — **BCRYPT**
6. NLISTGA — **SALTING**
7. TTIMUAEORLFT — **MULTIFATTORE**
8. SHHGPNII — **PHISHING**

### CHIAVE DELLA SFIDA DEL CODICE SEGRETO

**"PROTEGGI PASSWORD TRAPELATE CON MULTIFATTORE"**

# Soluzioni dei casi di studio

## A Caso di studio 1: risoluzione di una fuga di credenziali aziendali

Soluzione per l'insegnante

### LINEA GUIDA DI VALUTAZIONE

**Le risposte degli studenti dovrebbero coprire i seguenti punti:**

- Analisi dello scenario: un servizio di monitoraggio del dark web avvisa un'organizzazione che un dump di database contenente le password degli amministratori di sistema aziendali è stato pubblicato online.
- Strategia e soluzione consigliate: Revoca tutte le sessioni amministrative attive e reimposta le credenziali con un generatore ad alta entropia. Applica un'MFA resistente al phishing sui portali di amministrazione [6], ruota le chiavi API interessate, esamina i log di accesso, individua l'esposizione iniziale e controlla gli altri account con privilegi.

## B Caso di studio 2: Implementare gli standard di hashing delle password

Soluzione per l'insegnante

### LINEA GUIDA DI VALUTAZIONE

**Le risposte degli studenti dovrebbero coprire i seguenti punti:**

- Analisi dello scenario: Il database di un'azienda archivia attualmente le password degli utenti con hash MD5 obsoleti e senza salt crittografico, rendendole vulnerabili a una rapida estrazione.
- Strategia e soluzione consigliate: adottare Argon2id (o bcrypt sui sistemi legacy) con un salt univoco per ogni utente [2]. Incapsulare subito gli hash MD5 esistenti nel nuovo algoritmo, rieseguire l'hashing direttamente al successivo accesso di ciascun utente e forzare il reset per gli account inattivi da molto tempo.