שם: _____ תאריך: _____ ציון: _____

# דליפות סיסמאות ואבטחת פרטי גישה

Credential Stuffing, פרצות נתונים, אלגוריתמי גיבוב, אימות רב-שלבי ואבטחת סיסמאות.

## סקירת למידה: דליפות סיסמאות

### אובטח

**הצפנת נתונים**

תקן AES של 256 סיביות

### תואם

**תקנים עולמיים**

מסגרות GDPR ו-CCPA

### אפס אמון

**מדיניות גישה**

אימות רב-גורמי

**ברוכים הבאים!** חוברת הפעילויות הזו תדריך אתכם דרך דליפות סיסמאות ואבטחת פרטי כניסה. תחקרו מילוי אישורים (credential stuffing), פריצות נתונים, אלגוריתמי גיבוב, אימות רב-גורמי ומנהלי סיסמאות.

**נקודות הביקורת בדף העבודה**

- ☐ **חלק 1-4: שלטו באבטחת סייבר ובמניעת איומים.**
- ☐ **חלק 5-7: פתרו תשבצים ופאזלי חיפוש מילים.**
- ☐ **חלק 8-9: פתרו מקרי בוחן ואתגר צופן.**
- ☐ **חלק 10: סקרו את דפי השאלות הנפוצות הבסיסיים והמתקדמים.**
- ☐ **חלק 11: חקרו 10 עובדות מעניינות מהעולם האמיתי.**
- ☐ **בונוס: אתגר חשבו מהר**

**פתחו את מדריך אבטחת הסייבר של VPN.com**

URL: https://www.vpn.com/cybersecurity/passwords-leak/

# מפת הלמידה שלכם: אבטחת סיסמאות

- הבינו את סיכוני חשיפת פרטי הכניסה בפורומים ברשת האפלה.
- יישמו אימות רב-גורמי (MFA) וניטור פרטי התחברות שנחשפו.
- תכננו הגנות אבטחה ארגוניות מפני הונאות הנדסה חברתית ממוקדות.

### הוראות למדריך דליפות סיסמאות

ענו על שאלות אמריקאיות ועל שאלות נכון/לא נכון, השלימו את המשפטים החסרים בעזרת בנק המילים, התאימו הגדרות ופתרו את התשבץ ואת תפזורת המילים. יישמו את הידע שלכם בנושא הגנה על פרטי גישה. ולסיום, פעילות הבונוס "חשבו מהר".

### דליפות סיסמאות ואבטחת פרטי גישה (מבוא)

דליפות סיסמאות חושפות פרטי גישה של משתמשים באתרים ציבוריים ובדארקנט. סיסמאות ייחודיות ממנהל סיסמאות, סינון סיסמאות שנחשפו ואימות רב-שלבי (MFA) מצמצמים את הסיכון להתקפות credential stuffing, ואילו גיבוב סיסמאות איטי עם מלח מגביל את הנזק אם מסד נתוני סיסמאות נגנב.

**קראו כל נקודת ביקורת בעיון ובחרו או כתבו את התגובה הנכונה.**

# נקודת ביקורת 1: אתגר שאלות אמריקאיות

**1** 1. מהו credential stuffing?

- A. שימוש באוטומציה כדי לבדוק צירופי שם משתמש/סיסמה שדלפו בכמה אתרים
- B. הצפנת קובצי אחסון של מסד נתונים מקומי
- C. הצפת שרתי אינטרנט בבקשות תעבורת רשת
- D. ניטור סמוי של קלט מהמקלדת

**2** 2. איזה אלגוריתם OWASP מציין כבחירה הראשונה לאחסון סיסמאות כיום?

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

**3** 3. כיצד אימות רב-שלבי (MFA) מפחית את הסיכון בדליפות סיסמאות?

- A. הוא דורש גורם אימות נוסף, כך שסיסמה גנובה לבדה אינה מספיקה
- B. הוא משנה את הסיסמה אוטומטית כל שעה
- C. הוא מצפין את שם המשתמש בזמן ההעברה
- D. הוא מתריע למשרד האשראי על בקשות הונאה

**4** 4. מהו ייצוא (dump) של נתונים מפרצת נתונים?

- A. אוסף של אישורי גישה שדלפו של משתמשים, שפורסמו ברשת או נמכרים בפורומים של האקרים
- B. עותק גיבוי של קובצי מסד נתונים המאוחסן מחוץ לאתר
- C. מטמון זמני של יומני שרת אינטרנט
- D. כלי ניהול לאיפוס סיסמאות משתמשים

**5** 5. מהו תפקידו של מנהל סיסמאות?

- A. יצירה ואחסון של סיסמאות חזקות וייחודיות לכל חשבון
- B. ניטור תעבורת רשת לאיתור דליפות סיסמאות
- C. חסימת התקפות כוח גס (brute-force) אוטומטיות בשער
- D. סריקת בלוקי האחסון של מסד הנתונים בחיפוש סיסמאות לא מוצפנות

# נקודת ביקורת 2: אתגר נכון או לא נכון

**שאלה 6**

6. שימוש חוזר בסיסמאות בכמה חשבונות מגדיל את הסיכון ל-credential stuffing.

נכון לא נכון

**שאלה 7**

7. SHA-1 היא פונקציית גיבוב מומלצת לאחסון סיסמאות מודרני.

נכון לא נכון

**שאלה 8**

8. אכיפת מורכבות סיסמאות בלבד (ללא MFA) עוצרת לחלוטין מילוי פרטי גישה.

נכון לא נכון

**שאלה 9**

9. כלי ניטור האינטרנט האפל סורקים את האינטרנט בחיפוש אחר פרטי גישה ארגוניים שנפרצו.

נכון לא נכון

**שאלה 10**

10. גיבובים עם מלח (salted hashes) מוסיפים נתונים אקראיים ייחודיים לסיסמאות לפני הגיבוב כדי להכשיל התקפות rainbow table.

נכון לא נכון

# נקודת ביקורת 3: השלמת מונחי מפתח

קראו כל משפט שלהלן והשלימו את החסר במונח הנכון מבנק המילים.

1. בדיקת אישורים שדלפו ביישומי אינטרנט רבים נקראת _____ אישורים.
2. אלגוריתם גיבוב סיסמאות איטי ואדפטיבי ש-OWASP עדיין מקבלת הוא _____ .
3. חשיפה של קובצי מסד נתונים סודיים באינטרנט מהווה _____ של נתונים.
4. הוספת ערכים אקראיים לסיסמאות לפני הגיבוב נקראת _____ .
5. מסד נתונים מקומי מאובטח לאישורי משתמש הוא _____ סיסמאות.
6. הוספת שלב אימות שני בכניסה משתמשת באימות _____ .

**בנק מילים**

המלחה | טבלת קשת | מילוי | מנהל | פישינג | פריצה | רב גורמי | bcrypt

**כתבו את תשובותיכם כאן:**

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

# נקודת ביקורת 4: התאמת מושגים באבטחה

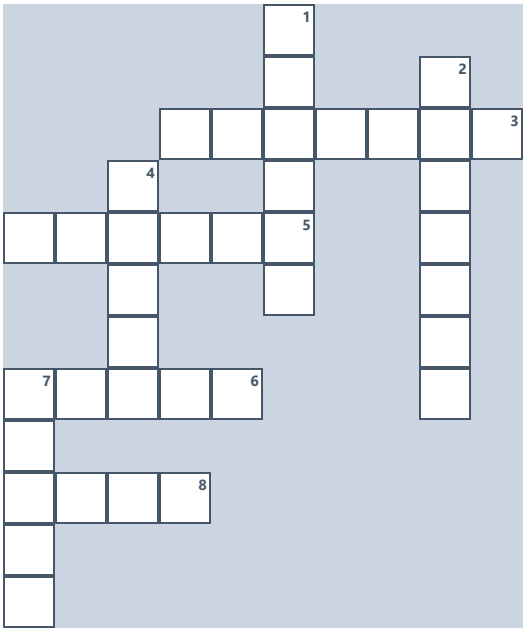
**התאמת הגדרות**

התאימו כל מונח אוצר מילים בצד ימין להגדרה הנכונה שלו בצד שמאל על ידי כתיבת האות המתאימה (A-H) בתיבת הקלט הניתנת למילוי.

| | | |
|---|---|---|
| 1. מילוי אישורים | A | טבלה מחושבת מראש של גיבובי סיסמאות. |
| 2. bcrypt | B | בדיקת התחברות רב-גורמית. |
| 3. פריצה | C | כלי לאחסון אישורי גישה. |
| 4. הוספת מלח | D | חשיפה לא מורשית של מסד נתונים. |
| 5. מנהל | E | הנדסה חברתית לגניבת פרטי כניסה. |
| 6. MFA | F | בדיקת פרטי גישה שדלפו. |
| 7. קשת | G | הוספת מלח אקראי לגיבוב הסיסמה. |
| 8. פישינג | H | אלגוריתם גיבוב סיסמאות איטי. |

# נקודת ביקורת 5: תשבץ

פתרו את התשבץ על ידי הקלדת אותיות בתיבות הלבנות הפעילות. המספרים מתאימים לרמזים שלהלן.




### מאונן

3. בדיקת כניסה ברמות אימות מרובות (7)
5. הנדסה חברתית לגניבת כניסות (6)
6. חשיפה בלתי מורשית של מסד נתונים (5)
8. כלי לאחסון אישורים (4)

### מאונך

1. אלגוריתם גיבוב סיסמאות איטי (6)
2. טבלה מחושבת מראש של גיבובי סיסמאות (7)
4. בדיקת אישורים שדלפו (5)
7. הוספת מלח אקראי לגיבוב סיסמה (5)

# נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

משתמשי קורא מסך ומקלדת יכולים להקליד את תשובות התשבץ ישירות בשדות הטקסט שלהלן.

## מאוזן

**3 מאוזן: בדיקת כניסה ברמות אימות מרובות (7 אותיות):**

**5 מאוזן: הנדסה חברתית לגניבת כניסות (6 אותיות):**

**6 מאוזן: חשיפה בלתי מורשית של מסד נתונים (5 אותיות):**

**8 מאוזן: כלי לאחסון אישורים (4 אותיות):**

## מאונך

**1 מאונך: אלגוריתם גיבוב סיסמאות איטי (6 אותיות):**

**2 מאונך: טבלה מחושבת מראש של גיבובי סיסמאות (7 אותיות):**

**4 מאונך: בדיקת אישורים שדלפו (5 אותיות):**

**7 מאונך: הוספת מלח אקראי לגיבוב סיסמה (5 אותיות):**

# נקודת ביקורת 6: חיפוש מילה נסתרת

מצאו את 8 מונחי המפתח בלוח שלהלן. מילים יכולות להופיע אופקית, אנכית או באלכסון.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ח | ט | ת | מ | ע | ק | א | ה | ס | ט | ד | ט | ר | כ | ת |
| נ | פ | ש | ו | נ | כ | ג | מ | מ | ע | ח | ו | ל | ס | כ |
| נ | י | ר | נ | מ | ג | צ | ל | ע | י | פ | ד | י | ח | ב |
| א | ר | ב | ג | מ | ש | י | ח | ט | ש | ל | י | ר | פ | ט |
| ד | ק | ס | כ | ט | ר | ד | ה | ח | ל | ל | ו | י | פ | נ |
| נ | ב | ו | כ | כ | ב | ס | ט | ס | ע | פ | פ | י | ר | ו |
| ג | ב | ע | נ | מ | ג | ז | ע | ב | ב | ק | ד | ע | י | ת |
| נ | צ | ג | ת | ק | ו | ה | ט | ז | ל | ת | ג | ל | צ | ד |
| י | ס | ר | נ | ב | ר | צ | ב | א | ת | ת | ל | ד | ה | י |
| ש | א | ד | מ | ד | מ | ה | ז | ח | ג | ס | ק | ס | כ | ד |
| י | ח | ע | ת | ע | י | ה | ס | ק | ה | א | א | ש | ס | מ |
| פ | ל | נ | פ | ש | מ | נ | ט | ע | פ | ע | ג | ל | ת | ש |
| ב | ה | ע | ר | ר | ח | נ | א | ס | ת | ש | ש | י | ו | ח |
| כ | ס | ט | כ | כ | פ | מ | ה | ז | נ | ס | ז | ת | א | מ |
| צ | ו | צ | ב | ש | ע | ש | ב | ל | ז | כ | ת | ו | ט | מ |

**רשימת מילים**

מילוי | בקריפט | פריצה | המלחה | מנהל | רבגורמי | טבלתקשת | פישינג

# נקודת ביקורת 6 – פעילות חלופית: התאמת אוצר מילים נגישה

התאימו כל אחד מ-8 מונחי המילון מתפזורת המילים להגדרה הנכונה שלו על ידי כתיבת האות (A-H) במקום הריק.

| מונחי אוצר מילים |
| --- |
| **A. מילוי** |
| **B. בקריפט** |
| **C. פריצה** |
| **D. המלחה** |
| **E. מנהל** |
| **F. רבגורמי** |
| **G. טבלתקשת** |
| **H. פישינג** |

| הגדרות ושדות התאמה | |
| --- | --- |
| 1. הנדסה חברתית לגניבת כניסות. | |
| 2. חשיפה בלתי מורשית של מסד נתונים. | |
| 3. אלגוריתם גיבוב סיסמאות איטי. | |
| 4. טבלה מחושבת מראש של גיבובי סיסמאות. | |
| 5. בדיקת אישורים שדלפו. | |
| 6. הוספת מלח אקראי לגיבוב סיסמה. | |
| 7. כלי לאחסון אישורים. | |
| 8. בדיקת כניסה ברמות אימות מרובות. | |

## נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים באבטחת סייבר. כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. ולמיי
2. פהציר
3. למהנ
4. תבקתשטל
5. ירטבפק
6. חהלהמ
7. רמריבוג
8. שגפניי

# פעילות בונוס: חשבו מהר

כתבו 3 תשובות לכל קטגוריה. מי שמסיים ראשון את הרשימה מנצח.

| | | | |
|---|---|---|---|
| 1 | הרגלים בטוחים שאפשר להתחיל כבר היום | | |
| 2 | כללים לסיסמה חזקה | | |
| 3 | מנהלי סיסמאות שאתם מכירים | | |
| 4 | כלי אבטחה שאתם מכירים | | |
| 5 | סימני אזהרה באימייל | | |
| 6 | מילים משעשעות לביטוי סיסמה ארוך | | |
| 7 | דרכים להתחבר בלי סיסמה | | |
| 8 | מידע שלעולם אסור לשתף | | |
| 9 | סיבות לעדכן תוכנה | | |
| 10 | דברים שעושים כשסיסמה דולפת | | |
| 11 | חשבונות שזקוקים ל-MFA | | |
| 12 | מקומות שבהם אסור לשמור סיסמאות | | |
| 13 | סימנים לכך שמחשב נדבק | | |
| 14 | סיסמאות גרועות שאנשים משתמשים בהן | | |
| 15 | דברים שמגבים | | |

# נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

יישמו את המושגים שלמדתם כדי לפתור את התרחישים מהעולם האמיתי שלהלן.

### מקרה בוחן 1: טיפול בדליפת אישורי גישה ארגוניים



**תרחיש:** שירות ניטור הרשת האפלה (dark web) מתריע בפני ארגון שמאגר נתונים המכיל סיסמאות של מנהלי מערכת בארגון פורסם באינטרנט.

**שאלה לדיון:** נתחו את סיכוני דליפת פרטי הגישה, והציעו אסטרטגיית איפוס מנהלית.

### מקרה בוחן 2: הטמעת תקני גיבוב סיסמאות



**תרחיש:** מסד נתונים ארגוני שומר כעת סיסמאות משתמשים באמצעות גיבובי MD5 מיושנים ללא מלח (salt) קריפטוגרפי, מה שהופך אותן לפגיעות לחילוץ מהיר.

**שאלה לדיון:** תכננו אסטרטגיית מעבר לשדרוג אלגוריתם הגיבוב של מסד הנתונים.

# נקודת ביקורת 9: פענוח הצופן

איש מקצוע באבטחת סייבר מגן על נכסי רשת מפני גורמי איום מקוונים. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה, וכתבו את האותיות המתאימות במקומות הריקים.

**מפתח הצפנה של אות למספר**

**א=1 ב=2 ג=3 ד=4 ה=5 ו=6 ז=7 ח=8 ט=9**

**י=10 כ=11 ל=12 מ=13 נ=14 ס=15 ע=16 פ=17 צ=18**

**ק=19 ר=20 ש=21 ת=22 ך=23 ם=24 ן=25 ף=26 ץ=27**

| 6 | 17 | 12 | 4 | 21 | | 22 | 6 | 1 | 13 | 15 | 10 | 15 | | 6 | 8 | 9 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | |
| **24** | **10** | **13** | **20** | **6** | **3** | | **22** | **2** | **6** | **20** | **13** | | **5** | **15** | **10** | **14** | **11** | **2** |
| | | | | | | | | | | | | | | | | | | |

**ההודעה המפוענחת:**

**טיפ: כל מספר מייצג אות עברית אחת מהמפתח שלמעלה.**

# נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק A)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

### Q1: מהי דליפת סיסמאות?

דליפת סיסמאות מתרחשת כאשר פרטי התחברות של משתמשים נחשפים בשל פריצות נתונים או הגדרות שגויות בשרת.

### Q2: כיצד האקרים מוצאים סיסמאות שדלפו?

האקרים סורקים פורומים ברשת האפלה, השלכות מסדי נתונים פומביות ואתרי הדבקה שבהם מתפרסם מידע מפריצות [8].

### Q3: האם שימוש חוזר בסיסמה מסוכן?

כן, משום שאם אתר אחד נפרץ, האקרים יכולים לבדוק את אותם פרטי התחברות באלפי פלטפורמות אחרות [3].

### Q4: מהו מלח קריפטוגרפי (salt)?

מלח (salt) הוא נתונים אקראיים שנוספים לסיסמה לפני הגיבוב, ומייתרים התקפות חיפוש מחושבות מראש [2].

### Q5: מדוע MD5 מיושן?

MD5 הוא גיבוב כללי מהיר ומיושן, ולכן תוקפים יכולים לבדוק ניחושי סיסמה במהירות רבה מאוד, במיוחד כשהגיבובים אינם מומלחים [2].

# נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק B)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

### Q6: כיצד מנהל סיסמאות מגן על משתמשים?

הוא יוצר אוטומטית פרטי התחברות מורכבים וייחודיים לכל אתר ומצמצם טעויות זיכרון אנושיות ושימוש חוזר.

### Q7: מהי התקפת כוח גס (brute force)?

התקפה שבודקת באופן שיטתי כל צירוף תווים אפשרי עד שמוצאים את הסיסמה הנכונה [4].

### Q8: כיצד נעילת חשבון עוזרת?

נעילה או הגבלת קצב מאטות ניחושים חוזרים מקוונים, ובשילוב ניטור ו-MFA הן מפחיתות את סיכון התקפות כוח גס [4].

### Q9: האם סיסמאות ראשיות מאובטחות?

הן מאובטחות אם הן ביטויי סיסמה בעלי אנטרופיה גבוהה שלעולם אינם נעשים בהם שימוש חוזר במערכות אינטרנט אחרות.

### Q10: האם יש להחליף סיסמאות באופן קבוע?

NIST קובע שאין לכפות החלפות תקופתיות; יש להחליף סיסמאות עם עדות לפריצה ולתת עדיפות לאורך, לרשימות חסימה ול-MFA [1].

# נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק C)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

### Q1: כיצד Argon2 משתווה ל-bcrypt?

OWASP מציגה את Argon2id כבחירה הראשונה; הגדרות הזיכרון הכבדות שלו עמידות יותר מ-bcrypt בפני פיצוח באמצעות GPU ו-ASIC [2].

### Q2: מהו מתיחת מפתח (key stretching)?

טכניקה שמפעילה אלגוריתם גיבוב בלולאה אלפי פעמים כדי להאט את תהליך אימות הסיסמה ולייקר את הפריצה [2].

### Q3: כיצד פועלות טבלאות קשת (rainbow tables)?

אלה טבלאות בדיקה מחושבות מראש המקשרות סיסמאות בטקסט גלוי לגיבובים שלהן, ומשמשות להיפוך מהיר של גיבובים ללא מלח [2].

### Q4: מהו מיחזור אישורי גישה?

שימוש חוזר בזוגות שם משתמש/סיסמה גנובים מפריצה אחת כדי לנסות לגשת לשירותים אחרים, במיוחד כשאנשים השתמשו שוב בסיסמאות [3].

### Q5: האם אפשר לפרוץ למנהלי סיסמאות?

כן. רבים משתמשים בהצפנה בלי ידע (zero-knowledge), כך שפריצה לשרת חושפת רק כספות מוצפנות, אך סיסמאות ראשיות חלשות עדיין עלולות להיפרץ במצב לא מקוון.

# נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק D)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

### Q6: מהי התקפת מילון?

וריאציה של כוח גס שבודקת מילים נפוצות, ביטויים וסיסמאות שדלפו בעבר, ולא אותיות אקראיות.

### Q7: מדוע ביטויי סיסמה (passphrases) מועדפים?

ביטויי סיסמה משתמשים במספר מילים אקראיות, ויוצרים אנטרופיה גבוהה שקל לבני אדם לזכור אך יקר חישובית לפצח [1].

### Q8: כיצד כניסה יחידה (SSO) משפיעה על דליפות סיסמאות?

SSO מצמצם את שפע הסיסמאות, אך ספק הזהות הופך ליעד בעל ערך גבוה שזקוק ל-MFA חזק, רצוי עמיד לפישינג [6].

### Q9: מהי חטיפת הפעלה (session hijacking)?

תוקף משיג או מנצל לרעה אסימון הפעלה תקף כדי להתחזות למשתמש מחובר בלי צורך בסיסמה נוספת [5].

### Q10: כיצד מזהים password spraying?

על ידי חיפוש אחר אותן סיסמאות מועטות המנוסות על פני חשבונות רבים, לעיתים באיטיות כדי להישאר מתחת לספי הנעילה [7].

# חלק 11: 10 עובדות ותובנות מהעולם האמיתי על אבטחת סייבר

עיינו בעובדות מהעולם האמיתי על פריצות אבטחה, מנגנוני הגנה ותקני ציות.

### 1. תובנות על אבטחה

NIST SP 800-63B דורש לבדוק סיסמאות חדשות מול רשימות חסימה של סיסמאות נפוצות ופרוצות [1].

### 2. תובנות על אבטחה

הדליפה 'Collection #1' מ-2019 מיזגה נתונים מפרצות קודמות רבות לקובץ ענק אחד של צמדי דוא"ל וסיסמה [8].

### 3. תובנות על אבטחה

NIST דורש כעת שסיסמאות המשמשות כגורם האימות היחיד יהיו באורך של 15 תווים לפחות [1].

### 4. תובנות על אבטחה

חומרת ASIC יכולה לחשב מיליארדי גיבובי SHA-256 בשנייה, ולכן גיבוב SHA גולמי אינו בטוח לסיסמאות משתמשים [2].

### 5. תובנות על אבטחה

מלחים ייחודיים פירושם ששני משתמשים עם אותה סיסמה בדיוק מקבלים גיבובים שונים במסד הנתונים [2].

### 6. תובנות על אבטחה

מנהלי סיסמאות רבים מצפינים את נתוני הכספת באופן מקומי באמצעות הצפנה חזקה הנגזרת מהסיסמה הראשית של המשתמש.

### 7. תובנה על אבטחה

Credential Stuffing עובד מפני שאנשים רבים משתמשים באותה סיסמה בחשבונות מסחר אלקטרוני, בנקאות ודוא"ל [3].

### 8. תובנה על אבטחה

NIST SP 800-63B קובע שגורמי האימות לא ידרשו החלפת סיסמאות תקופתית, אלא רק לאחר עדות לפריצה [1].

### 9. תובנה על אבטחה

הוספת אות גדולה אחת וסמל אחד לסיסמה קצרה אינה עוצרת התקפות מילון אוטומטיות מודרניות מבוססות GPU [1].

### 10. תובנות על אבטחה

MFA יכול לחסום ניסיונות רבים של מילוי אישורים (credential stuffing) גם לאחר דליפת סיסמה; MFA עמיד לפישינג חזק יותר מקודי SMS [3].

# מקורות והפניות טכניים

מדריך הלימוד והפאזלים האינטראקטיביים נערכו על סמך תקנים גלובליים של NIST, OWASP ותאימות לפרטיות נתונים.

## מקורות אקדמיים ותעשייתיים

[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/

## מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

**1 שאלה 1** — **תשובה נכונה: A**

### הערה למורה

Credential stuffing משתמש באוטומציה כדי לנסות צמדי שם משתמש/סיסמה שדלפו באתרים אחרים [3].

**2 שאלה 2** — **תשובה נכונה: A**

### הערה למורה

OWASP ממליצה קודם על Argon2id; bcrypt מיועד בעיקר למערכות ישנות שבהן Argon2id או scrypt אינם זמינים [2].

**3 שאלה 3** — **תשובה נכונה: A**

### הערה למורה

אימות רב-שלבי דורש גורם נוסף, ולכן סיסמה גנובה לבדה אינה יכולה לפתוח את החשבון [3].

**4 שאלה 4** — **תשובה נכונה: A**

### הערה למורה

מאגרי פריצה (breach dumps) הם אוספים של פרטי גישה שדלפו, כגון האוסף Collection #1 מ-2019 [8].

**5 שאלה 5** — **תשובה נכונה: A**

### הערה למורה

מנהל סיסמאות מייצר ושומר סיסמה ייחודית וחזקה לכל חשבון, ומונע שימוש חוזר [3].

## מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

**שאלה 6** — **תשובה נכונה: נכון**

### הערה למורה

נכון: סיסמאות שנעשה בהן שימוש חוזר מאפשרות לתוקפים להשתמש בפרטי גישה שדלפו מאתר אחד באתרים אחרים [3].

**שאלה 7** — **תשובה נכונה: לא נכון**

### הערה למורה

לא נכון: SHA-1 הוא גיבוב מהיר; OWASP ממליצה במקומו על Argon2id, scrypt, bcrypt או PBKDF2 [2].

**שאלה 8** — **תשובה נכונה: לא נכון**

### הערה למורה

לא נכון: כללי מורכבות לבדם אינם יכולים לעצור stuffing עם סיסמאות שדלפו ונעשה בהן שימוש חוזר; נדרש אימות רב-שלבי [3].

**שאלה 9** — **תשובה נכונה: נכון**

### הערה למורה

נכון: שירותי ניטור מחפשים במאגרי פריצה ובמקורות הרשת האפלה פרטי גישה חשופים [8].

**שאלה 10** — **תשובה נכונה: נכון**

### הערה למורה

נכון: מלח (salt) ייחודי לכל סיסמה הופך טבלאות קשת (rainbow tables) מחושבות מראש ללא יעילות [2].

# מפתחות אוצר מילים ומחוון הערכה

**מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 6 נקודות).**

## נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

| | | | |
|---|---|---|---|
| F 1. מילוי אישורים | H 2. bcrypt | D 3. פריצה | G 4. הוספת מלח |
| C 5. מנהל | B 6. MFA | A 7. קשת | E 8. פישינג |

## נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

| | | | |
|---|---|---|---|
| 1 מילוי | 2 bcrypt | 3 פריצה | 4 המלחה |
| 5 מנהל | 6 רב גורמי | | |

## נקודת ביקורת 6 – פעילות חלופית: מפתח תשובות – התאמת אוצר מילים

| | | | |
|---|---|---|---|
| 1 H – פישינג | 2 C – פריצה | 3 B – בקריפט | 4 G – טבלתקשת |
| 5 A – מילוי | 6 D – המלחה | 7 E – מנהל | 8 F – רבגורמי |

### הערות לדיון עבור מורים

**מונחי מפתח:**
ודאו שהתלמידים מסבירים במילים שלהם את מילוי אישורים, bcrypt ו-פריצה ונותנים דוגמה לכל אחד מהם.

**מקרי בוחן:**
בקשו מהתלמידים לבסס את ההמלצות שלהם על עובדות מדף העבודה ולא על דעות.

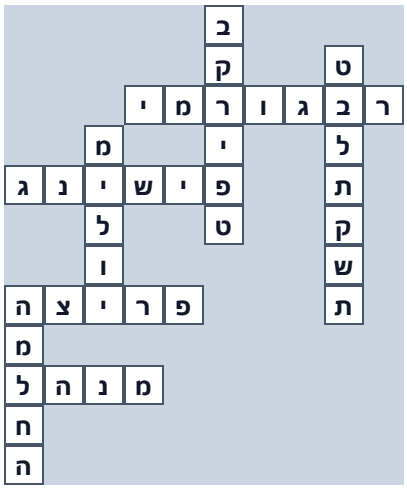
**הערכת מקורות:**
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

# מפתחות פאזלים והערות למורה

## פתרון תפזורת

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ת | כ | ר | ט | ד | ט | ס | ה | א | ק | ע | מ | ת | ט | ח |
| כ | ס | ל | ו | ח | ע | מ | מ | ג | כ | נ | ו | ש | פ | נ |
| ב | ח | י | ד | פ | י | ע | ל | צ | ג | מ | נ | ר | י | נ |
| ט | פ | ר | י | ל | ש | ט | ח | י | ש | מ | ג | ב | ר | א |
| נ | פ | י | ו | ל | ל | ח | ה | ד | ר | ט | כ | ס | ק | ד |
| ו | ר | י | פ | פ | ע | ס | ט | ס | ב | כ | כ | ו | ב | נ |
| ת | י | ע | ד | ק | ב | ב | ג | ז | ע | ב | נ | ע | ב | ג |
| ד | צ | ל | ג | ת | ל | ז | ט | ה | ו | ק | ת | ג | צ | נ |
| י | ה | ד | ל | ת | ת | א | ב | צ | ר | ב | נ | ר | ס | י |
| ד | כ | ס | ק | ס | ג | ח | ז | ה | מ | ד | מ | ד | א | ש |
| מ | ס | ש | א | א | ה | ק | ס | ה | י | ע | ת | ע | ח | י |
| ש | ת | ל | ג | ע | פ | ע | ט | נ | מ | ש | פ | נ | ל | פ |
| ח | ו | י | ש | ש | ת | ס | א | נ | ח | ר | ר | ע | ה | ב |
| מ | א | ת | ז | ס | נ | ז | ה | מ | פ | כ | כ | ט | ס | כ |
| מ | ט | ו | ת | כ | ז | ל | ב | ש | ע | ש | ב | צ | ו | צ |

## פתרון תשבץ



## מדריך למורה לפתרונות התשבץ

### מאוזן

**3 מאוזן: רבגורמי** בדיקת כניסה ברמות אימות מרובות (7 אותיות)

**5 מאוזן: פישינג** הנדסה חברתית לגניבת כניסות (6 אותיות)

**6 מאוזן: פריצה** חשיפה בלתי מורשית של מסד נתונים (5 אותיות)

**8 מאוזן: מנהל** כלי לאחסון אישורים (4 אותיות)

### מאונך

**1 מאונך: בקריפט** אלגוריתם גיבוב סיסמאות איטי (6 אותיות)

**2 מאונך: טבלתקשת** טבלה מחושבת מראש של גיבובי סיסמאות (7 אותיות)

**4 מאונך: מילוי** בדיקת אישורים שדלפו (5 אותיות)

**7 מאונך: המלחה** הוספת מלח אקראי לגיבוב סיסמה (5 אותיות)

# מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

### מפתח פענוח מילים מבולבלות

1. ולמיי — **מילוי**
2. פהציר — **פריצה**
3. למהנ — **מנהל**
4. תבקתשטל — **טבלתקשת**
5. ירטבפק — **בקריפט**
6. חהלהמ — **המלחה**
7. רמריבוג — **רבגורמי**
8. שגפניי — **פישינג**

**מפתח אתגר הצופן הסודי**

**"אבטחו סיסמאות שדלפו בכניסה מרובת גורמים"**

# מפתח תשובות למקרי הבוחן

## A מקרה בוחן 1: טיפול בדליפת אישורי גישה ארגוניים

פתרון למורה

### הנחיות הערכה

### תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: שירות ניטור הרשת האפלה מתריע בפני ארגון שקובץ dump של מסד נתונים המכיל סיסמאות של מנהלי מערכת ארגוניים פורסם ברשת.
- אסטרטגיה ופתרון מומלצים: בטלו את כל הפעלות המנהל הפעילות ואפסו את פרטי ההתחברות באמצעות מחולל בעל אנטרופיה גבוהה. אכפו MFA עמיד לפישינג בפורטלי הניהול [6], החליפו מפתחות API שנפגעו, בדקו יומני התחברות, אתרו את החשיפה הראשונית ובדקו חשבונות מורשים אחרים.

## B מקרה בוחן 2: הטמעת תקני גיבוב סיסמאות

פתרון למורה

### הנחיות הערכה

### תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: מסד נתונים ארגוני שומר כעת סיסמאות משתמשים באמצעות גיבובי MD5 מיושנים ללא salt קריפטוגרפי, ולכן הם חשופים לחילוץ מהיר.
- אסטרטגיה ופתרון מומלצים: אמצו את Argon2id (או bcrypt במערכות ישנות) עם salt ייחודי לכל משתמש [2]. עטפו את גיבובי ה-MD5 הקיימים באלגוריתם החדש כעת, בצעו גיבוב מחדש ישירות בכניסה הבאה של כל משתמש, ואלצו איפוס עבור חשבונות לא פעילים זמן רב.