الاسم: _____ التاريخ: _____ الدرجة: _____

تسريبات كلمات المرور وأمان بيانات الاعتماد

حشو بيانات الاعتماد، واختراقات البيانات، وخوارزميات التجزئة، والمصادقة متعددة العوامل، وأمان كلمات المرور.

نظرة عامة على التعلّم: تسريبات كلمات المرور

مرحبًا! ترشدك حزمة الأنشطة هذه عبر تسرّب كلمات المرور وأمان بيانات الاعتماد. ستستكشف حشو بيانات الاعتماد وخروقات البيانات وخوارزميات التجزئة والمصادقة متعددة العوامل ومديري كلمات المرور.

نقاط التحقق في ورقة العمل

- [ ] **الجزء 1-4: أتقن الأمن السيبراني ومنع التهديدات.**
- [ ] **الجزء 5-7: حل الكلمات المتقاطعة وألغاز البحث عن الكلمات.**
- [ ] **الجزء 8-9: حل دراسات الحالة وتحدي الشيفرة.**
- [ ] **الجزء 10: راجع صفحات الأسئلة الشائعة الأساسية والمتقدمة.**
- [ ] **الجزء 11: استكشف 10 حقائق مثيرة من الواقع.**
- [ ] **إضافي: تحدّي فكّر بسرعة**

مؤمَّن
تشفير البيانات
معيار AES بطول 256 بت

متوافق
المعايير العالمية
أطر GDPR وCCPA

انعدام الثقة
سياسة الوصول
المصادقة متعددة العوامل

افتح دليل VPN.com للأمن السيبراني

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

خارطة طريقك لتعلّم أمان كلمات المرور

- افهم مخاطر انكشاف بيانات الاعتماد في منتديات الشبكة المظلمة.
- طبّق المصادقة متعددة العوامل (MFA) ومراقبة بيانات الاعتماد المخترَقة.
- صمّم دفاعات أمنية للشركات ضد عمليات الاحتيال الموجّهة بالهندسة الاجتماعية.

تعليمات دليل تسريبات كلمات المرور

أجب عن أسئلة الاختيار من متعدد وأسئلة صحيح/خطأ، وأكمل الجمل الناقصة باستخدام بنك الكلمات، وطابق التعريفات، وحُلّ الكلمات المتقاطعة وبحث الكلمات. طبّق معرفتك على حماية بيانات الاعتماد. واختم بالنشاط الإضافي «فكّر بسرعة».

تسريبات كلمات المرور وأمان بيانات الاعتماد (مقدمة)

تكشف تسريبات كلمات المرور بيانات اعتماد المستخدمين على مواقع الويب العامة والمظلمة. وتقلل كلمات المرور الفريدة من مدير كلمات المرور، وفحص كلمات المرور المخترقة، والمصادقة متعددة العوامل (MFA) من خطر حشو بيانات الاعتماد، بينما يحد التجزئة البطيئة المملّحة لكلمات المرور من الضرر إذا سُرقت قاعدة بيانات كلمات المرور.

اقرأ كل نقطة تحقق بعناية، ثم اختر الإجابة الصحيحة أو اكتبها.

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما هو حشو بيانات الاعتماد؟
   - A. استخدام الأتمتة لاختبار تركيبات اسم المستخدم/كلمة المرور المسرّبة عبر مواقع متعددة
   - B. تشفير ملفات تخزين قواعد البيانات المحلية
   - C. إغراق خوادم الويب بطلبات حركة الشبكة
   - D. مراقبة مدخلات لوحة المفاتيح سرًّا

2. أي خوارزمية تدرجها OWASP كخيارها الأول لتخزين كلمات المرور اليوم؟
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. كيف تخفف المصادقة متعددة العوامل (MFA) من خطر تسريب كلمات المرور؟
   - A. تتطلب عامل تحقق إضافيًا، لذا فإن كلمة مرور مسروقة وحدها لا تكفي
   - B. تغير كلمة المرور تلقائيًا كل ساعة
   - C. تشفّر اسم المستخدم أثناء الإرسال
   - D. تنبه مكتب الائتمان إلى الطلبات الاحتيالية

4. ما هو تفريغ بيانات الاختراق؟
   - A. مجموعة من بيانات اعتماد المستخدمين المسرّبة منشورة على الإنترنت أو تُباع في منتديات المخترقين
   - B. نسخة احتياطية من ملفات قاعدة البيانات مخزّنة خارج الموقع
   - C. ذاكرة مؤقتة لسجلات خادم الويب
   - D. أداة إدارية تُستخدم لإعادة تعيين كلمات مرور المستخدمين

5. ما دور مدير كلمات المرور؟
   - A. إنشاء كلمات مرور فريدة وقوية لكل حساب وتخزينها
   - B. مراقبة حركة مرور الشبكة بحثًا عن تسريبات كلمات المرور
   - C. حظر هجمات القوة الغاشمة الآلية عند البوابة
   - D. فحص كتل تخزين قاعدة البيانات بحثًا عن كلمات مرور غير مشفرة

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. تؤدي إعادة استخدام كلمات المرور عبر عدة حسابات إلى زيادة خطر حشو بيانات الاعتماد.

صحيح خطأ

7 سؤال 7

7. SHA-1 دالة تجزئة موصى بها لتخزين كلمات المرور الحديثة.

صحيح خطأ

8 سؤال 8

8. فرض تعقيد كلمة المرور وحده (دون MFA) يوقف حشو بيانات الاعتماد تمامًا.

صحيح خطأ

9 سؤال 9

9. تفحص أدوات مراقبة الويب المظلم الإنترنت بحثًا عن بيانات اعتماد الشركات المخترقة.

صحيح خطأ

10 سؤال 10

10. تضيف التجزئات المملّحة بيانات عشوائية فريدة إلى كلمات المرور قبل التجزئة لإحباط هجمات جداول قوس القزح.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

اقرأ كل جملة أدناه وأكمل الفراغ بالمصطلح الصحيح من بنك الكلمات.

1. يسمى اختبار بيانات الاعتماد المسربة عبر تطبيقات ويب عديدة _____ بيانات الاعتماد.
2. خوارزمية تجزئة كلمات المرور البطيئة والتكيفية التي لا تزال OWASP تقبلها هي _____ .
3. يعد كشف ملفات قواعد البيانات السرية على الإنترنت _____ للبيانات.
4. تسمى إضافة قيم عشوائية إلى كلمات المرور قبل التجزئة _____ .
5. قاعدة البيانات المحلية الآمنة لبيانات اعتماد المستخدم هي _____ كلمات المرور.
6. تستخدم إضافة خطوة ثانية للتحقق عند الدخول _____ .

بنك كلمات المفردات

اختراق | التمليح | المصادقة متعددة العوامل | بيكريبت | حشو | قوس قزح | مدير | bcrypt

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

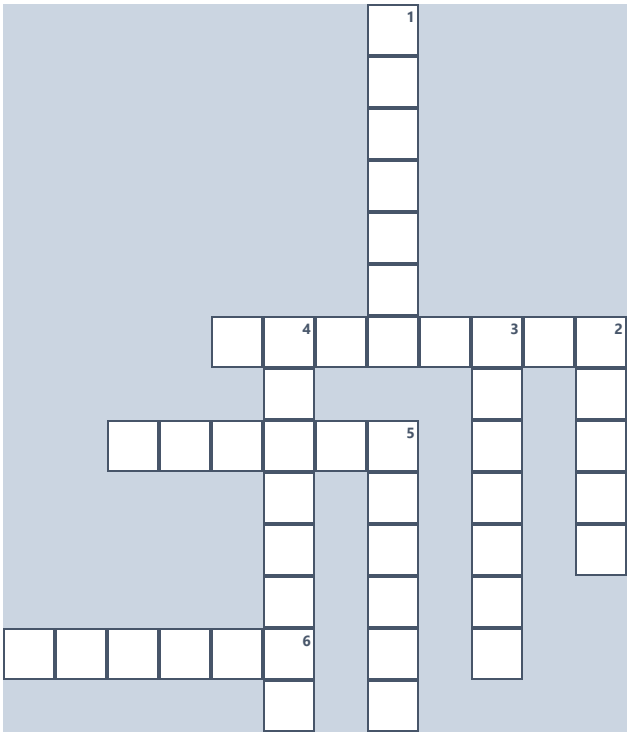
مطابقة التعريفات

طابق كل مصطلح مفردات على اليمين مع تعريفه الصحيح على اليسار بكتابة الحرف المقابل (A-H) في مربع الإدخال القابل للتعبئة.

1. الحشو	A	جدول محسوب مسبقًا لتجزئات كلمات المرور.
2. bcrypt	B	فحص تسجيل دخول متعدد العوامل.
3. الاختراق	C	أداة تخزين بيانات الاعتماد.
4. التمليح	D	كشف غير مصرح به لقاعدة بيانات.
5. المدير	E	هندسة اجتماعية لسرقة بيانات تسجيل الدخول.
6. MFA	F	اختبار بيانات الاعتماد المسرّبة.
7. قوس قزح	G	إضافة ملح عشوائي إلى تجزئة كلمة المرور.
8. التصيّد الاحتيالي	H	خوارزمية تجزئة بطيئة لكلمات المرور.

نقطة التحقق 5: لغز الكلمات المتقاطعة

حلّ الكلمات المتقاطعة بكتابة الحروف في المربعات البيضاء النشطة. تتوافق الأرقام مع الدلائل أدناه.



أفقي

2. كشف غير مصرح به لقاعدة بيانات (8)

5. أداة لتخزين بيانات الاعتماد (6)

6. جدول محسوب مسبقا لتجزئات كلمات المرور (6)

عمودي

1. خوارزمية بطيئة لتجزئة كلمات المرور (7)

2. اختبار بيانات الاعتماد المسربة (5)

3. إضافة قيمة ملح عشوائية إلى تجزئة كلمة المرور (7)

4. فحص تسجيل دخول متعدد العوامل (8)

5. هندسة اجتماعية لسرقة بيانات الدخول (6)

نقطة التحقق 5 – نشاط بديل: أدلة الكلمات المتقاطعة الميسَّرة

يمكن لمستخدمي قارئ الشاشة ولوحة المفاتيح كتابة إجابات الكلمات المتقاطعة مباشرة في حقول النص أدناه.

أفقي

2 أفقي: كشف غير مصرح به لقاعدة بيانات (8 حروف):

5 أفقي: أداة لتخزين بيانات الاعتماد (6 حروف):

6 أفقي: جدول محسوب مسبقا لتجزئات كلمات المرور (6 حروف):

عمودي

1 عمودي: خوارزمية بطيئة لتجزئة كلمات المرور (7 حروف):

2 عمودي: اختبار بيانات الاعتماد المسربة (5 حروف):

3 عمودي: إضافة قيمة ملح عشوائية إلى تجزئة كلمة المرور (7 حروف):

4 عمودي: فحص تسجيل دخول متعدد العوامل (8 حروف):

5 عمودي: هندسة اجتماعية لسرقة بيانات الدخول (6 حروف):

نقطة التحقق 6: البحث عن الكلمة المخفية

ابحث عن 8 مصطلحات مفردات رئيسية مخبأة في الشبكة أدناه. يمكن أن تكون الكلمات أفقية أو رأسية أو قطرية.

د	ق	د	س	ت	ل	ز	د	ع	ك	ط	ق	ي	ك	ف
ت	ن	ي	م	م	ح	س	ا	ب	ا	ب	ت	ف	خ	
س	ش	س	خ	س	ي	ن	ش	ج	ل	ك	ط	س	ج	ز
ع	ع	ت	ح	ز	ق	س	و	ق	ش	م	ك	ق	ر	ط
ط	ك	ل	ل	م	ا	ن	ن	ر	ت	م	د	ق	ف	ز
ح	ل	ا	ب	و	ل	ج	ب	م	و	ة	ه	ي	ت	ة
ي	و	د	ش	ر	ا	ة	ج	ي	ع	ش	ج	ك	ر	ي
ل	ق	ت	ن	ب	خ	ا	ة	ع	ك	ج	ح	س	ا	ج
م	ف	ج	ح	ر	ت	ز	ج	ل	ك	ر	ط	ل	ح	ز
ت	ل	ة	م	ح	ر	ك	ه	ح	ا	ا	ي	ك	ا	ف
ل	ا	ل	م	س	ا	د	ق	ة	ع	ق	ن	ب	ي	ك
ا	ش	ل	ن	ل	ق	ت	ع	خ	ب	د	ل	ي	ت	و
س	ا	ل	ة	خ	خ	ص	د	ز	ط	ك	ش	ط	ط	م
ف	ر	ق	ك	ر	ة	ا	ف	ه	د	ه	ب	خ	ل	خ
ب	ر	ط	ة	ر	ش	ف	ق	ع	ي	ت	ط	ة	خ	د

قائمة كلمات المفردات

الحشو بيكربيت الاختراق التمليح المدير المصادقة قوسقزح التصيد

نقطة التحقق 6 – نشاط بديل: مطابقة المفردات الميسَّرة

طابق كل مصطلح من المصطلحات الـ 8 في البحث عن الكلمات مع تعريفه الصحيح بكتابة الحرف (A-H) في الفراغ.

مصطلحات المفردات
A. الحشو
B. بيكربيت
C. الاختراق
D. التمليح
E. المدير
F. المصادقة
G. قوسقزح
H. التصيد

التعريفات وحقول المطابقة
1. هندسة اجتماعية لسرقة بيانات الدخول.
2. كشف غير مصرح به لقاعدة بيانات.
3. خوارزمية بطيئة لتجزئة كلمات المرور.
4. جدول محسوب مسبقا لتجزئات كلمات المرور.
5. اختبار بيانات الاعتماد المسربة.
6. إضافة قيمة ملح عشوائية إلى تجزئة كلمة المرور.
7. أداة لتخزين بيانات الاعتماد.
8. فحص تسجيل دخول متعدد العوامل.

نقطة التحقق 7: تحدي الكلمات المبعثرة

أعد ترتيب الحروف أدناه للكشف عن المفاهيم والمصطلحات الأساسية في الأمن السيبراني. اكتب إجاباتك في مربعات الإدخال المخصصة.

1. ش ح ا و ل _____
2. خ ا ق ل ا ر ت ا _____
3. ا م د ر ي ل _____
4. ح ق س ز ق و _____
5. ي ت ر ك ب ب ي _____
6. ي ت ل ا م ح ل _____
7. ا ة ا د ق ل ص م _____
8. ت د ا ي ص ل _____

نشاط إضافي: فكّر بسرعة

اكتب 3 إجابات لكل فئة. يفوز أول من يكمل القائمة.

1	عادات آمنة يمكنك البدء بها اليوم		
2	قواعد لكلمة مرور قوية		
3	مديرو كلمات المرور الذين تعرفهم		
4	أدوات أمنية تعرفها		
5	علامات تحذيرية في البريد الإلكتروني		
6	كلمات ممتعة لعبارة مرور طويلة		
7	طرق لتسجيل الدخول بدون كلمة مرور		
8	معلومات لا ينبغي أن تشاركها أبدًا		
9	أسباب لتحديث البرامج		
10	أشياء تفعلها عند تسرّب كلمة مرور		
11	حسابات تحتاج إلى المصادقة متعددة العوامل (MFA)		
12	أماكن لا ينبغي تخزين كلمات المرور فيها أبدًا		
13	علامات إصابة الحاسوب		
14	كلمات مرور سيئة يستخدمها الناس		
15	أشياء تحتفظ بنسخة احتياطية منها		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: معالجة تسرب بيانات الاعتماد في المؤسسات



السيناريو: تنبّه خدمة مراقبة الشبكة المظلمة مؤسسة إلى أن تسريبًا لقاعدة بيانات تحتوي على كلمات مرور مديري أنظمة الشركة قد نُشر على الإنترنت.

سؤال للنقاش: حلّل مخاطر تسريب بيانات الاعتماد، واقترح استراتيجية لإعادة التعيين الإدارية.

دراسة الحالة 2: تطبيق معايير تجزئة كلمات المرور



السيناريو: تخزّن قاعدة بيانات مؤسسية حاليًا كلمات مرور المستخدمين باستخدام تجزئات MD5 قديمة دون ملح تشفيري، مما يجعلها عرضة للاستخراج السريع.

سؤال للنقاش: صمّم استراتيجية ترحيل لترقية خوارزمية التجزئة في قاعدة البيانات.

نقطة التحقق 9: فك الشيفرة

يحمي متخصص الأمن السيبراني أصول الشبكة من الجهات التهديدية عبر الإنترنت. استخدم مفتاح الحرف إلى الرقم أدناه لفك تشفير الرسالة بكتابة الحروف المطابقة في الفراغات.

مفتاح التشفير من الحرف إلى الرقم

ا=1 ب=2 ت=3 ث=4 ج=5 ح=6 خ=7 د=8 ذ=9 ر=10 ز=11

س=12 ش=13 ص=14 ض=15 ط=16 ظ=17 ع=18 غ=19 ف=20 ق=21 ك=22

ل=23 م=24 ن=25 هـ=26 و=27 ي=28 ة=29 ى=30 ء=31 ؤ=32 ئ=33

10	27	10	24	23	1		3	1	24	23	22		25	24	1

29	21	8	1	14	24	2		29	2	10	12	24	23	1

29	8	8	18	3	24

الرسالة بعد فك التشفير:

نصيحة: يمثل كل رقم حرفًا عربيًا واحدًا من المفتاح أعلاه.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء A)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q1: ما تسريب كلمة المرور؟

يحدث تسرب كلمات المرور عندما تنكشف بيانات تسجيل دخول المستخدمين عبر اختراقات البيانات أو أخطاء تهيئة الخوادم.

Q2: كيف يعثر المخترقون على كلمات المرور المسرّبة؟

يفحص المخترقون منتديات الويب المظلم وتسريبات قواعد البيانات العامة ومواقع اللصق التي تُنشر فيها بيانات الاختراقات [8].

Q3: هل إعادة استخدام كلمة المرور خطيرة؟

نعم، لأنه إذا اختُرق موقع واحد، يمكن للمخترقين تجربة بيانات الاعتماد نفسها عبر آلاف المنصات الأخرى [3].

Q4: ما الملح التشفيري (cryptographic salt)؟

الملح بيانات عشوائية تُضاف إلى كلمة المرور قبل التجزئة، مما يجعل هجمات البحث المحسوبة مسبقًا غير فعالة [2].

Q5: لماذا أصبح MD5 قديمًا؟

MD5 دالة تجزئة سريعة وقديمة للأغراض العامة، لذا يستطيع المهاجمون اختبار تخمينات كلمات المرور بسرعة كبيرة جدًا، خاصةً عندما تكون التجزئات بلا ملح [2].

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء B)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: كيف يحمي مدير كلمات المرور المستخدمين؟

يولّد تلقائيًا بيانات اعتماد معقدة وفريدة لكل موقع، ما يقلل أخطاء الذاكرة البشرية وإعادة الاستخدام.

Q7: ما هجوم القوة الغاشمة؟

هجوم يختبر بانتظام كل تركيبة أحرف ممكنة إلى أن يُعثر على كلمة المرور الصحيحة [4].

Q8: كيف يفيد قفل الحساب؟

يبطئ القفل أو تحديد المعدل محاولات التخمين المتكررة عبر الإنترنت، ومع المراقبة والمصادقة متعددة العوامل (MFA) يقلل خطر هجمات القوة الغاشمة [4].

Q9: هل كلمات المرور الرئيسية آمنة؟

تكون آمنة إذا كانت عبارات مرور عالية الإنتروبيا لا يُعاد استخدامها أبدًا في أنظمة ويب أخرى.

Q10: هل يجب تغيير كلمات المرور بانتظام؟

يقول NIST ألا يُفرض التغيير الدوري؛ بل يُغيَّر عند ظهور دليل على الاختراق مع إعطاء الأولوية للطول وقوائم الحظر والمصادقة متعددة العوامل (MFA) [1].

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء C)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q1: كيف تُقارن Argon2 بـ bcrypt؟

تدرج OWASP خوارزمية Argon2id خيارًا أول لها؛ وتقاوم إعداداتها كثيفة الذاكرة هجمات الكسر بوحدات GPU وASIC بصورة أفضل من bcrypt [2].

Q2: ما تمديد المفاتيح (key stretching)؟

تقنية تكرّر خوارزمية التجزئة آلاف المرات لإبطاء عملية التحقق من كلمة المرور، مما يجعل الكسر مكلفًا [2].

Q3: كيف تعمل الجداول القوس قزحية (rainbow tables)؟

هي جداول بحث محسوبة مسبقًا تربط كلمات المرور النصية بقيم تجزئتها، وتُستخدم لعكس التجزئات غير المملحة بسرعة [2].

Q4: ما إعادة تدوير بيانات الاعتماد؟

إعادة استخدام أزواج اسم المستخدم/كلمة المرور المسروقة من اختراق واحد لمحاولة الوصول إلى خدمات أخرى، خصوصًا حيث أعاد الناس استخدام كلمات المرور [3].

Q5: هل يمكن اختراق مديري كلمات المرور؟

نعم. يستخدم كثير منها تشفير المعرفة الصفرية، لذا لا يكشف اختراق الخادم سوى خزائن مشفّرة، لكن كلمات المرور الرئيسية الضعيفة قد تظل قابلة للكسر دون اتصال.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء D)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q6: ما هجوم القاموس؟

صيغة من القوة الغاشمة تختبر الكلمات والعبارات الشائعة وكلمات المرور المسرّبة تاريخيًا بدلًا من الأحرف العشوائية.

Q7: لماذا تُفضَّل عبارات المرور؟

تستخدم عبارات المرور عدة كلمات عشوائية، ما يوفر عشوائية عالية يسهل على البشر تذكرها لكن كسرها مكلف حسابيًا [1].

Q8: كيف يؤثر تسجيل الدخول الموحد (SSO) في تسرب كلمات المرور؟

يقلل SSO من تشتت كلمات المرور، لكن مزود الهوية يصبح هدفًا عالي القيمة يحتاج إلى مصادقة متعددة العوامل قوية، ويفضل أن تكون مقاومة للتصيّد الاحتيالي [6].

Q9: ما اختطاف الجلسة؟

يحصل مهاجم على رمز جلسة صالح أو يسيء استخدامه لانتحال شخصية مستخدم مسجَّل الدخول دون الحاجة إلى كلمة المرور مجددًا [5].

Q10: كيف تكتشف هجمات رش كلمات المرور؟

بالبحث عن كلمات المرور القليلة نفسها المجرَّبة عبر حسابات كثيرة، وغالبًا ببطء للبقاء دون عتبات القفل [7].

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

يشترط NIST SP 800-63B فحص كلمات المرور الجديدة مقابل قوائم حظر لكلمات المرور الشائعة والمخترقة [1].

2. نظرة على الأمن

دمج تسريب 'Collection #1' لعام 2019 بيانات من اختراقات سابقة كثيرة في ملف ضخم واحد من أزواج البريد الإلكتروني وكلمة المرور [8].

3. نظرة على الأمن

يشترط NIST الآن ألا يقل طول كلمات المرور المستخدمة عامل مصادقة وحيدًا عن 15 حرفًا [1].

4. نظرة على الأمن

تستطيع عتاد ASIC حساب مليارات تجزئات SHA-256 في الثانية، مما يجعل تجزئة SHA الخام غير آمنة لكلمات مرور المستخدمين [2].

5. نظرة على الأمن

تعني الأملاح الفريدة أن مستخدمَين بكلمة المرور نفسها تمامًا يحصلان على تجزئتين مختلفتين في قاعدة البيانات [2].

6. نظرة على الأمن

تشفّر كثير من مديري كلمات المرور بيانات الخزنة محليًا بتشفير قوي مشتق من كلمة المرور الرئيسية للمستخدم.

7. رؤية حول الأمان

ينجح حشو بيانات الاعتماد لأن كثيرًا من الناس يعيدون استخدام كلمة المرور نفسها في حسابات التجارة الإلكترونية والخدمات المصرفية والبريد الإلكتروني [3].

8. رؤية حول الأمان

يذكر NIST SP 800-63B أن جهات التحقق يجب ألا تشترط تغيير كلمات المرور دوريًا، بل فقط بعد ظهور دليل على الاختراق [1].

9. رؤية حول الأمان

إضافة حرف كبير ورمز واحد إلى كلمة مرور قصيرة لا توقف هجمات القواميس الآلية الحديثة المعتمدة على GPU [1].

10. نظرة على الأمن

يمكن للمصادقة متعددة العوامل (MFA) أن تحجب كثيرًا من محاولات حشو بيانات الاعتماد حتى بعد تسرب كلمة المرور؛ والمصادقة متعددة العوامل المقاومة للتصيّد الاحتيالي أقوى من رموز الرسائل النصية SMS [3].

المراجع والمصادر التقنية

أُعد دليل الدراسة والألغاز التفاعلية استنادًا إلى معايير NIST وOWASP العالمية ومعايير الامتثال لخصوصية البيانات.

المراجع الأكاديمية والصناعية

[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/

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

يستخدم حشو بيانات الاعتماد الأتمتة لتجربة أزواج اسم المستخدم/كلمة المرور المسرّبة على مواقع أخرى [3].

2 السؤال 2 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

توصي OWASP بـ Argon2id أولًا؛ أما bcrypt فهي أساسًا للأنظمة القديمة التي لا يتوفر فيها Argon2id أو scrypt [2].

3 السؤال 3 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

تتطلب MFA عاملًا إضافيًا، لذا لا تستطيع كلمة مرور مسروقة وحدها فتح الحساب [3].

4 السؤال 4 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

مجموعات التسريب (Breach dumps) هي مجموعات بيانات اعتماد مسرّبة، مثل تجميعة Collection #1 لعام 2019 [8].

5 السؤال 5 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

يولّد مدير كلمات المرور كلمة مرور فريدة وقوية لكل حساب ويخزنها، مما يمنع إعادة استخدامها [3].

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

صحيح: تتيح كلمات المرور المعاد استخدامها للمهاجمين إعادة تشغيل بيانات الاعتماد المسرّبة من موقع على مواقع أخرى [3].

7 السؤال 7

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: SHA-1 تجزئة سريعة؛ وتوصي OWASP بدلًا من ذلك بـ Argon2id أو scrypt أو bcrypt أو PBKDF2 [2].

8 السؤال 8

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: لا تستطيع قواعد التعقيد وحدها إيقاف الحشو بكلمات المرور المسرّبة المعاد استخدامها؛ والمطلوب MFA [3].

9 السؤال 9

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

صحيح: تبحث خدمات المراقبة في مجموعات التسريب ومصادر الشبكة المظلمة عن بيانات الاعتماد المكشوفة [8].

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

صحيح: ملح فريد لكل كلمة مرور يجعل جداول قوس قزح المحسوبة مسبقًا غير فعالة [2].

مفاتيح المفردات ومعيار التقييم

معيار التصحيح للمعلم: امنح 1 نقطة لكل مطابقة صحيحة (المجموع 8 نقطة) ولكل مصطلح سياق (المجموع 6 نقطة).

نقطة التحقق 4: مفتاح الإجابة – مطابقة المفاهيم

F 1. الحشو	H 2. bcrypt	D 3. الاختراق	G 4. التمليح
C 5. المدير	B 6. MFA	A 7. قوس قزح	E 8. التصيّد الاحتيالي

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 حشو	2 bcrypt	3 اختراق	4 التمليح
5 مدير	6 المصادقة متعددة العوامل		

نقطة التحقق 6 – نشاط بديل: مفتاح الإجابة – مطابقة المفردات

1 H – التصيد	2 C – الاختراق	3 B – بيكربيت	4 G – قوسقزح
5 A – الحشو	6 D – التمليح	7 E – المدير	8 F – المصادقة

ملاحظات النقاش للمعلمين

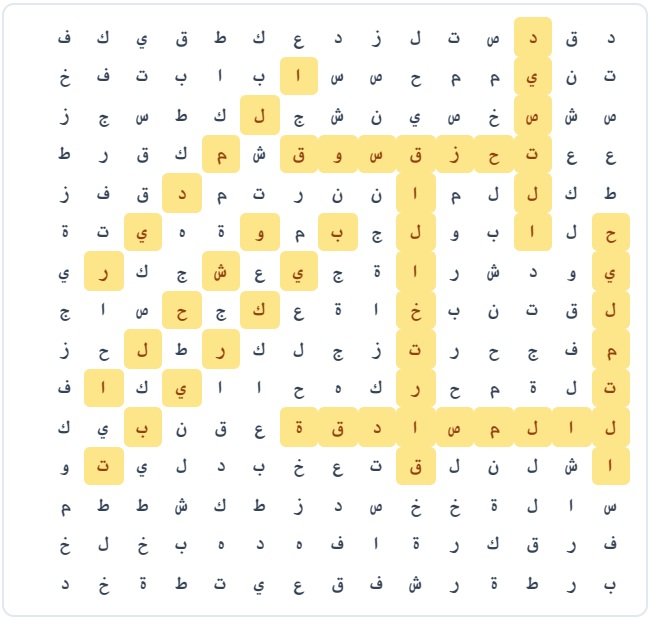
المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح الحشو وbcryptوالاختراق بكلماتهم الخاصة وإعطاء مثال على كل منها.

دراسات الحالة:
اطلب من الطلاب أن يدعموا توصياتهم بحقائق من ورقة العمل لا بآرائهم.

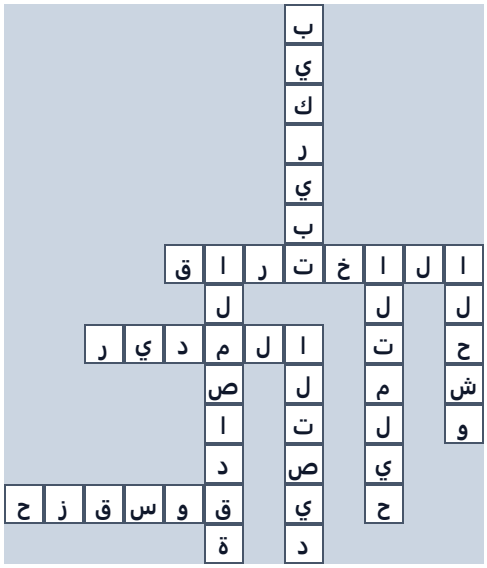
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات



حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

2 أفقي: الاختراق كشف غير مصرح به لقاعدة بيانات (8 حروف)

5 أفقي: المدير أداة لتخزين بيانات الاعتماد (6 حروف)

6 أفقي: قوسقزح جدول محسوب مسبقا لتجزئات كلمات المرور (6 حروف)

عمودي

1 عمودي: بيكربيت خوارزمية بطيئة لتجزئة كلمات المرور (7 حروف)

2 عمودي: الحشو اختبار بيانات الاعتماد المسربة (5 حروف)

3 عمودي: التمليح إضافة قيمة ملح عشوائية إلى تجزئة كلمة المرور (7 حروف)

4 عمودي: المصادقة فحص تسجيل دخول متعدد العوامل (8 حروف)

5 عمودي: التصيد هندسة اجتماعية لسرقة بيانات الدخول (6 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. شحاول — **الحشو**
2. خاقلارتا — **الاختراق**
3. امدريل — **المدير**
4. حقسزقو — **قوسقزح**
5. يتركببي — **بيكريبت**
6. يتلامحل — **التمليح**
7. اةادقلصم — **المصادقة**
8. تدايصل — **التصيد**

مفتاح تحدي الشيفرة السرية

"أمن كلمات المرور المسربة بمصادقة متعددة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: معالجة تسرب بيانات الاعتماد في المؤسسات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تنبّه خدمة مراقبة الويب المظلم مؤسسة إلى أن نسخة من قاعدة بيانات تحتوي على كلمات مرور مسؤولي أنظمة الشركة قد نُشرت على الإنترنت.
- الاستراتيجية والحل الموصى بهما: ألغِ جميع جلسات المسؤولين النشطة وأعد تعيين بيانات الاعتماد باستخدام مولّد عالي العشوائية. وفرض مصادقة متعددة العوامل مقاومة للتصيّد الاحتيالي على بوابات المسؤولين [6]، وبدّل مفاتيح API المتأثرة، وراجع سجلات تسجيل الدخول، وحدد نقطة التعرض الأولى وافحص الحسابات المميزة الأخرى.

B دراسة الحالة 2: تطبيق معايير تجزئة كلمات المرور

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تخزّن قاعدة بيانات في مؤسسة كلمات مرور المستخدمين حاليًا باستخدام تجزئات MD5 قديمة دون ملح تشفيري، مما يجعلها عرضة للاستخراج السريع.
- الاستراتيجية والحل الموصى بهما: اعتمد Argon2id (أو bcrypt على الأنظمة القديمة) مع ملح فريد لكل مستخدم [2]. غلِّف قيم MD5 المخزنة حاليًا بالخوارزمية الجديدة الآن، وأعد التجزئة مباشرةً عند تسجيل دخول كل مستخدم التالي، وافرض إعادة تعيين كلمات المرور للحسابات الخاملة منذ مدة طويلة.