نام: _____ تاریخ: _____ نمبر: _____

پاس ورڈ لیکس اور اسناد کی سیکیورٹی

کریڈینشل اسٹفنگ، ڈیٹا کی خلاف ورزیاں، ہیش الگورتھمز، ملٹی فیکٹر توثیق، اور پاس ورڈ سیکیورٹی۔

پاس ورڈ لیکس سیکھنے کا جائزہ

محفوظ شدہ
ڈیٹا کی خفیہ کاری
256 بٹ AES معیار

تعمیل شدہ
عالمی معیارات
GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ
رسائی کی پالیسی
ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو پاس ورڈ لیکس اور اسناد کی سیکیورٹی سے متعارف کراتا ہے۔ آپ کریڈینشل اسٹفنگ، ڈیٹا کی خلاف ورزیوں، ہیشنگ الگورتھمز، ملٹی فیکٹر تصدیق، اور پاس ورڈ مینیجرز کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- ☐ **حصہ 1-4: سائبر سیکیورٹی اور خطرات سے بچاؤ میں مہارت حاصل کریں۔**
- ☐ **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- ☐ **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- ☐ **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- ☐ **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- ☐ **اضافی: تیزی سے سوچیں چیلنج**

VPN.com سائبر سیکیورٹی گائیڈ کھولیں

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

آپ کا پاس ورڈ سیکیورٹی لرننگ روڈ میپ

- ڈارک ویب فورمز پر اسناد کے افشا کے خطرات کو سمجھیں۔
- ملٹی فیکٹر تصدیق (MFA) اور متاثرہ اسناد کی نگرانی نافذ کریں۔
- ہدف بنائے گئے سوشل انجینئرنگ فراڈز کے خلاف کارپوریٹ سیکیورٹی دفاع ڈیزائن کریں۔

پاس ورڈ لیکس گائیڈ ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو اسناد کے تحفظ پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

پاس ورڈ لیکس اور اسناد کی سیکیورٹی (تعارف)

پاس ورڈ لیکس عوامی اور ڈارک ویب سائٹس پر صارفین کی اسناد ظاہر کر دیتے ہیں۔ پاس ورڈ مینیجر سے بنائے گئے منفرد پاس ورڈز، لیک شدہ پاس ورڈز کی جانچ اور ملٹی فیکٹر تصدیق (MFA) اسناد اسٹفنگ کا خطرہ کم کرتے ہیں، جبکہ سالٹ شدہ، سست پاس ورڈ ہیشنگ پاس ورڈ ڈیٹا بیس چوری ہونے کی صورت میں نقصان کو محدود کرتی ہے۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1 1. کریڈینشل اسٹفنگ کیا ہے؟

- A. متعدد سائٹس پر لیک شدہ یوزر نیم/پاس ورڈ کے امتزاج کو آزمانے کے لیے آٹومیشن استعمال کرنا
- B. مقامی ڈیٹا بیس اسٹوریج فائلوں کو خفیہ کرنا
- C. ویب سرورز کو نیٹ ورک ٹریفک کی درخواستوں سے مغلوب کرنا
- D. کی بورڈ ان پٹس کی خفیہ نگرانی کرنا

2 2. OWASP آج پاس ورڈز محفوظ کرنے کے لیے کس الگورتھم کو اپنی پہلی ترجیح کے طور پر درج کرتا ہے؟

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

3 3. ملٹی فیکٹر تصدیق (MFA) پاس ورڈ لیکس کے خطرے کو کیسے کم کرتی ہے؟

- A. یہ ایک اضافی تصدیقی عنصر کا تقاضا کرتی ہے، اس لیے صرف چوری شدہ پاس ورڈ کافی نہیں ہوتا
- B. یہ پاس ورڈ ہر گھنٹے خودکار طور پر تبدیل کر دیتی ہے
- C. یہ ترسیل کے دوران یوزر نیم کو خفیہ کرتی ہے
- D. یہ کریڈٹ بیورو کو جعلی درخواستوں سے آگاہ کرتی ہے

4 4. ڈیٹا بریچ ڈمپ کیا ہے؟

- A. آن لائن شائع کی گئی یا ہیکر فورمز پر بیچی گئی لیک شدہ صارف اسناد کا مجموعہ
- B. ڈیٹا بیس فائلوں کی بیک اپ کاپی جو آف سائٹ محفوظ ہو
- C. ویب سرور لاگز کا عارضی کیش
- D. ایک ایڈمنسٹریٹو ٹول جو صارف کے پاس ورڈز ری سیٹ کرنے کے لیے استعمال ہوتا ہے

5 5. پاس ورڈ مینیجر کا کردار کیا ہے؟

- A. ہر اکاؤنٹ کے لیے منفرد، مضبوط پاس ورڈز بنانا اور محفوظ رکھنا
- B. پاس ورڈ لیکس کے لیے نیٹ ورک ٹریفک کی نگرانی کرنا
- C. گیٹ وے پر خودکار بروٹ فورس حملوں کو روکنا
- D. غیر خفیہ شدہ پاس ورڈز کے لیے ڈیٹا بیس اسٹوریج بلاکس کو اسکین کرنا

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. متعدد اکاؤنٹس میں پاس ورڈ دوبارہ استعمال کرنے سے کریڈینشل اسٹفنگ کا خطرہ بڑھ جاتا ہے۔

○ درست ○ غلط

7 سوال 7

7. SHA-1 جدید پاس ورڈ اسٹوریج کے لیے تجویز کردہ ہیشنگ فنکشن ہے۔

○ درست ○ غلط

8 سوال 8

8. صرف پاس ورڈ کی پیچیدگی نافذ کرنا (MFA کے بغیر) کریڈینشل اسٹفنگ کو مکمل طور پر روک دیتا ہے۔

○ درست ○ غلط

9 سوال 9

9. ڈارک ویب مانیٹرنگ ٹولز انٹرنیٹ کو اسکین کر کے سمجھوتا شدہ کارپوریٹ اسناد تلاش کرتے ہیں۔

○ درست ○ غلط

10 سوال 10

10. نمک لگے ہیشز رینبو ٹیبل حملوں کو ناکام بنانے کے لیے ہیشنگ سے پہلے پاس ورڈز میں منفرد بے ترتیب ڈیٹا شامل کرتے ہیں۔

○ درست ○ غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. متعدد ویب ایپلی کیشنز میں لیک شدہ اسناد کو آزمانا کریڈنشل _____ ہے۔
2. OWASP کی جانب سے اب بھی قابل قبول ایک سست، ایڈاپٹیو پاس ورڈ ہیشنگ الگورتھم _____ ہے۔
3. انٹرنیٹ پر خفیہ ڈیٹابیس فائلوں کا انکشاف ڈیٹا کی _____ ہے۔
4. ہیشنگ سے پہلے پاس ورڈز میں بے ترتیب قدریں شامل کرنا _____ کہلاتا ہے۔
5. صارف کی اسناد کے لیے محفوظ مقامی ڈیٹابیس پاس ورڈ _____ ہے۔
6. دوسرا لاگ اِن تصدیقی مرحلہ شامل کرنے میں _____ استعمال ہوتا ہے۔

الفاظ کا بینک

اسٹفنگ ایم ایف اے بی کرپٹ خلاف ورزی رین بو سالٹنگ فشنگ منیجر

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

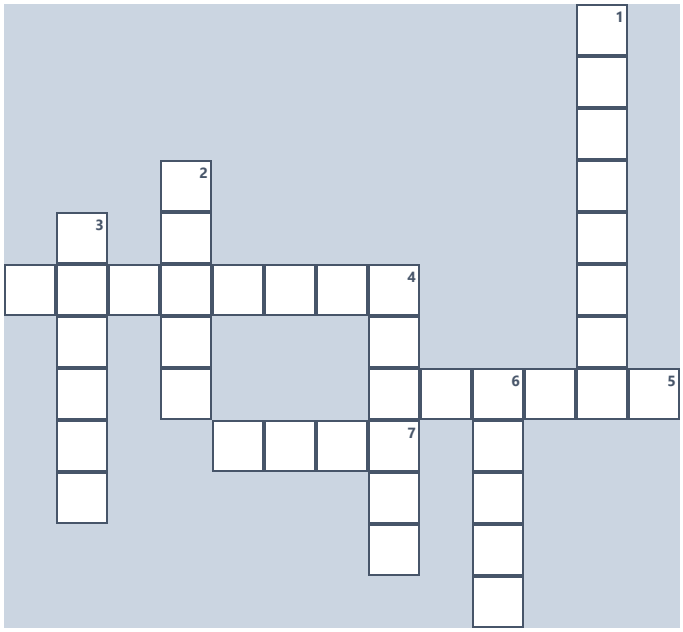
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. اسٹفنگ	A	پاس ورڈ ہیشز کی پہلے سے حساب شدہ ٹیبل۔
2. bcrypt	B	ملٹی فیکٹر لاگ اِن کی جانچ۔
3. بریچ	C	کریڈینشل اسٹوریج ٹول۔
4. سالٹنگ	D	غیر مجاز ڈیٹا بیس کا افشا۔
5. مینیجر	E	لاگ اِنز چرانے کے لیے سوشل انجینئرنگ۔
6. MFA	F	لیک شدہ اسناد کی جانچ کرنا۔
7. رین بو	G	پاس ورڈ ہیش میں بے ترتیب سالٹ شامل کرنا۔
8. فشنگ	H	سست پاس ورڈ ہیشنگ الگورتھم۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

4. کثیر عنصری لاگ اِن چیک (8)

5. پاس ورڈ ہیشنگ کا سست الگورتھم (6)

7. لاگ اِن چرانے کے لیے سوشل انجینئرنگ (4)

عمودی

1. ڈیٹابیس کا غیر مجاز انکشاف (8)

2. اسناد محفوظ کرنے کا ٹول (5)

3. پاس ورڈ ہیش میں بے ترتیب نمک (سالٹ) شامل کرنا (6)

4. لیک شدہ اسناد کی جانچ (6)

6. پاس ورڈ ہیشز کی پہلے سے تیار شدہ جدول (5)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

4 افقی: کثیر عنصری لاگ اِن چیک (8 حروف):

5 افقی: پاس ورڈ ہیشنگ کا سست الگورتھم (6 حروف):

7 افقی: لاگ اِن چرانے کے لیے سوشل انجینئرنگ (4 حروف):

عمودی

1 عمودی: ڈیٹابیس کا غیر مجاز انکشاف (8 حروف):

2 عمودی: اسناد محفوظ کرنے کا ٹول (5 حروف):

3 عمودی: پاس ورڈ ہیش میں بے ترتیب نمک (سالٹ) شامل کرنا (6 حروف):

4 عمودی: لیک شدہ اسناد کی جانچ (6 حروف):

6 عمودی: پاس ورڈ ہیشز کی پہلے سے تیار شدہ جدول (5 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ت	ت	ز	چ	ل	س	ن	گ	ا	ت	ہ	ب	ش	ٹ	م
ت	ر	م	ٹ	گ	ٹ	م	ن	ک	و	د	چ	ک	پ	ا
و	گ	ز	د	د	ن	ی	ف	ر	چ	ا	ز	و	ر	ب
چ	ف	م	ز	ی	ک	ف	ٹ	ر	ت	ر	م	ا	ک	ے
م	ر	ک	چ	ن	گ	ج	س	د	خ	ن	پ	ش	ی	ل
ر	ی	ر	س	ٹ	و	و	ا	ہ	ل	پ	گ	م	ب	ف
ر	ن	س	خ	ل	پ	ی	ب	ا	ا	ب	ف	ش	ن	گ
د	ب	ت	ر	ک	م	م	ت	س	ف	ہ	ف	س	خ	ن
و	و	ن	م	ا	ک	ک	چ	ل	و	م	س	ک	ک	ٹ
ت	ے	ب	ی	ن	د	گ	م	و	ر	ب	چ	ہ	ہ	ل
ک	ت	ف	ز	چ	س	ج	ے	ز	ز	پ	ی	ز	و	ا
س	ا	ت	گ	ز	ا	ب	ی	ب	ی	ل	ف	ن	ت	س
ے	ن	د	ٹ	ک	م	ن	ت	د	چ	ٹ	ت	گ	ت	ا
م	ف	ہ	ل	ک	ل	ن	ا	ا	ٹ	ے	ن	ٹ	و	ز
ن	ا	ر	ف	ف	ن	ج	ب	خ	ک	پ	و	ہ	ن	ر

الفاظ کی فہرست

اسٹفنگ بیکرپٹ خلافورزی سالٹنگ منیجر ایمایفاے رینبو فشنگ

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. اسٹفنگ
B. بیکرپٹ
C. خلافورزی
D. سالٹنگ
E. منیجر
F. ایمایفاے
G. رینبو
H. فشنگ

تعریفیں اور ملان کے خانے
1. لاگ اِن چرانے کے لیے سوشل انجینئرنگ۔
2. ڈیٹابیس کا غیر مجاز انکشاف۔
3. پاس ورڈ ہیشنگ کا سست الگورتھم۔
4. پاس ورڈ ہیشز کی پہلے سے تیار شدہ جدول۔
5. لیک شدہ اسناد کی جانچ۔
6. پاس ورڈ ہیش میں بے ترتیب نمک (سالٹ) شامل کرنا۔
7. اسناد محفوظ کرنے کا ٹول۔
8. کثیر عنصری لاگ اِن چیک۔

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

سائبر سیکیورٹی کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ٹ ا ف ن گ س
2. ف خ ی ل ز ر و ا
3. ی م ر چ ن
4. ن و ب ر ی
5. ر ک ٹ ب پ ی
6. ن ٹ س ل گ ا
7. ا ے ی ف ا ی ا م
8. ف گ ن ش

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1	محفوظ عادات جو آپ آج شروع کر سکتے ہیں		
2	مضبوط پاس ورڈ کے اصول		
3	آپ کے جانے پہچانے پاس ورڈ مینیجرز کے نام		
4	آپ کے جانے پہچانے سیکیورٹی ٹولز کے نام		
5	ای میل میں انتباہی علامات		
6	طویل پاس فریز کے لیے دلچسپ الفاظ		
7	پاس ورڈ کے بغیر لاگ ان کرنے کے طریقے		
8	وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں		
9	سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات		
10	پاس ورڈ لیک ہونے پر کرنے کے کام		
11	وہ اکاؤنٹس جنہیں MFA کی ضرورت ہے		
12	وہ مقامات جہاں پاس ورڈ کبھی محفوظ نہیں کرنے چاہئیں		
13	کمپیوٹر کے متاثر ہونے کی علامات		
14	وہ کمزور پاس ورڈ جو لوگ استعمال کرتے ہیں		
15	وہ چیزیں جن کا آپ بیک اپ لیتے ہیں		

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: انٹرپرائز کریڈینشلز کے لیک کا ازالہ



منظرنامہ: ڈارک ویب مانیٹرنگ سروس ایک ادارے کو خبردار کرتی ہے کہ کارپوریٹ سسٹم ایڈمنسٹریٹر کے پاس ورڈز پر مشتمل ڈیٹا بیس ڈمپ آن لائن شائع ہو گیا ہے۔

بحث کا سوال: کریڈینشلز لیک کے خطرات کا تجزیہ کریں، اور ایڈمنسٹریٹو ری سیٹ کی حکمت عملی تجویز کریں۔

کیس اسٹڈی 2: پاس ورڈ ہیشنگ کے معیارات نافذ کرنا



منظرنامہ: ایک انٹرپرائز ڈیٹا بیس اس وقت صارفین کے پاس ورڈز کرپٹوگرافک سالٹ کے بغیر پرانے MD5 ہیشز کے ذریعے محفوظ کرتا ہے، جس سے وہ تیزی سے نکالے جانے کے خطرے میں ہیں۔

بحث کا سوال: ڈیٹا بیس کے ہیشنگ الگورتھم کو اپ گریڈ کرنے کی مائیگریشن حکمت عملی ڈیزائن کریں۔

چیک پوائنٹ 9: سائفر حل کریں

سائبر سیکیورٹی پیشہ ور نیٹ ورک اثاثوں کو آن لائن خطرات پیدا کرنے والوں سے بچاتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

16	12	14	34	18	1	3		38	18		14	5	28	37	26		37	5	30	31

33	37	14	28		23	34	26	9	31

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ A)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q1: پاس ورڈ لیک کیا ہے؟

پاس ورڈ لیک اس وقت ہوتا ہے جب ڈیٹا کی خلاف ورزیوں یا سرور کی غلط ترتیب کے ذریعے صارف کی لاگ اِن اسناد ظاہر ہو جائیں۔

Q2: ہیکرز لیک شدہ پاس ورڈز کیسے تلاش کرتے ہیں؟

ہیکرز ڈارک ویب فورمز، عوامی ڈیٹا بیس ڈمپس اور پیسٹ سائٹس کو اسکین کرتے ہیں جہاں خلاف ورزی کا ڈیٹا شائع کیا جاتا ہے [8]۔

Q3: کیا پاس ورڈ دوبارہ استعمال کرنا خطرناک ہے؟

جی ہاں، کیونکہ اگر ایک سائٹ سے سمجھوتہ ہو جائے تو ہیکرز انہی اسناد کو ہزاروں دوسرے پلیٹ فارمز پر آزما سکتے ہیں [3]۔

Q4: کرپٹوگرافک سالٹ کیا ہے؟

سالٹ بے ترتیب ڈیٹا ہے جو ہیشنگ سے پہلے پاس ورڈ میں شامل کیا جاتا ہے اور پہلے سے تیار شدہ تلاش کے حملوں کو غیر مؤثر بنا دیتا ہے [2]۔

Q5: MD5 متروک کیوں ہے؟

MD5 ایک تیز، متروک عمومی مقصد کا ہیش ہے، اس لیے حملہ آور پاس ورڈ کے اندازے بہت تیزی سے آزما سکتے ہیں، خاص طور پر جب ہیشز میں سالٹ نہ ہو [2]۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ B)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q6: پاس ورڈ مینیجر صارفین کا تحفظ کیسے کرتا ہے؟

یہ ہر سائٹ کے لیے پیچیدہ، منفرد اسناد خود بخود بناتا ہے، جس سے انسانی یادداشت کی غلطیاں اور دوبارہ استعمال کم ہوتے ہیں۔

Q7: بروٹ فورس حملہ کیا ہے؟

حملہ جو درست پاس ورڈ ملنے تک ہر ممکن حروف کے امتزاج کو منظم طریقے سے آزماتا ہے [4]۔

Q8: اکاؤنٹ لاک آؤٹ کیسے مدد کرتا ہے؟

لاک آؤٹ یا ریٹ لمٹنگ بار بار آن لائن اندازے لگانے کو سست کرتی ہے اور، مانیٹرنگ اور MFA کے ساتھ مل کر، بروٹ فورس کا خطرہ کم کرتی ہے [4]۔

Q9: کیا ماسٹر پاس ورڈ محفوظ ہوتے ہیں؟

یہ اس صورت میں محفوظ ہیں اگر یہ زیادہ اینٹروپی والے پاس فریزز ہوں جو دوسرے ویب سسٹمز پر کبھی دوبارہ استعمال نہ کیے جائیں۔

Q10: کیا پاس ورڈز باقاعدگی سے تبدیل کیے جانے چاہییں؟

NIST کہتا ہے کہ وقتاً فوقتاً تبدیلی پر مجبور نہ کریں؛ سمجھوتے کے ثبوت پر تبدیل کریں اور لمبائی، بلاک لسٹس اور MFA کو ترجیح دیں [1]۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ C)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: Argon2، bcrypt سے کیسے مختلف ہے؟

OWASP نے Argon2id کو اپنی پہلی ترجیح قرار دیا ہے؛ اس کی میموری ہارڈ سیٹنگز GPU اور ASIC کریکنگ کے خلاف bcrypt سے بہتر مزاحمت کرتی ہیں [2]۔

Q2: کی اسٹریچنگ کیا ہے؟

تکنیک جو ہیشنگ الگورتھم کو ہزاروں بار دہراتی ہے تاکہ پاس ورڈ کی تصدیق سست ہو اور اسے توڑنا مہنگا پڑے [2]۔

Q3: رین بو ٹیبلز کیسے کام کرتے ہیں؟

یہ پہلے سے حساب شدہ تلاش کے جدول ہیں جو سادہ متن پاس ورڈز کو ان کے ہیشز سے جوڑتے ہیں، اور بغیر سالٹ کے ہیشز کو جلدی الٹنے کے لیے استعمال ہوتے ہیں [2]۔

Q4: اسناد کی ری سائیکلنگ کیا ہے؟

ایک خلاف ورزی سے چوری ہوئے صارف نام/پاس ورڈ جوڑے دوبارہ استعمال کر کے دیگر سروسز تک رسائی کی کوشش کرنا، خاص طور پر جہاں لوگوں نے پاس ورڈ دہرائے ہوں [3]۔

Q5: کیا پاس ورڈ مینیجرز ہیک ہو سکتے ہیں؟

ہاں۔ بہت سے زیرو نالج خفیہ کاری استعمال کرتے ہیں، اس لیے سرور کی خلاف ورزی صرف خفیہ شدہ والٹس ظاہر کرتی ہے، لیکن کمزور ماسٹر پاس ورڈ پھر بھی آف لائن توڑے جا سکتے ہیں۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ D)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: ڈکشنری اٹیک کیا ہے؟

بروٹ فورس کی ایک قسم جو بے ترتیب حروف کے بجائے عام الفاظ، جملوں اور ماضی میں لیک شدہ پاس ورڈز کو آزماتی ہے۔

Q7: پاس فریزز کو ترجیح کیوں دی جاتی ہے؟

پاس فریزز متعدد بے ترتیب الفاظ استعمال کرتے ہیں، جس سے اعلیٰ اینٹروپی بنتی ہے جو انسانوں کے لیے یاد رکھنا آسان لیکن کریک کرنا حسابی طور پر مہنگا ہوتا ہے [1]۔

Q8: سنگل سائن آن (SSO) پاس ورڈ لیکس پر کیسے اثر ڈالتا ہے؟

SSO پاس ورڈز کے پھیلاؤ کو کم کرتا ہے، لیکن شناخت فراہم کنندہ ایک انتہائی قیمتی ہدف بن جاتا ہے جسے مضبوط، ترجیحاً فشنگ سے محفوظ MFA کی ضرورت ہوتی ہے [6]۔

Q9: سیشن ہائی جیکنگ کیا ہے؟

حملہ آور درست سیشن ٹوکن حاصل کرتا یا اس کا غلط استعمال کرتا ہے تاکہ دوبارہ پاس ورڈ کی ضرورت کے بغیر لاگ اِن صارف کی نقالی کر سکے [5]۔

Q10: آپ پاس ورڈ اسپرے کا پتا کیسے لگاتے ہیں؟

ایسے چند ہی پاس ورڈز دیکھ کر جو کئی اکاؤنٹس پر آزمائے جاتے ہیں، اکثر آہستہ آہستہ تاکہ لاک آؤٹ کی حدوں سے نیچے رہیں [7]۔

حصہ 11: 10 حقیقی دنیا کے سائبر سیکیورٹی حقائق اور بصیرتیں

سیکیورٹی خلاف ورزیوں، دفاعی نظاموں اور تعمیل کے معیارات کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. سیکیورٹی بصیرت

NIST SP 800-63B تقاضا کرتا ہے کہ نئے پاس ورڈز کو عام اور سمجھوتہ شدہ پاس ورڈز کی بلاک لسٹس کے خلاف جانچا جائے [1]۔

2. سیکیورٹی بصیرت

2019 کے 'Collection #1' ڈمپ نے کئی پرانی خلاف ورزیوں کا ڈیٹا ایک بہت بڑی فائل میں ملا دیا جس میں ای میل اور پاس ورڈ جوڑے تھے [8]۔

3. سیکیورٹی بصیرت

NIST اب تقاضا کرتا ہے کہ واحد تصدیقی عنصر کے طور پر استعمال ہونے والے پاس ورڈز کم از کم 15 حروف لمبے ہوں [1]۔

4. سیکیورٹی بصیرت

ASIC ہارڈ ویئر فی سیکنڈ اربوں SHA-256 ہیشز کا حساب لگا سکتا ہے، اس لیے خام SHA ہیشنگ صارف پاس ورڈز کے لیے غیر محفوظ ہے [2]۔

5. سیکیورٹی بصیرت

منفرد سالٹس کا مطلب ہے کہ بالکل ایک جیسا پاس ورڈ رکھنے والے دو صارفین کے ڈیٹا بیس ہیشز مختلف ہوتے ہیں [2]۔

6. سیکیورٹی بصیرت

کئی پاس ورڈ مینیجرز صارف کے ماسٹر پاس ورڈ سے اخذ کی گئی مضبوط کرپٹوگرافی کے ذریعے والٹ ڈیٹا کو مقامی طور پر خفیہ کرتے ہیں۔

7. سیکیورٹی کی بصیرت

کریڈینشل اسٹفنگ اس لیے کام کرتی ہے کہ بہت سے لوگ ای کامرس، بینکنگ اور ای میل اکاؤنٹس میں ایک ہی پاس ورڈ دوبارہ استعمال کرتے ہیں [3]۔

8. سیکیورٹی کی بصیرت

NIST SP 800-63B کہتا ہے کہ تصدیق کنندگان وقتاً فوقتاً پاس ورڈ کی تبدیلی لازمی نہیں کریں گے، صرف سمجھوتے کے ثبوت کے بعد تبدیلی کروائیں گے [1]۔

9. سیکیورٹی کی بصیرت

مختصر پاس ورڈ میں ایک بڑا حرف اور علامت شامل کرنے سے جدید خودکار GPU ڈکشنری حملے نہیں رکتے [1]۔

10. سیکیورٹی بصیرت

MFA پاس ورڈ لیک ہونے کے بعد بھی کریڈنشل اسٹفنگ کی کئی کوششوں کو روک سکتا ہے؛ فشنگ سے مزاحم MFA، SMS کوڈز سے زیادہ مضبوط ہے [3]۔

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی NIST، OWASP اور ڈیٹا پرائیویسی کمپلائنس معیارات سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[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/

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — درست جواب: **A**

تدریسی نوٹ

کریڈینشل اسٹفنگ آٹومیشن کے ذریعے دوسری سائٹس پر لیک شدہ یوزر نیم/پاس ورڈ جوڑوں کو آزماتی ہے [3]۔

2 سوال 2 — درست جواب: **A**

تدریسی نوٹ

OWASP سب سے پہلے Argon2id کی سفارش کرتا ہے؛ bcrypt بنیادی طور پر پرانے سسٹمز کے لیے ہے جہاں Argon2id یا scrypt دستیاب نہیں [2]۔

3 سوال 3 — درست جواب: **A**

تدریسی نوٹ

MFA ایک اضافی عنصر مانگتی ہے، اس لیے صرف چوری شدہ پاس ورڈ اکاؤنٹ کو ان لاک نہیں کر سکتا [3]۔

4 سوال 4 — درست جواب: **A**

تدریسی نوٹ

بریچ ڈمپس لیک شدہ کریڈینشلز کے مجموعے ہیں، جیسے 2019 کی Collection #1 تالیف [8]۔

5 سوال 5 — درست جواب: **A**

تدریسی نوٹ

پاس ورڈ مینیجر ہر اکاؤنٹ کے لیے منفرد، مضبوط پاس ورڈ بناتا اور محفوظ کرتا ہے، جس سے دوبارہ استعمال کی روک تھام ہوتی ہے [3]۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6 — درست جواب: درست

تدریسی نوٹ

درست: دوبارہ استعمال شدہ پاس ورڈز حملہ آوروں کو ایک سائٹ سے لیک شدہ کریڈینشلز دوسری سائٹس پر آزمانے دیتے ہیں [3]۔

7 سوال 7 — درست جواب: غلط

تدریسی نوٹ

غلط: SHA-1 ایک تیز ہیش ہے؛ OWASP اس کے بجائے Argon2id، scrypt، bcrypt یا PBKDF2 کی سفارش کرتا ہے [2]۔

8 سوال 8 — درست جواب: غلط

تدریسی نوٹ

غلط: صرف پیچیدگی کے اصول دوبارہ استعمال شدہ لیک شدہ پاس ورڈز کے ساتھ اسٹفنگ کو نہیں روک سکتے؛ MFA درکار ہے [3]۔

9 سوال 9 — درست جواب: درست

تدریسی نوٹ

درست: مانیٹرنگ سروسز بے نقاب کریڈینشلز کے لیے بریچ ڈمپس اور ڈارک ویب ذرائع کو تلاش کرتی ہیں [8]۔

10 سوال 10 — درست جواب: درست

تدریسی نوٹ

درست: ہر پاس ورڈ کے لیے منفرد سالٹ پہلے سے تیار شدہ رینبو ٹیبلز کو غیر مؤثر بنا دیتا ہے [2]۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

F 1. اسٹفنگ	H 2. bcrypt	D 3. بریچ	G 4. سالٹنگ
C 5. مینیجر	B 6. MFA	A 7. رین بو	E 8. فشنگ

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 اسٹفنگ	2 بی کرپٹ	3 خلاف ورزی	4 سالٹنگ
5 منیجر	6 ایم ایف اے		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 H – فشنگ	2 C – خلافورزی	3 B – بیکرپٹ	4 G – رینبو
5 A – اسٹفنگ	6 D – سالٹنگ	7 E – منیجر	8 F – ایمایفاے

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ اسٹفنگ، bcrypt اور بریچ کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

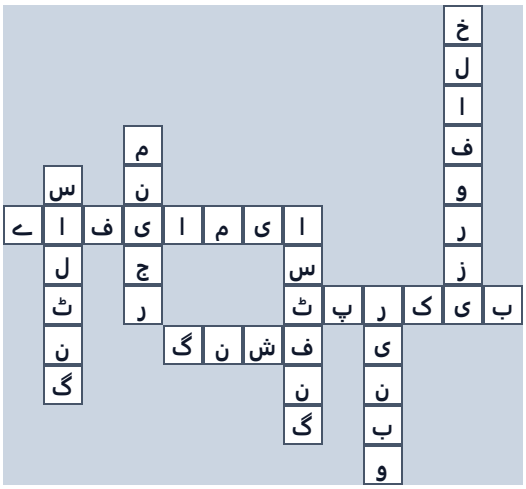
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

م	ٹ	ش	ب	ہ	ت	ا	گ	ن	س	ل	ج	ز	ت	ت
ا	پ	ک	چ	د	و	ک	ن	م	ٹ	گ	ٹ	م	ر	ت
ب	ر	و	ز	ا	چ	ر	ف	ی	ن	د	د	ز	گ	و
ے	ک	ا	م	ر	ت	ر	ٹ	ف	ک	ی	ز	م	ف	چ
ل	ی	ش	پ	ن	خ	د	س	ج	گ	ن	چ	ک	ر	م
ف	ب	م	گ	پ	ل	ہ	ا	و	و	ٹ	س	ر	ی	ر
گ	ن	ش	ف	ب	ا	ا	ی	پ	ل	خ	س	ن	ر	ر
ن	خ	س	ف	ہ	ف	س	م	ک	ر	ت	ب	ب	ر	د
ٹ	ک	س	م	و	ل	چ	ک	ک	م	ن	و	و	ن	و
ل	ہ	ہ	چ	ب	ر	و	م	گ	د	ن	ی	ب	ے	ت
ا	و	ز	ی	پ	ز	ے	چ	س	ج	ز	ف	ت	ک	ک
س	ت	ن	ف	ل	ی	ب	ی	ز	ا	ب	گ	ت	ا	س
ا	ت	گ	ٹ	ت	چ	د	ت	ن	م	ک	ٹ	د	ن	ے
ز	و	ٹ	ے	ن	ا	ا	ٹ	ل	ن	ک	ل	ہ	ف	م
ر	ن	ہ	و	پ	ک	خ	ب	چ	ن	ف	ف	ر	ا	ن

کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

4 افقی: ایمایفاے کثیر عنصری لاگ اِن چیک (8 حروف)

5 افقی: بیکرپٹ پاس ورڈ ہیشنگ کا سست الگورتھم (6 حروف)

7 افقی: فشنگ لاگ اِن چرانے کے لیے سوشل انجینئرنگ (4 حروف)

عمودی

1 عمودی: خلافورزی ڈیٹابیس کا غیر مجاز انکشاف (8 حروف)

2 عمودی: منیجر اسناد محفوظ کرنے کا ٹول (5 حروف)

3 عمودی: سالٹنگ پاس ورڈ ہیش میں بے ترتیب نمک (سالٹ) شامل کرنا (6 حروف)

4 عمودی: اسٹفنگ لیک شدہ اسناد کی جانچ (6 حروف)

6 عمودی: رینبو پاس ورڈ ہیشز کی پہلے سے تیار شدہ جدول (5 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. ٹافنگس — اسٹفنگ
2. فخیلزروا — خلافورزی
3. یمرجن — منیجر
4. نوبری — رینبو
5. رکٹیپی — بیکرپٹ
6. نٹسلگا — سالٹنگ
7. اےیفایام — ایمایفاے
8. فگنش — فشنگ

خفیہ سائفر چیلنج کی کلید

"ملٹی فیکٹر سے پاسورڈز محفوظ کریں"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: انٹرپرائز کریڈینشلز کے لیک کا ازالہ

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ڈارک ویب مانیٹرنگ سروس ایک ادارے کو الرٹ کرتی ہے کہ کارپوریٹ سسٹم ایڈمنسٹریٹر پاس ورڈز پر مشتمل ڈیٹا بیس ڈمپ آن لائن شائع ہو گیا ہے۔
- تجویز کردہ حکمت عملی اور حل: تمام فعال ایڈمنسٹریٹر سیشنز منسوخ کریں اور ہائی اینٹروپی جنریٹر سے اسناد ری سیٹ کریں۔ ایڈمن پورٹلز پر فشنگ سے محفوظ MFA نافذ کریں [6]، متاثرہ API کیز تبدیل کریں، لاگ اِن لاگز کا جائزہ لیں، ابتدائی نمائش تلاش کریں اور دیگر مراعات یافتہ اکاؤنٹس چیک کریں۔

B کیس اسٹڈی 2: پاس ورڈ ہیشنگ کے معیارات نافذ کرنا

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک انٹرپرائز ڈیٹا بیس فی الحال صارفین کے پاس ورڈز کو کرپٹوگرافک سالٹ کے بغیر پرانے MD5 ہیشز کی صورت میں محفوظ کرتا ہے، جس کی وجہ سے وہ تیزی سے نکالے جانے کے خطرے کا شکار ہیں۔
- تجویز کردہ حکمت عملی اور حل: ہر صارف کے لیے منفرد سالٹ کے ساتھ Argon2id (یا پرانے سسٹمز پر bcrypt) اپنائیں [2]۔ موجودہ MD5 ہیشز کو ابھی نئے الگورتھم میں لپیٹیں، ہر صارف کے اگلے لاگ ان پر براہ راست دوبارہ ہیش کریں، اور طویل عرصے سے غیر فعال اکاؤنٹس کے لیے ری سیٹ لازمی کریں۔