नाम: _____ दिनांक: _____ अंक: _____

पासवर्ड लीक और क्रेडेंशियल सुरक्षा

क्रेडेंशियल स्टफ़िंग, डेटा उल्लंघन, हैश एल्गोरिदम, बहु-कारक प्रमाणीकरण और पासवर्ड सुरक्षा।

पासवर्ड लीक सीखने का अवलोकन

सुरक्षित किया गया
डेटा एन्क्रिप्शन
256-बिट AES मानक

अनुपालक
वैश्विक मानक
GDPR और CCPA फ़्रेमवर्क

ज़ीरो-ट्रस्ट
एक्सेस नीति
मल्टी-फ़ैक्टर ऑथेंटिकेशन

स्वागत है! यह गतिविधि पैकेट आपको पासवर्ड लीक और क्रेडेंशियल सुरक्षा से परिचित कराता है। आप क्रेडेंशियल स्टफ़िंग, डेटा ब्रीच, हैशिंग एल्गोरिदम, मल्टी-फ़ैक्टर प्रमाणीकरण और पासवर्ड मैनेजर का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

- [ ] भाग 1-4: साइबर सुरक्षा और खतरों की रोकथाम में महारत हासिल करें।
- [ ] भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।
- [ ] भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।
- [ ] भाग 10: बुनियादी और उन्नत FAQ पेज देखें।
- [ ] भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।
- [ ] अतिरिक्त: झटपट सोचें चुनौती।

VPN.com साइबर सुरक्षा गाइड खोलें

URL: https://www.vpn.com/hi/saibhar-suraksha/passwords-leak/

आपका पासवर्ड सुरक्षा लर्निंग रोडमैप

- डार्क वेब फ़ोरम पर क्रेडेंशियल के उजागर होने के जोखिम को समझें।
- मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) और समझौता किए गए क्रेडेंशियल की निगरानी लागू करें।
- लक्षित सोशल इंजीनियरिंग घोटालों के विरुद्ध कॉर्पोरेट सुरक्षा बचाव तैयार करें।

पासवर्ड लीक गाइड निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को क्रेडेंशियल सुरक्षा पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

पासवर्ड लीक और क्रेडेंशियल सुरक्षा (परिचय)

पासवर्ड लीक से उपयोगकर्ता के क्रेडेंशियल सार्वजनिक और डार्क वेब साइटों पर उजागर हो जाते हैं। पासवर्ड मैनेजर के अनूठे पासवर्ड, लीक हुए पासवर्ड की जाँच और मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) क्रेडेंशियल स्टफ़िंग का जोखिम घटाते हैं, जबकि सॉल्ट के साथ धीमी पासवर्ड हैशिंग से पासवर्ड डेटाबेस चोरी होने पर नुकसान सीमित रहता है।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1. **1. क्रेडेंशियल स्टफ़िंग क्या है?**
   - A. कई साइटों पर लीक हुए यूज़रनेम/पासवर्ड संयोजनों को आज़माने के लिए ऑटोमेशन का उपयोग करना
   - B. स्थानीय डेटाबेस स्टोरेज फ़ाइलों को एन्क्रिप्ट करना
   - C. नेटवर्क ट्रैफ़िक अनुरोधों से वेब सर्वरों को ओवरलोड करना
   - D. कीबोर्ड इनपुट की चुपके से निगरानी करना

2. **2. OWASP आज पासवर्ड स्टोर करने के लिए किस एल्गोरिदम को अपनी पहली पसंद बताता है?**
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. **3. मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) पासवर्ड लीक के जोखिम को कैसे कम करता है?**
   - A. यह एक अतिरिक्त सत्यापन कारक माँगता है, इसलिए अकेला चोरी हुआ पासवर्ड काफ़ी नहीं होता
   - B. यह हर घंटे अपने-आप पासवर्ड बदल देता है
   - C. यह ट्रांसमिशन के दौरान यूज़रनेम को एन्क्रिप्ट करता है
   - D. यह धोखाधड़ी वाले अनुरोधों के बारे में क्रेडिट ब्यूरो को सचेत करता है

4. **4. डेटा ब्रीच डंप क्या है?**
   - A. लीक हुए उपयोगकर्ता क्रेडेंशियल का संग्रह, जो ऑनलाइन प्रकाशित होता है या हैकर फ़ोरम पर बेचा जाता है
   - B. डेटाबेस फ़ाइलों की बैकअप कॉपी जो ऑफ़साइट रखी जाती है
   - C. वेब सर्वर लॉग का अस्थायी कैश
   - D. उपयोगकर्ता पासवर्ड रीसेट करने के लिए उपयोग किया जाने वाला प्रशासनिक टूल

5. **5. पासवर्ड मैनेजर की भूमिका क्या है?**
   - A. हर खाते के लिए अनूठे, मज़बूत पासवर्ड बनाना और संग्रहीत करना
   - B. पासवर्ड लीक के लिए नेटवर्क ट्रैफ़िक की निगरानी करना
   - C. गेटवे पर स्वचालित ब्रूट-फ़ोर्स हमलों को रोकना
   - D. अनएन्क्रिप्टेड पासवर्ड के लिए डेटाबेस स्टोरेज ब्लॉक स्कैन करना

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. कई अकाउंट में पासवर्ड दोबारा इस्तेमाल करने से क्रेडेंशियल स्टफ़िंग का जोखिम बढ़ता है।

○ सही ○ गलत

7 प्रश्न 7

7. SHA-1 आधुनिक पासवर्ड स्टोरेज के लिए अनुशंसित हैशिंग फ़ंक्शन है।

○ सही ○ गलत

8 प्रश्न 8

8. केवल पासवर्ड जटिलता लागू करने (MFA के बिना) से क्रेडेंशियल स्टफ़िंग पूरी तरह रुक जाती है।

○ सही ○ गलत

9 प्रश्न 9

9. डार्क वेब मॉनिटरिंग टूल इंटरनेट को स्कैन करके समझौता हो चुके कॉर्पोरेट क्रेडेंशियल खोजते हैं।

○ सही ○ गलत

10 प्रश्न 10

10. सॉल्टेड हैश रेनबो टेबल हमलों को विफल करने के लिए हैश करने से पहले पासवर्ड में अद्वितीय रैंडम डेटा जोड़ते हैं।

○ सही ○ गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. पासवर्ड को अपठनीय कोड में बदलकर सहेजने की विधि _____ कहलाती है।
2. डार्क वेब पर लीक हुए पासवर्ड की लगातार जाँच करने वाली सेवा _____ कहलाती है।
3. लीक हुए डेटाबेस में आपका ईमेल मौजूद है या नहीं, इसकी _____ ऑनलाइन जाँच-सेवाएँ करती हैं।
4. हैश करने से पहले पासवर्ड में यादृच्छिक मान जोड़ना _____ कहलाता है।
5. संदिग्ध लॉगिन पर लगातार _____ रखने से खाते की चोरी जल्दी पकड़ में आती है।
6. ईमेल _____ ठगी वाले संदिग्ध संदेशों को इनबॉक्स तक पहुँचने से पहले रोक देती है।

शब्दावली शब्द-बैंक

निगरानी | फ़िल्टरिंग | मैनेजर | मॉनिटरिंग | सॉल्टिंग | स्कैनिंग | हैशिंग | MFA

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

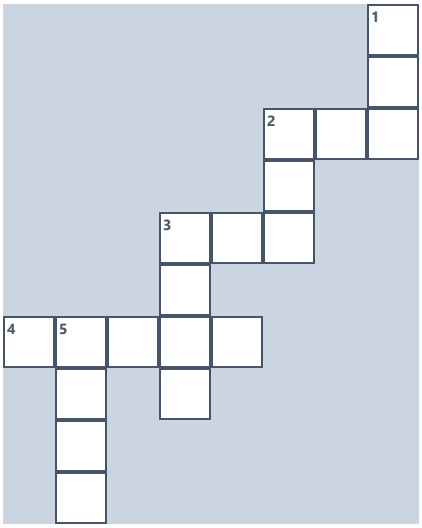
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. स्टफ़िंग**	**A**	पासवर्ड हैश की पहले से गणना की गई तालिका।
☐	**2. bcrypt**	**B**	मल्टी-फ़ैक्टर लॉगिन जाँच।
☐	**3. उल्लंघन**	**C**	क्रेडेंशियल स्टोरेज टूल।
☐	**4. सॉल्टिंग**	**D**	डेटाबेस का अनधिकृत रूप से उजागर होना।
☐	**5. मैनेजर**	**E**	लॉगिन चुराने के लिए सोशल इंजीनियरिंग।
☐	**6. MFA**	**F**	लीक हुए क्रेडेंशियल की जाँच करना।
☐	**7. रेनबो**	**G**	पासवर्ड हैश में यादृच्छिक सॉल्ट जोड़ना।
☐	**8. फ़िशिंग**	**H**	धीमा पासवर्ड हैशिंग एल्गोरिदम।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

2. संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच (3)

3. लॉगिन चुराने के लिए सोशल इंजीनियरिंग। (3)

4. किसी खाते या नेटवर्क पर लगातार नज़र रखकर गड़बड़ी पकड़ना (5)

ऊपर से नीचे

1. पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि (3)

2. लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी (3)

3. संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया (4)

5. किसी गतिविधि पर लगातार नज़र रखने की प्रक्रिया (4)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

बाएँ से दाएँ

2 बाएँ से दाएँ: संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच (3 अक्षर):

3 बाएँ से दाएँ: लॉगिन चुराने के लिए सोशल इंजीनियरिंग। (3 अक्षर):

4 बाएँ से दाएँ: किसी खाते या नेटवर्क पर लगातार नज़र रखकर गड़बड़ी पकड़ना (5 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि (3 अक्षर):

2 ऊपर से नीचे: लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी (3 अक्षर):

3 ऊपर से नीचे: संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया (4 अक्षर):

5 ऊपर से नीचे: किसी गतिविधि पर लगातार नज़र रखने की प्रक्रिया (4 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

ई म पि इ ठ दा ज द दि ते वी ति च ह री
रा व त सा स ई ते घ स्कै इ नी ल रि द जे
घ छ ई के द प ति के ट निं मि ट सा य च
ऊ ग नी जी इ त म पे ब प ग जि मी ने ले
इ शिं सी य छ मॉ र दे कि जा सा वा ड रे स
ख फ़ि नि फ ढ नि मा सॉ ना का रे दे सि मी क
पि ता ति ज श ट भ ऊ ल्टिं अ ऊ ए रि वि श
य वि व वा पा रिं ल च से ग कि य घ प के
की व सि री त ग की कि सि ना ने पा ते ण ए
ग ता सा मी न नी ऋ ले घ ति जि ला ए जी ले
मिं फ़ि ल्ट रिं ग ड ल द जे घ के च से दे है
स्कै री ए पी नि उ अ जे मि घ व आ च शिं मी
च ट थ फ ग ग ना सी का ज फ नी ग जी ता
ठ से लि ट रा आ इ से रा के री पा वा सि य
नि पि ने ख नी के वे ऊ ड नी दे दि भ आ नि

शब्दावली शब्द-सूची

सॉल्टिंग फ़िशिंग स्कैमिंग स्कैनिंग हैशिंग फ़िल्टरिंग मॉनिटरिंग निगरानी

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द
A. सॉल्टिंग
B. फ़िशिंग
C. स्कैमिंग
D. स्कैनिंग
E. हैशिंग
F. फ़िल्टरिंग
G. मॉनिटरिंग
H. निगरानी

परिभाषाएँ और मिलान फ़ील्ड
1. किसी गतिविधि पर लगातार नज़र रखने की प्रक्रिया।
2. लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी।
3. लॉगिन चुराने के लिए सोशल इंजीनियरिंग।
4. किसी खाते या नेटवर्क पर लगातार नज़र रखकर गड़बड़ी पकड़ना।
5. पासवर्ड हैश में यादृच्छिक सॉल्ट जोड़ना।
6. संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच।
7. पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि।
8. संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर साइबर सुरक्षा की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. **ल्टिं ग सॉ**
2. **ग मिं स्कै**
3. **ग शिं है**
4. **ट ग रिं मॉ नि**
5. **ग शिं फ़ि**
6. **निं ग स्कै**
7. **रिं फ़ि ग ल्ट**
8. **नि नी रा ग**

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
2	मज़बूत पासवर्ड के नियम			
3	आपके जाने-पहचाने पासवर्ड मैनेजर			
4	आपके जाने-पहचाने सुरक्षा टूल			
5	ईमेल में चेतावनी के संकेत			
6	लंबे पासफ़्रेज़ के लिए मज़ेदार शब्द			
7	पासवर्ड के बिना लॉग इन करने के तरीके			
8	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
9	सॉफ़्टवेयर अपडेट करने के कारण			
10	पासवर्ड लीक होने पर की जाने वाली चीज़ें			
11	ऐसे अकाउंट जिन्हें MFA चाहिए			
12	ऐसी जगहें जहाँ पासवर्ड कभी स्टोर नहीं करने चाहिए			
13	कंप्यूटर के संक्रमित होने के संकेत			
14	लोगों के इस्तेमाल किए खराब पासवर्ड			
15	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			

चेकपॉइंट 8: साइबर सुरक्षा केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

केस स्टडी 1: एंटरप्राइज़ क्रेडेंशियल लीक का समाधान



परिदृश्य: एक डार्क वेब मॉनिटरिंग सेवा किसी संगठन को सचेत करती है कि कॉर्पोरेट सिस्टम एडमिनिस्ट्रेटरों के पासवर्ड वाला एक डेटाबेस डंप ऑनलाइन प्रकाशित हो गया है।

चर्चा प्रश्न: क्रेडेंशियल लीक के जोखिमों का विश्लेषण कीजिए और प्रशासनिक रीसेट रणनीति प्रस्तावित कीजिए।

केस स्टडी 2: पासवर्ड हैशिंग मानक लागू करना



परिदृश्य: एक एंटरप्राइज़ डेटाबेस फ़िलहाल उपयोगकर्ता पासवर्ड को क्रिप्टोग्राफ़िक सॉल्ट के बिना पुराने MD5 हैश से स्टोर करता है, जिससे वे तेज़ी से निकाले जाने के प्रति असुरक्षित हैं।

चर्चा प्रश्न: डेटाबेस हैशिंग एल्गोरिदम को अपग्रेड करने की माइग्रेशन रणनीति डिज़ाइन कीजिए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

साइबर सुरक्षा पेशेवर नेटवर्क संपत्तियों को ऑनलाइन ख़तरा पैदा करने वालों से बचाता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

37	40	61	23	48	34	60	53	13	61	23	39		40	56	15	47	32		44	52
		33	46	44	41	39	61	25		44	49	39	13	61	43	47	28			

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग A)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q1: पासवर्ड लीक क्या है?

पासवर्ड लीक तब होता है जब डेटा उल्लंघनों या सर्वर की गलत कॉन्फ़िगरेशन से उपयोगकर्ताओं के लॉगिन क्रेडेंशियल उजागर हो जाते हैं।

Q2: हैकर लीक हुए पासवर्ड कैसे ढूँढते हैं?

हैकर डार्क वेब फ़ोरम, सार्वजनिक डेटाबेस डंप और पेस्ट साइटों को स्कैन करते हैं, जहाँ ब्रीच डेटा प्रकाशित होता है [8]।

Q3: क्या पासवर्ड दोबारा उपयोग करना खतरनाक है?

हाँ, क्योंकि यदि एक साइट से समझौता हो जाए, तो हैकर वही क्रेडेंशियल हज़ारों अन्य प्लेटफ़ॉर्म पर आज़मा सकते हैं [3]।

Q4: क्रिप्टोग्राफ़िक सॉल्ट क्या है?

सॉल्ट वह यादृच्छिक डेटा है जो हैशिंग से पहले पासवर्ड में जोड़ा जाता है, जिससे पहले से तैयार लुकअप हमले बेअसर हो जाते हैं [2]।

Q5: MD5 अप्रचलित क्यों है?

MD5 एक तेज़, अप्रचलित सामान्य-उद्देश्य हैश है, इसलिए हमलावर पासवर्ड के अंदाज़ों को बेहद तेज़ी से परख सकते हैं, खासकर तब जब हैश में सॉल्ट न हो [2]।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q6: पासवर्ड मैनेजर उपयोगकर्ताओं की सुरक्षा कैसे करता है?

यह हर साइट के लिए जटिल, अनूठे क्रेडेंशियल अपने-आप बनाता है, जिससे मानवीय याददाश्त की भूल और दोहराव घटता है।

Q7: ब्रूट फ़ोर्स अटैक क्या है?

ऐसा हमला जो सही पासवर्ड मिलने तक हर संभव अक्षर संयोजन को व्यवस्थित रूप से आज़माता है [4]।

Q8: अकाउंट लॉकआउट कैसे मदद करता है?

लॉकआउट या रेट लिमिटिंग बार-बार ऑनलाइन अंदाज़ा लगाने की गति धीमी करती है और निगरानी तथा MFA के साथ मिलकर ब्रूट-फ़ोर्स का जोखिम घटाती है [4]।

Q9: क्या मास्टर पासवर्ड सुरक्षित हैं?

ये तब सुरक्षित हैं जब ये उच्च-एन्ट्रॉपी वाले पासफ़्रेज़ हों और अन्य वेब सिस्टमों पर कभी दोबारा इस्तेमाल न किए जाएँ।

Q10: क्या पासवर्ड नियमित रूप से बदले जाने चाहिए?

NIST कहता है कि समय-समय पर बदलाव के लिए बाध्य न करें; समझौता होने के प्रमाण पर पासवर्ड बदलें और लंबाई, ब्लॉकलिस्ट तथा MFA को प्राथमिकता दें [1]।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q1: Argon2 की तुलना bcrypt से कैसे की जाती है?

OWASP, Argon2id को अपनी पहली पसंद बताता है; इसकी मेमोरी-हार्ड सेटिंग्स GPU और ASIC क्रैकिंग का bcrypt से बेहतर प्रतिरोध करती हैं [2]।

Q2: की स्ट्रेचिंग क्या है?

ऐसी तकनीक जो पासवर्ड सत्यापन प्रक्रिया को धीमा करने के लिए हैशिंग एल्गोरिदम को हज़ारों बार दोहराती है, जिससे क्रैक करना महँगा हो जाता है [2]।

Q3: रेनबो टेबल कैसे काम करती हैं?

ये पहले से गणना की गई लुकअप तालिकाएँ हैं जो सादे टेक्स्ट पासवर्ड को उनके हैश से जोड़ती हैं, और बिना सॉल्ट वाले हैश को जल्दी उलटने में काम आती हैं [2]।

Q4: क्रेडेंशियल रीसाइक्लिंग क्या है?

किसी एक डेटा उल्लंघन से चुराए गए यूज़रनेम/पासवर्ड जोड़ों को दोबारा इस्तेमाल करके दूसरी सेवाओं तक पहुँचने की कोशिश करना, खासकर जहाँ लोगों ने पासवर्ड दोहराए हों [3]।

Q5: क्या पासवर्ड मैनेजर हैक हो सकते हैं?

हाँ। कई ज़ीरो-नॉलेज एन्क्रिप्शन का उपयोग करते हैं, इसलिए सर्वर ब्रीच में केवल एन्क्रिप्टेड वॉल्ट उजागर होते हैं, लेकिन कमज़ोर मास्टर पासवर्ड फिर भी ऑफ़लाइन क्रैक हो सकते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q6: डिक्शनरी अटैक क्या है?

ब्रूट-फ़ोर्स का एक रूप जो यादृच्छिक अक्षरों के बजाय सामान्य शब्दों, वाक्यांशों और पहले लीक हुए पासवर्ड को आज़माता है।

Q7: पासफ़्रेज़ को प्राथमिकता क्यों दी जाती है?

पासफ़्रेज़ कई यादृच्छिक शब्दों का उपयोग करते हैं, जिससे उच्च एंट्रॉपी बनती है जो इंसानों के लिए याद रखना आसान लेकिन क्रैक करने में कम्प्यूटेशनल रूप से महँगी होती है [1]।

Q8: सिंगल साइन-ऑन (SSO) पासवर्ड लीक को कैसे प्रभावित करता है?

SSO पासवर्ड की भरमार घटाता है, लेकिन आइडेंटिटी प्रोवाइडर एक उच्च-मूल्य वाला निशाना बन जाता है, जिसे मज़बूत, बेहतर हो कि फ़िशिंग-प्रतिरोधी, MFA चाहिए [6]।

Q9: सेशन हाइजैकिंग क्या है?

हमलावर किसी वैध सत्र टोकन को हासिल करता या उसका दुरुपयोग करता है, ताकि पासवर्ड दोबारा डाले बिना साइन-इन उपयोगकर्ता की नकल कर सके [5]।

Q10: आप पासवर्ड स्प्रेइंग का पता कैसे लगाते हैं?

कई खातों पर आज़माए गए वही गिने-चुने पासवर्ड खोजकर, जो अक्सर लॉकआउट सीमा से नीचे रहने के लिए धीरे-धीरे आज़माए जाते हैं [7]।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

सुरक्षा उल्लंघनों, बचाव तंत्रों और अनुपालन मानकों से जुड़े वास्तविक तथ्य देखें।

1. सुरक्षा इनसाइट

NIST SP 800-63B के अनुसार नए पासवर्ड को आम और समझौता हो चुके पासवर्ड की ब्लॉकलिस्ट से जाँचना ज़रूरी है [1]।

2. सुरक्षा इनसाइट

2019 के 'Collection #1' डंप ने कई पुराने उल्लंघनों का डेटा ईमेल और पासवर्ड जोड़ों की एक विशाल फ़ाइल में मिला दिया था [8]।

3. सुरक्षा इनसाइट

NIST अब चाहता है कि प्रमाणीकरण के एकमात्र कारक के रूप में इस्तेमाल होने वाले पासवर्ड कम से कम 15 अक्षरों के हों [1]।

4. सुरक्षा इनसाइट

ASIC हार्डवेयर प्रति सेकंड अरबों SHA-256 हैश की गणना कर सकता है, इसलिए उपयोगकर्ता पासवर्ड के लिए सादा SHA हैशिंग असुरक्षित है [2]।

5. सुरक्षा इनसाइट

अद्वितीय सॉल्ट का मतलब है कि एक ही पासवर्ड वाले दो उपयोगकर्ताओं के डेटाबेस हैश अलग-अलग होते हैं [2]।

6. सुरक्षा इनसाइट

कई पासवर्ड मैनेजर वॉल्ट डेटा को उपयोगकर्ता के मास्टर पासवर्ड से बनी मज़बूत क्रिप्टोग्राफ़ी से स्थानीय रूप से एन्क्रिप्ट करते हैं।

7. सिक्योरिटी इनसाइट

क्रेडेंशियल स्टफ़िंग इसलिए काम करती है क्योंकि कई लोग ई-कॉमर्स, बैंकिंग और ईमेल खातों में एक ही पासवर्ड दोहराते हैं [3]।

8. सिक्योरिटी इनसाइट

NIST SP 800-63B कहता है कि वेरिफ़ायर को समय-समय पर पासवर्ड बदलने की माँग नहीं करनी चाहिए, केवल समझौता होने के प्रमाण के बाद बदलाव माँगना चाहिए [1]।

9. सिक्योरिटी इनसाइट

छोटे पासवर्ड में एक बड़ा अक्षर और एक प्रतीक जोड़ देने से आधुनिक स्वचालित GPU शब्दकोश हमले नहीं रुकते [1]।

10. सुरक्षा इनसाइट

पासवर्ड लीक होने के बाद भी MFA क्रेडेंशियल-स्टफ़िंग के कई प्रयासों को रोक सकता है; फ़िशिंग-प्रतिरोधी MFA, SMS कोड से ज़्यादा मज़बूत है [3]।

तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक NIST, OWASP और डेटा गोपनीयता अनुपालन मानकों से तैयार की गई हैं।

शैक्षणिक और उद्योग संदर्भ

[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/

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **प्रश्न 1** **सही उत्तर: A**

शिक्षण नोट

क्रेडेंशियल स्टफ़िंग लीक हुए यूज़रनेम/पासवर्ड जोड़ों को अन्य साइटों पर आज़माने के लिए ऑटोमेशन का उपयोग करती है [3]।

2 **प्रश्न 2** **सही उत्तर: A**

शिक्षण नोट

OWASP पहले Argon2id की सिफ़ारिश करता है; bcrypt मुख्य रूप से पुराने सिस्टमों के लिए है जहाँ Argon2id या scrypt उपलब्ध नहीं हैं [2]।

3 **प्रश्न 3** **सही उत्तर: A**

शिक्षण नोट

MFA एक अतिरिक्त कारक माँगता है, इसलिए अकेला चोरी हुआ पासवर्ड अकाउंट को अनलॉक नहीं कर सकता [3]।

4 **प्रश्न 4** **सही उत्तर: A**

शिक्षण नोट

ब्रीच डंप लीक हुए क्रेडेंशियल के संग्रह हैं, जैसे 2019 का Collection #1 संकलन [8]।

5 **प्रश्न 5** **सही उत्तर: A**

शिक्षण नोट

पासवर्ड मैनेजर हर अकाउंट के लिए एक अनोखा, मज़बूत पासवर्ड बनाता और स्टोर करता है, जिससे दोबारा उपयोग रुकता है [3]।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** — **सही उत्तर: सही**

शिक्षण नोट

सही: दोबारा इस्तेमाल किए गए पासवर्ड हमलावरों को एक साइट से लीक हुए क्रेडेंशियल दूसरी साइटों पर आज़माने देते हैं [3]।

7 **प्रश्न 7** — **सही उत्तर: गलत**

शिक्षण नोट

गलत: SHA-1 तेज़ हैश है; OWASP इसके बजाय Argon2id, scrypt, bcrypt या PBKDF2 की सिफ़ारिश करता है [2]।

8 **प्रश्न 8** — **सही उत्तर: गलत**

शिक्षण नोट

गलत: केवल जटिलता के नियम लीक हुए दोबारा इस्तेमाल किए पासवर्ड के साथ स्टफ़िंग नहीं रोक सकते; MFA चाहिए [3]।

9 **प्रश्न 9** — **सही उत्तर: सही**

शिक्षण नोट

सही: मॉनिटरिंग सेवाएँ उजागर क्रेडेंशियल के लिए ब्रीच डंप और डार्क वेब स्रोतों में खोज करती हैं [8]।

10 **प्रश्न 10** — **सही उत्तर: सही**

शिक्षण नोट

सही: हर पासवर्ड के लिए अनोखा सॉल्ट पहले से बनाई गई रेनबो तालिकाओं को बेअसर कर देता है [2]।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

F 1. स्टफ़िंग	H 2. bcrypt	D 3. उल्लंघन	G 4. सॉल्टिंग
C 5. मैनेजर	B 6. MFA	A 7. रेनबो	E 8. फ़िशिंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 हैशिंग	2 मॉनिटरिंग	3 स्कैनिंग	4 सॉल्टिंग
5 निगरानी	6 फ़िल्टरिंग		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 H – निगरानी	2 C – स्कैमिंग	3 B – फ़िशिंग	4 G – मॉनिटरिंग
5 A – सॉल्टिंग	6 D – स्कैनिंग	7 E – हैशिंग	8 F – फ़िल्टरिंग

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी स्टफ़िंग, bcrypt और उल्लंघन को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

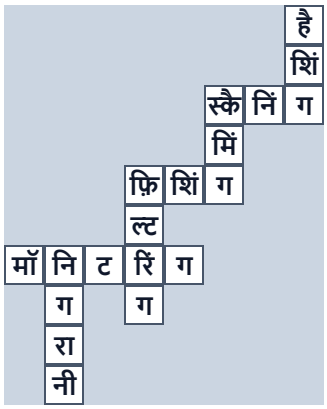
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

ई	म	पि	इ	ठ	दा	ज	द	दि	ते	वी	ति	च	ह	री
रा	व	त	सा	स	ई	ते	घ	स्कै	इ	नी	ल	रि	द	जे
घ	छ	ई	के	द	प	ति	के	ट	निं	मि	ट	सा	य	च
ऊ	ग	नी	जी	इ	त	म	पे	ब	प	ग	जि	मी	ने	ले
इ	शिं	सी	य	छ	मॉ	र	दे	कि	जा	सा	वा	ड	रे	स
ख	फ़ि	नि	फ	ढ	नि	मा	सॉ	ना	का	रे	दे	सि	मी	क
पि	ता	ति	ज	श	ट	भ	ऊ	ल्टिं	अ	ऊ	ए	रि	वि	श
य	वि	व	वा	पा	रिं	ल	च	से	ग	कि	य	घ	प	के
की	व	सि	री	त	ग	की	कि	सि	ना	ने	पा	ते	ण	ए
ग	ता	सा	मी	न	नी	ऋ	ले	घ	ति	जि	ला	ए	जी	ले
मिं	फ़ि	ल्ट	रिं	ग	ड	ल	द	जे	घ	के	च	से	दे	है
स्कै	री	ए	पी	नि	उ	अ	जे	मि	घ	व	आ	च	शिं	मी
च	ट	थ	फ	ग	ग	ना	सी	का	ज	फ	नी	ग	जी	ता
ठ	से	लि	ट	रा	आ	इ	से	रा	के	री	पा	वा	सि	य
नि	पि	ने	ख	नी	के	वे	ऊ	ड	नी	दे	दि	भ	आ	नि

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

2 बाएँ से दाएँ: स्कैनिंग संदिग्ध लिंक या फ़ाइल में ख़तरे खोजने के लिए की जाने वाली जाँच (3 अक्षर)

3 बाएँ से दाएँ: फ़िशिंग लॉगिन चुराने के लिए सोशल इंजीनियरिंग। (3 अक्षर)

4 बाएँ से दाएँ: मॉनिटरिंग किसी खाते या नेटवर्क पर लगातार नज़र रखकर गड़बड़ी पकड़ना (5 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: हैशिंग पासवर्ड को अपठनीय कोड में बदलकर सहेजने की एकतरफ़ा विधि (3 अक्षर)

2 ऊपर से नीचे: स्कैमिंग लोगों को झूठे वादों से फँसाकर उनसे पैसे ऐंठने की धोखाधड़ी (3 अक्षर)

3 ऊपर से नीचे: फ़िल्टरिंग संदिग्ध संदेशों या ट्रैफ़िक को पहचानकर रोक देने की प्रक्रिया (4 अक्षर)

5 ऊपर से नीचे: निगरानी किसी गतिविधि पर लगातार नज़र रखने की प्रक्रिया (4 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. ल्टिं ग सॉ — **सॉल्टिंग**
2. ग मिं स्कै — **स्कैमिंग**
3. ग शिं है — **हैशिंग**
4. ट ग रिं मॉ नि — **मॉनिटरिंग**
5. ग शिं फ़ि — **फ़िशिंग**
6. निं ग स्कै — **स्कैनिंग**
7. रिं फ़ि ग ल्ट — **फ़िल्टरिंग**
8. नि नी रा ग — **निगरानी**

गुप्त कूट चुनौती कुंजी

"मल्टीफ़ैक्टर लॉगिन से पासवर्ड सुरक्षित"

केस स्टडी के उत्तर

A केस स्टडी 1: एंटरप्राइज़ क्रेडेंशियल लीक का समाधान

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक डार्क वेब मॉनिटरिंग सेवा किसी संगठन को सचेत करती है कि कॉर्पोरेट सिस्टम एडमिनिस्ट्रेटर के पासवर्ड वाला डेटाबेस डंप ऑनलाइन प्रकाशित हो गया है।
- अनुशंसित रणनीति और समाधान: सभी सक्रिय एडमिनिस्ट्रेटर सेशन रद्द करें और हाई-एंट्रॉपी जनरेटर से क्रेडेंशियल रीसेट करें। एडमिन पोर्टल पर फ़िशिंग-प्रतिरोधी MFA लागू करें [6], प्रभावित API कुंजियाँ रोटेट करें, लॉगिन लॉग देखें, शुरुआती एक्सपोज़र का पता लगाएँ और अन्य विशेषाधिकार प्राप्त अकाउंट जाँचें।

B केस स्टडी 2: पासवर्ड हैशिंग मानक लागू करना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक एंटरप्राइज़ डेटाबेस फ़िलहाल उपयोगकर्ताओं के पासवर्ड पुराने MD5 हैश में, बिना क्रिप्टोग्राफ़िक सॉल्ट के संग्रहीत करता है, जिससे उन्हें तेज़ी से निकाला जा सकता है।
- अनुशंसित रणनीति और समाधान: प्रत्येक उपयोगकर्ता के लिए अद्वितीय सॉल्ट के साथ Argon2id (या पुराने सिस्टम पर bcrypt) अपनाएँ [2]। मौजूदा MD5 हैश को अभी नए एल्गोरिदम में लपेट दें, प्रत्येक उपयोगकर्ता के अगले लॉगिन पर सीधे दोबारा हैश करें, और लंबे समय से निष्क्रिय अकाउंट के लिए रीसेट अनिवार्य करें।