নাম: _____ তারিখ: _____ নম্বর: _____

পাসওয়ার্ড ফাঁস ও ক্রেডেনশিয়াল নিরাপত্তা

ক্রেডেনশিয়াল স্টাফিং, ডেটা ফাঁস, হ্যাশ অ্যালগরিদম, মাল্টি-ফ্যাক্টর প্রমাণীকরণ এবং পাসওয়ার্ড নিরাপত্তা।

পাসওয়ার্ড ফাঁস শিক্ষণ পরিচিতি

সুরক্ষিত
ডেটা এনক্রিপশন
256-বিট AES স্ট্যান্ডার্ড

সম্মতিপূর্ণ
বৈশ্বিক মান
GDPR ও CCPA কাঠামো

জিরো-ট্রাস্ট
অ্যাক্সেস নীতি
মাল্টি-ফ্যাক্টর অথেনটিকেশন

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে পাসওয়ার্ড লিক ও ক্রেডেনশিয়াল নিরাপত্তা বিষয়ে গাইড করবে। আপনি ক্রেডেনশিয়াল স্টাফিং, ডেটা ব্রিচ, হ্যাশিং অ্যালগরিদম, মাল্টি-ফ্যাক্টর প্রমাণীকরণ এবং পাসওয়ার্ড ম্যানেজার সম্পর্কে জানবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] **অংশ 1-4: সাইবার নিরাপত্তা ও হুমকি প্রতিরোধে দক্ষতা অর্জন করুন।**
- [ ] **অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।**
- [ ] **অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।**
- [ ] **অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।**
- [ ] **অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।**
- [ ] **অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।**

VPN.com সাইবার নিরাপত্তা গাইড খুলুন

URL: https://www.vpn.com/bn/saibar-nirapotta/password/

আপনার পাসওয়ার্ড নিরাপত্তা শেখার রোডম্যাপ

- ডার্ক ওয়েব ফোরামে ক্রেডেনশিয়াল প্রকাশের ঝুঁকি বুঝুন।
- মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) এবং ফাঁস হওয়া লগইন তথ্যের মনিটরিং বাস্তবায়ন করুন।
- লক্ষ্যভিত্তিক সোশ্যাল ইঞ্জিনিয়ারিং প্রতারণার বিরুদ্ধে কর্পোরেট নিরাপত্তা প্রতিরক্ষা নকশা করুন।

পাসওয়ার্ড ফাঁস গাইড নির্দেশনা

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। ক্রেডেনশিয়াল সুরক্ষা বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

পাসওয়ার্ড ফাঁস ও ক্রেডেনশিয়াল নিরাপত্তা (ভূমিকা)

পাসওয়ার্ড ফাঁসে পাবলিক ও ডার্ক ওয়েব সাইটে ব্যবহারকারীর ক্রেডেনশিয়াল প্রকাশ হয়ে পড়ে। পাসওয়ার্ড ম্যানেজারের অনন্য পাসওয়ার্ড, ফাঁস হওয়া পাসওয়ার্ড যাচাই এবং মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) ক্রেডেনশিয়াল স্টাফিংয়ের ঝুঁকি কমায়, আর সল্ট দেওয়া ধীরগতির পাসওয়ার্ড হ্যাশিং পাসওয়ার্ড ডেটাবেস চুরি হলে ক্ষতি সীমিত রাখে।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 **1. ক্রেডেনশিয়াল স্টাফিং কী?**

- A. একাধিক সাইটে ফাঁস হওয়া ইউজারনেম/পাসওয়ার্ডের জোড়া পরীক্ষা করতে অটোমেশন ব্যবহার করা
- B. স্থানীয় ডেটাবেস স্টোরেজ ফাইল এনক্রিপ্ট করা
- C. নেটওয়ার্ক ট্র্যাফিক অনুরোধে ওয়েব সার্ভারকে ভারাক্রান্ত করে ফেলা
- D. গোপনে কিবোর্ডের ইনপুট পর্যবেক্ষণ করা

2 **2. বর্তমানে পাসওয়ার্ড সংরক্ষণের জন্য OWASP প্রথম পছন্দ হিসেবে কোন অ্যালগরিদম তালিকাভুক্ত করে?**

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

3 **3. মাল্টি-ফ্যাক্টর প্রমাণীকরণ (MFA) পাসওয়ার্ড ফাঁসের ঝুঁকি কীভাবে কমায়?**

- A. এটি একটি অতিরিক্ত যাচাইকরণ ফ্যাক্টর চায়, তাই শুধু চুরি হওয়া পাসওয়ার্ড যথেষ্ট নয়
- B. এটি প্রতি ঘণ্টায় স্বয়ংক্রিয়ভাবে পাসওয়ার্ড বদলে দেয়
- C. এটি ট্রান্সমিশনের সময় ব্যবহারকারীর নাম এনক্রিপ্ট করে
- D. এটি প্রতারণামূলক অনুরোধের কথা ক্রেডিট ব্যুরোকে জানায়

4 **4. ডেটা ব্রিচ ডাম্প কী?**

- A. ফাঁস হওয়া ব্যবহারকারী ক্রেডেনশিয়ালের একটি সংগ্রহ, যা অনলাইনে প্রকাশিত বা হ্যাকার ফোরামে বিক্রি হয়
- B. অফসাইটে রাখা ডেটাবেস ফাইলের ব্যাকআপ কপি
- C. ওয়েব সার্ভার লগের একটি অস্থায়ী ক্যাশ
- D. ব্যবহারকারীর পাসওয়ার্ড রিসেট করতে ব্যবহৃত একটি প্রশাসনিক টুল

5 **5. পাসওয়ার্ড ম্যানেজারের ভূমিকা কী?**

- A. প্রতিটি অ্যাকাউন্টের জন্য অনন্য, শক্তিশালী পাসওয়ার্ড তৈরি ও সংরক্ষণ করা
- B. পাসওয়ার্ড ফাঁসের জন্য নেটওয়ার্ক ট্র্যাফিক পর্যবেক্ষণ করা
- C. গেটওয়েতে স্বয়ংক্রিয় ব্রুট-ফোর্স আক্রমণ ব্লক করা
- D. এনক্রিপ্ট না করা পাসওয়ার্ডের জন্য ডাটাবেস স্টোরেজ ব্লক স্ক্যান করা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. একাধিক অ্যাকাউন্টে পাসওয়ার্ড পুনর্ব্যবহার ক্রেডেনশিয়াল স্টাফিংয়ের ঝুঁকি বাড়ায়।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. SHA-1 আধুনিক পাসওয়ার্ড সংরক্ষণের জন্য একটি সুপারিশকৃত হ্যাশিং ফাংশন।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. শুধু পাসওয়ার্ডের জটিলতা কার্যকর করলেই (MFA ছাড়া) ক্রেডেনশিয়াল স্টাফিং সম্পূর্ণ বন্ধ হয়।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. ডার্ক ওয়েব মনিটরিং টুল ইন্টারনেট স্ক্যান করে ফাঁস হওয়া কর্পোরেট ক্রেডেনশিয়াল খোঁজে।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. সল্টেড হ্যাশ হ্যাশ করার আগে পাসওয়ার্ডে অনন্য র‍্যান্ডম ডেটা যোগ করে, ফলে রেইনবো টেবিল আক্রমণ ব্যর্থ হয়।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. অনেক ওয়েব অ্যাপ্লিকেশনে ফাঁস হওয়া লগইন তথ্য পরীক্ষা করাকে বলা হয় ক্রেডেনশিয়াল _____ ।

2. OWASP-এর কাছে এখনও গ্রহণযোগ্য ধীরগতির, অভিযোজিত পাসওয়ার্ড হ্যাশিং অ্যালগরিদম হলো _____ ।

3. ইন্টারনেটে গোপনীয় ডেটাবেস ফাইল প্রকাশ পেয়ে যাওয়া হলো ডেটা _____ ।

4. হ্যাশ করার আগে পাসওয়ার্ডে এলোমেলো মান যোগ করাকে বলা হয় _____ ।

5. ব্যবহারকারীর লগইন তথ্যের নিরাপদ স্থানীয় ডেটাবেস হলো পাসওয়ার্ড _____ ।

6. লগইনে দ্বিতীয় যাচাই-ধাপ যোগ করতে ব্যবহৃত হয় _____ ।

পরিভাষা শব্দভাণ্ডার

এমএফএ | ফিশিং | ম্যানেজার | রেইনবো | লঙঘন | সল্টিং | স্টাফিং | bcrypt

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

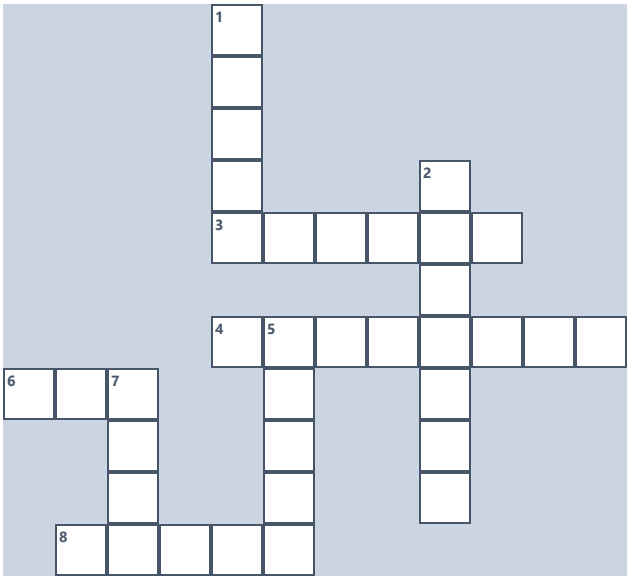
সংজ্ঞা মেলানো

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

☐	**1. স্টাফিং**	**A**	পাসওয়ার্ড হ্যাশের পূর্বগণনা করা টেবিল।
☐	**2. bcrypt**	**B**	মাল্টি-ফ্যাক্টর লগইন যাচাই।
☐	**3. নিরাপত্তা লঙ্ঘন**	**C**	ক্রেডেনশিয়াল সংরক্ষণ টুল।
☐	**4. সল্টিং**	**D**	অননুমোদিত ডেটাবেস প্রকাশ।
☐	**5. ম্যানেজার**	**E**	লগইন চুরির সোশ্যাল ইঞ্জিনিয়ারিং।
☐	**6. MFA**	**F**	ফাঁস হওয়া ক্রেডেনশিয়াল পরীক্ষা করা।
☐	**7. রেইনবো**	**G**	পাসওয়ার্ড হ্যাশে এলোমেলো সল্ট যোগ করা।
☐	**8. ফিশিং**	**H**	ধীরগতির পাসওয়ার্ড হ্যাশিং অ্যালগরিদম।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।



পাশাপাশি

3. পাসওয়ার্ড হ্যাশে এলোমেলো সল্ট যোগ করা (6)

4. ফাঁস হওয়া লগইন তথ্য পরীক্ষা করা (8)

6. আসল জিনিসের অবিকল অনুকরণ (3)

8. ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5)

উপর-নিচ

1. বহু-ধাপের লগইন যাচাই (5)

2. লগইন তথ্যের জন্য নিরাপদ স্থানীয় সংরক্ষণ-সরঞ্জাম (7)

5. অননুমোদিত ডেটাবেস প্রকাশ (5)

7. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

পাশাপাশি

3 পাশাপাশি: পাসওয়ার্ড হ্যাশে এলোমেলো সল্ট যোগ করা (6 অক্ষর):

4 পাশাপাশি: ফাঁস হওয়া লগইন তথ্য পরীক্ষা করা (8 অক্ষর):

6 পাশাপাশি: আসল জিনিসের অবিকল অনুকরণ (3 অক্ষর):

8 পাশাপাশি: ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5 অক্ষর):

উপর-নিচ

1 উপর-নিচ: বহু-ধাপের লগইন যাচাই (5 অক্ষর):

2 উপর-নিচ: লগইন তথ্যের জন্য নিরাপদ স্থানীয় সংরক্ষণ-সরঞ্জাম (7 অক্ষর):

5 উপর-নিচ: অননুমোদিত ডেটাবেস প্রকাশ (5 অক্ষর):

7 উপর-নিচ: নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

ণ ল্ট দ নে স ঝ কা ন জ রা ফ ঘ উ সে জি
আ স ড প পা ধ দ ক এ জি কি না লি ই রে
ফ লো চ ব দি শ জা ল রা ম দে ট মে র ক
সি মে দ ঠ হ সা শ মে দে রা এ কি ঋ তে না
নে লো ছ য প ক্রে উ অ উ ঋ মা ফ বা অ য
ফ এ বা ম দে ডে তি পা ভ ঘ রে ষ এ ন ফ
ন ই গ ল ঘ ন দ হ স স ভ রি মি লা ঢ
ন ষ ষ রি সি শি না তি তা ও ড ঊ নি ই রা
ঙ্ঘ কি থ সে ঊ য়া লি গ নি জা য়া পি ঋ ন জি
ল লি ট ভ ণ ল জে গ স ঘ রে র্ড দি মি ঋ
টা পা উ অ জে স্টা কা গ ম আ ঘ কি ভ ঘ ঝ
ডে ণ ধ গ সি ফিং রি শ ছ দ সে জি নি ল্ট ঝ
রে পে জ আ আ রে মা স মে তি দে রি ফ সি তি
সে খ স বে উ ট সে দি দা প আ সি জে বি বি
য ড দ ষ সা ফ ল ল তা কে ণ রা রি ণ জে

পরিভাষা শব্দতালিকা

ক্রেডেনশিয়ালস্টাফিং ডেটালঙ্ঘন এলোমেলোসল্ট পাসওয়ার্ডভল্ট এমএফএ লগইন
অনলাইন নকল

চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

পরিভাষা

A. ক্রেডেনশিয়ালস্টাফিং

B. ডেটালঙ্ঘন

C. এলোমেলোসল্ট

D. পাসওয়ার্ডভল্ট

E. এমএফএ

F. লগইন

G. অনলাইন

H. নকল

সংজ্ঞা ও মিলের ঘর

1. আসল জিনিসের অবিকল অনুকরণ।
2. পাসওয়ার্ড হ্যাশে এলোমেলো সল্ট যোগ করা।
3. অননুমোদিত ডেটাবেস প্রকাশ।
4. ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা।
5. ফাঁস হওয়া লগইন তথ্য পরীক্ষা করা।
6. লগইন তথ্যের জন্য নিরাপদ স্থানীয় সংরক্ষণ-সরঞ্জাম।
7. বহু-ধাপের লগইন যাচাই।
8. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

সাইবার নিরাপত্তার মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর দেওয়া ইনপুট বাক্সে লিখুন।

1. স্টা শি য়া ক্রে ল ডে ফিং ন
2. ল্ট এ মে স লো লো
3. এ এ এ ফ ম
4. লা ন ই অ ন
5. ল ন ডে ঙ্ঘ টা
6. ভ ও র্ড পা য়া ল্ট স
7. ই ল ন গ
8. ল ক ন

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

1	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
2	শক্তিশালী পাসওয়ার্ডের নিয়ম			
3	আপনার জানা পাসওয়ার্ড ম্যানেজার			
4	আপনার জানা নিরাপত্তা টুল			
5	ইমেইলে সতর্কতার লক্ষণ			
6	লম্বা পাসফ্রেজের জন্য মজার শব্দ			
7	পাসওয়ার্ড ছাড়া লগইন করার উপায়			
8	যে তথ্য আপনার কখনো শেয়ার করা উচিত নয়			
9	সফটওয়্যার আপডেট করার কারণ			
10	পাসওয়ার্ড ফাঁস হলে যা করবেন			
11	যেসব অ্যাকাউন্টে MFA দরকার			
12	যেসব জায়গায় পাসওয়ার্ড কখনো সংরক্ষণ করা উচিত নয়			
13	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
14	মানুষের ব্যবহৃত দুর্বল পাসওয়ার্ড			
15	যা যা আপনি ব্যাকআপ করেন			

চেকপয়েন্ট 8: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: এন্টারপ্রাইজ ক্রেডেনশিয়াল ফাঁসের প্রতিকার



পরিস্থিতি: একটি ডার্ক ওয়েব মনিটরিং সেবা একটি প্রতিষ্ঠানকে সতর্ক করে যে কর্পোরেট সিস্টেম অ্যাডমিনিস্ট্রেটরদের পাসওয়ার্ডসহ একটি ডেটাবেস ডাম্প অনলাইনে প্রকাশিত হয়েছে।

আলোচনার প্রশ্ন: ক্রেডেনশিয়াল ফাঁসের ঝুঁকি বিশ্লেষণ করুন এবং একটি প্রশাসনিক রিসেট কৌশলের প্রস্তাব করুন।

কেস স্টাডি 2: পাসওয়ার্ড হ্যাশিং মান বাস্তবায়ন



পরিস্থিতি: একটি এন্টারপ্রাইজ ডেটাবেস বর্তমানে ক্রিপ্টোগ্রাফিক সল্ট ছাড়া পুরোনো MD5 হ্যাশ দিয়ে ব্যবহারকারীর পাসওয়ার্ড সংরক্ষণ করে, ফলে সেগুলো দ্রুত বের করে নেওয়ার ঝুঁকিতে আছে।

আলোচনার প্রশ্ন: ডেটাবেসের হ্যাশিং অ্যালগরিদম আপগ্রেড করার জন্য একটি মাইগ্রেশন কৌশল ডিজাইন করুন।

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

একজন সাইবার নিরাপত্তা পেশাজীবী অনলাইন হুমকিদাতাদের হাত থেকে নেটওয়ার্ক সম্পদ রক্ষা করেন। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে বার্তাটি ডিক্রিপ্ট করুন।

অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12

খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24

ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36

য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48

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

34	43	48	30	45	32		39	14	3	31	51		33	45	57	42
32	**45**	**42**	**10**	**37**	**59**	**45**	**38**	**58**	**24**		**38**	**12**	**58**	**41**	**45**	

ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ A)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: পাসওয়ার্ড ফাঁস কী?

ডেটা ভঙ্গ বা সার্ভার ভুল কনফিগারেশনের মাধ্যমে ব্যবহারকারীর লগইন ক্রেডেনশিয়াল প্রকাশ পেয়ে গেলে পাসওয়ার্ড লিক ঘটে।

Q2: হ্যাকাররা ফাঁস হওয়া পাসওয়ার্ড কীভাবে খুঁজে পায়?

হ্যাকাররা ডার্ক ওয়েব ফোরাম, প্রকাশ্য ডেটাবেস ডাম্প এবং পেস্ট সাইট স্ক্যান করে, যেখানে ডেটা ফাঁসের তথ্য প্রকাশ করা হয় [৪]।

Q3: পাসওয়ার্ড পুনরায় ব্যবহার করা কি বিপজ্জনক?

হ্যাঁ, কারণ একটি সাইট আপস হলে হ্যাকাররা একই ক্রেডেনশিয়াল হাজার হাজার অন্য প্ল্যাটফর্মে পরীক্ষা করে দেখতে পারে [3]।

Q4: ক্রিপ্টোগ্রাফিক সল্ট কী?

সল্ট হলো হ্যাশ করার আগে পাসওয়ার্ডে যোগ করা এলোমেলো ডেটা, যা প্রি-কম্পিউটেড লুকআপ আক্রমণকে অকার্যকর করে [2]।

Q5: MD5 কেন অচল হয়ে গেছে?

MD5 একটি দ্রুত, অচল সাধারণ-উদ্দেশ্যের হ্যাশ, তাই বিশেষ করে হ্যাশ সল্টবিহীন হলে আক্রমণকারীরা অত্যন্ত দ্রুত পাসওয়ার্ড অনুমান যাচাই করতে পারে [2]।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: পাসওয়ার্ড ম্যানেজার কীভাবে ব্যবহারকারীদের সুরক্ষা দেয়?

এটি প্রতিটি সাইটের জন্য জটিল, অনন্য পরিচয়পত্র স্বয়ংক্রিয়ভাবে তৈরি করে, ফলে মানুষের স্মৃতিজনিত ভুল ও পুনর্ব্যবহার কমে।

Q7: ব্রুট ফোর্স আক্রমণ কী?

একটি আক্রমণ, যা সঠিক পাসওয়ার্ড না পাওয়া পর্যন্ত প্রতিটি সম্ভাব্য অক্ষর-সমন্বয় পদ্ধতিগতভাবে পরীক্ষা করে [4]।

Q8: অ্যাকাউন্ট লকআউট কীভাবে সাহায্য করে?

লকআউট বা রেট লিমিটিং বারবার অনলাইন অনুমান ধীর করে এবং মনিটরিং ও MFA-র সঙ্গে মিলিত হয়ে ব্রুট-ফোর্স ঝুঁকি কমায় [4]।

Q9: মাস্টার পাসওয়ার্ড কি নিরাপদ?

এগুলো নিরাপদ, যদি তা উচ্চ-এন্ট্রপির পাসফ্রেজ হয় এবং অন্য কোনো ওয়েব সিস্টেমে কখনো পুনরায় ব্যবহার করা না হয়।

Q10: পাসওয়ার্ড কি নিয়মিত বদলানো উচিত?

NIST বলে পর্যায়ক্রমিক পরিবর্তন বাধ্য করা উচিত নয়; আপস হওয়ার প্রমাণ মিললে পরিবর্তন করুন এবং দৈর্ঘ্য, ব্লকলিস্ট ও MFA-কে অগ্রাধিকার দিন [1]।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q1: Argon2 ও bcrypt-এর তুলনা কেমন?

OWASP প্রথম পছন্দ হিসেবে Argon2id-এর কথা বলে; এর মেমরি-নির্ভর সেটিংস bcrypt-এর চেয়ে GPU ও ASIC ক্র্যাকিং ভালোভাবে প্রতিরোধ করে [2]।

Q2: কী স্ট্রেচিং কী?

পাসওয়ার্ড যাচাই প্রক্রিয়া ধীর করতে একটি হ্যাশিং অ্যালগরিদমকে হাজার হাজার বার লুপে চালানোর কৌশল, যা ক্র্যাকিংকে ব্যয়বহুল করে তোলে [2]।

Q3: রেইনবো টেবিল কীভাবে কাজ করে?

এগুলো আগে থেকে হিসাব করা লুকআপ টেবিল, যা প্লেইনটেক্সট পাসওয়ার্ডকে তাদের হ্যাশের সঙ্গে যুক্ত করে এবং সল্ট-বিহীন হ্যাশ দ্রুত উল্টাতে ব্যবহৃত হয় [2]।

Q4: ক্রেডেনশিয়াল রিসাইক্লিং কী?

একটি ডেটা ফাঁস থেকে চুরি হওয়া ইউজারনেম/পাসওয়ার্ড জোড়া অন্য সেবায় প্রবেশের চেষ্টায় আবার ব্যবহার করা, বিশেষ করে যেখানে মানুষ পাসওয়ার্ড পুনর্ব্যবহার করেছে [3]।

Q5: পাসওয়ার্ড ম্যানেজার কি হ্যাক হতে পারে?

হ্যাঁ। অনেকে জিরো-নলেজ এনক্রিপশন ব্যবহার করে, ফলে সার্ভার ভাঙলে কেবল এনক্রিপ্টেড ভল্ট প্রকাশ পায়, তবে দুর্বল মাস্টার পাসওয়ার্ড অফলাইনে ক্র্যাক করা যেতে পারে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q6: ডিকশনারি আক্রমণ কী?

একটি ব্রুট-ফোর্স ধরন, যা এলোমেলো অক্ষরের বদলে প্রচলিত শব্দ, বাক্যাংশ ও অতীতে ফাঁস হওয়া পাসওয়ার্ড পরীক্ষা করে।

Q7: পাসফ্রেজ কেন পছন্দনীয়?

পাসফ্রেজ একাধিক এলোমেলো শব্দ ব্যবহার করে, ফলে উচ্চ এনট্রপি তৈরি হয়, যা মানুষের মনে রাখা সহজ কিন্তু ক্র্যাক করতে গণনাগতভাবে ব্যয়বহুল [1]।

Q8: সিঙ্গেল সাইন-অন (SSO) পাসওয়ার্ড ফাঁসকে কীভাবে প্রভাবিত করে?

SSO পাসওয়ার্ডের বিস্তার কমায়, কিন্তু আইডেন্টিটি প্রোভাইডার একটি উচ্চ-মূল্যের লক্ষ্যে পরিণত হয়, যার জন্য শক্তিশালী, বিশেষত ফিশিং-প্রতিরোধী MFA দরকার [6]।

Q9: সেশন হাইজ্যাকিং কী?

আক্রমণকারী একটি বৈধ সেশন টোকেন সংগ্রহ বা অপব্যবহার করে পাসওয়ার্ড ছাড়াই সাইন-ইন করা ব্যবহারকারীর ছদ্মবেশ ধারণ করে [5]।

Q10: পাসওয়ার্ড স্প্রেয়িং কীভাবে শনাক্ত করবেন?

অনেক অ্যাকাউন্টে একই কয়েকটি পাসওয়ার্ড চেষ্টা করা হচ্ছে কি না তা খুঁজে, যা প্রায়ই লকআউট সীমার নিচে থাকতে ধীরে করা হয় [7]।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

নিরাপত্তা লঙ্ঘন, প্রতিরক্ষা কৌশল ও সম্মতির মান সম্পর্কে বাস্তব তথ্য দেখে নিন।

1. নিরাপত্তা ইনসাইট

NIST SP 800-63B অনুযায়ী নতুন পাসওয়ার্ড সাধারণ ও আপস হওয়া পাসওয়ার্ডের ব্লকলিস্টের বিপরীতে যাচাই করতে হবে [1]।

2. নিরাপত্তা ইনসাইট

2019 সালের 'Collection #1' ডাম্প আগের অনেক লঙ্ঘনের ডেটা এক বিশাল ফাইলে ইমেইল ও পাসওয়ার্ড জোড়া হিসেবে একত্র করেছিল [8]।

3. নিরাপত্তা ইনসাইট

NIST এখন একমাত্র প্রমাণীকরণ উপাদান হিসেবে ব্যবহৃত পাসওয়ার্ড অন্তত 15 অক্ষরের হতে বাধ্যতামূলক করেছে [1]।

4. নিরাপত্তা ইনসাইট

ASIC হার্ডওয়্যার প্রতি সেকেন্ডে কোটি কোটি SHA-256 হ্যাশ গণনা করতে পারে, ফলে ব্যবহারকারীর পাসওয়ার্ডের জন্য কাঁচা SHA হ্যাশিং অনিরাপদ [2]।

5. নিরাপত্তা ইনসাইট

অনন্য সল্ট মানে একই পাসওয়ার্ডের দুজন ব্যবহারকারীর ডেটাবেসে ভিন্ন হ্যাশ থাকে [2]।

6. নিরাপত্তা ইনসাইট

অনেক পাসওয়ার্ড ম্যানেজার ব্যবহারকারীর মাস্টার পাসওয়ার্ড থেকে প্রাপ্ত শক্তিশালী ক্রিপ্টোগ্রাফি দিয়ে ভল্ট ডেটা স্থানীয়ভাবে এনক্রিপ্ট করে।

7. সিকিউরিটি ইনসাইট

ক্রেডেনশিয়াল স্টাফিং কাজ করে কারণ অনেকে ই-কমার্স, ব্যাংকিং ও ইমেইল অ্যাকাউন্টে একই পাসওয়ার্ড পুনরায় ব্যবহার করেন [3]।

8. সিকিউরিটি ইনসাইট

NIST SP 800-63B বলে, ভেরিফায়ার পর্যায়ক্রমিক পাসওয়ার্ড পরিবর্তন বাধ্যতামূলক করবে না, শুধু আপস হওয়ার প্রমাণ মিললে পরিবর্তন করাবে [1]।

9. সিকিউরিটি ইনসাইট

একটি ছোট পাসওয়ার্ডে একটিমাত্র বড় হাতের অক্ষর ও প্রতীক যোগ করলে আধুনিক স্বয়ংক্রিয় GPU ডিকশনারি আক্রমণ ঠেকানো যায় না [1]।

10. নিরাপত্তা ইনসাইট

MFA পাসওয়ার্ড ফাঁসের পরও অনেক ক্রেডেনশিয়াল-স্টাফিং প্রচেষ্টা ঠেকাতে পারে; ফিশিং-প্রতিরোধী MFA SMS কোডের চেয়ে শক্তিশালী [3]।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

স্টাডি গাইড ও ইন্টারঅ্যাক্টিভ ধাঁধাগুলো বৈশ্বিক NIST, OWASP এবং ডেটা গোপনীয়তা সম্মতির মানদণ্ড থেকে সংকলিত।

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[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/

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1 সঠিক উত্তর: A

শিক্ষণ নোট

ক্রেডেনশিয়াল স্টাফিং অটোমেশন ব্যবহার করে ফাঁস হওয়া ইউজারনেম/পাসওয়ার্ড জোড়া অন্য সাইটে চেষ্টা করে [3]।

2 প্রশ্ন 2 সঠিক উত্তর: A

শিক্ষণ নোট

OWASP প্রথমে Argon2id সুপারিশ করে; bcrypt মূলত পুরোনো সিস্টেমের জন্য, যেখানে Argon2id বা scrypt পাওয়া যায় না [2]।

3 প্রশ্ন 3 সঠিক উত্তর: A

শিক্ষণ নোট

MFA একটি অতিরিক্ত ফ্যাক্টর চায়, তাই শুধু চুরি হওয়া পাসওয়ার্ড দিয়ে অ্যাকাউন্ট খোলা যায় না [3]।

4 প্রশ্ন 4 সঠিক উত্তর: A

শিক্ষণ নোট

ব্রিচ ডাম্প হলো ফাঁস হওয়া ক্রেডেনশিয়ালের সংগ্রহ, যেমন 2019 সালের Collection #1 সংকলন [8]।

5 প্রশ্ন 5 সঠিক উত্তর: A

শিক্ষণ নোট

পাসওয়ার্ড ম্যানেজার প্রতিটি অ্যাকাউন্টের জন্য আলাদা, শক্তিশালী পাসওয়ার্ড তৈরি ও সংরক্ষণ করে, যা পুনর্ব্যবহার প্রতিরোধ করে [3]।

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সত্য: পুনর্ব্যবহৃত পাসওয়ার্ড আক্রমণকারীদের এক সাইট থেকে ফাঁস হওয়া ক্রেডেনশিয়াল অন্য সাইটে চালাতে দেয় [3]।

7 প্রশ্ন 7 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: SHA-1 একটি দ্রুত হ্যাশ; OWASP এর বদলে Argon2id, scrypt, bcrypt বা PBKDF2 সুপারিশ করে [2]।

8 প্রশ্ন 8 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: শুধু জটিলতার নিয়ম পুনর্ব্যবহৃত ফাঁস হওয়া পাসওয়ার্ড দিয়ে স্টাফিং ঠেকাতে পারে না; MFA লাগে [3]।

9 প্রশ্ন 9 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সত্য: মনিটরিং সেবা প্রকাশ পাওয়া ক্রেডেনশিয়ালের জন্য ব্রিচ ডাম্প ও ডার্ক ওয়েবের উৎসে খোঁজ করে [8]।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সত্য: প্রতিটি পাসওয়ার্ডের জন্য আলাদা সল্ট আগে থেকে হিসাব করা রেইনবো টেবিলকে অকার্যকর করে [2]।

শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট ৬ নম্বর) 1 নম্বর দিন।

চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

F 1. স্টাফিং	H 2. bcrypt	D 3. নিরাপত্তা লঙ্ঘন	G 4. সল্টিং
C 5. ম্যানেজার	B 6. MFA	A 7. রেইনবো	E 8. ফিশিং

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 স্টাফিং	2 bcrypt	3 লঙ্ঘন	4 সল্টিং
5 ম্যানেজার	6 এমএফএ		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 H – নকল	2 C – এলোমেলোসল্ট	3 B – ডেটালঙ্ঘন	4 G – অনলাইন
5 A – ক্রেডেনশিয়ালস্টাফিং	6 D – পাসওয়ার্ডভল্ট	7 E – এমএফএ	8 F – লগইন

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা স্টাফিং, bcrypt ও নিরাপত্তা লঙ্ঘন নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

কেস স্টাডি:
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

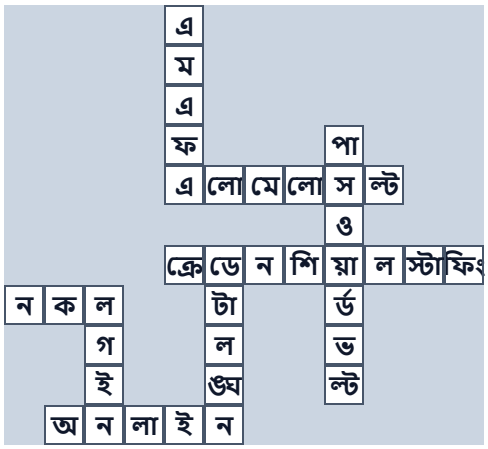
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

ণ	ল্ট	দ	নে	স	ঝ	কা	ন	জ	রা	ফ	ঘ	উ	সে	জি
আ	স	ড	প	পা	ধ	দ	ক	এ	জি	কি	না	লি	ই	রে
ফ	লো	চ	ব	দি	শ	জা	ল	রা	ম	দে	ট	মে	র	ক
সি	মে	দ	ঠ	হ	সা	শ	মে	দে	রা	এ	কি	ঋ	তে	না
নে	লো	ছ	য	প	ক্রে	উ	অ	উ	ঋ	মা	ফ	বা	অ	য
ফ	এ	বা	ম	দে	ডে	তি	পা	ভ	ঘ	রে	ষ	এ	ন	ফ
ন	ই	গ	ল	ঘ	ন	দ	হ	স	স	ভ	রি	মি	লা	ঢ
ন	ষ	ষ	রি	সি	শি	না	তি	তা	ও	ড	ঊ	নি	ই	রা
ঙ্ঘ	কি	থ	সে	ঊ	য়া	লি	গ	নি	জা	য়া	পি	ঋ	ন	জি
ল	লি	ট	ভ	ণ	ল	জে	গ	স	ঘ	রে	র্ড	দি	মি	ঋ
টা	পা	উ	অ	জে	স্টা	কা	গ	ম	আ	ঘ	কি	ভ	ঘ	ঝ
ডে	ণ	ধ	গ	সি	ফিং	রি	শ	ছ	দ	সে	জি	নি	ল্ট	ঝ
রে	পে	জ	আ	আ	রে	মা	স	মে	তি	দে	রি	ফ	সি	তি
সে	খ	স	বে	উ	ট	সে	দি	দা	প	আ	সি	জে	বি	বি
য	ড	দ	ষ	সা	ফ	ল	ল	তা	কে	ণ	রা	রি	ণ	জে

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

3 পাশাপাশি: এলোমেলোসল্ট পাসওয়ার্ড হ্যাশে এলোমেলো সল্ট যোগ করা (6 অক্ষর)

4 পাশাপাশি: ক্রেডেনশিয়ালস্টাফিং ফাঁস হওয়া লগইন তথ্য পরীক্ষা করা (8 অক্ষর)

6 পাশাপাশি: নকল আসল জিনিসের অবিকল অনুকরণ (3 অক্ষর)

8 পাশাপাশি: অনলাইন ইন্টারনেটের সঙ্গে সংযুক্ত থাকার অবস্থা (5 অক্ষর)

উপর-নিচ

1 উপর-নিচ: এমএফএ বহু-ধাপের লগইন যাচাই (5 অক্ষর)

2 উপর-নিচ: পাসওয়ার্ডভল্ট লগইন তথ্যের জন্য নিরাপদ স্থানীয় সংরক্ষণ-সরঞ্জাম (7 অক্ষর)

5 উপর-নিচ: ডেটালঙ্ঘন অননুমোদিত ডেটাবেস প্রকাশ (5 অক্ষর)

7 উপর-নিচ: লগইন নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

শব্দ সাজানোর উত্তরমালা

1.	স্টা শি য়া ক্রে ল ডে ফিং ন	ক্রেডেনশিয়ালস্টাফিং	5.	ল ন ডে ঙ্ঘ টা	ডেটালঙ্ঘন
2.	ল্ট এ মে স লো লো	এলোমেলোসল্ট	6.	ভ ও র্ড পা য়া ল্ট স	পাসওয়ার্ডভল্ট
3.	এ এ এ ফ ম	এমএফএ	7.	ই ল ন গ	লগইন
4.	লা ন ই অ ন	অনলাইন	8.	ল ক ন	নকল

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"বহুধাপ লগইনে ফাঁস পাসওয়ার্ড রক্ষা"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: এন্টারপ্রাইজ ক্রেডেনশিয়াল ফাঁসের প্রতিকার

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি ডার্ক ওয়েব পর্যবেক্ষণ সেবা একটি প্রতিষ্ঠানকে সতর্ক করে যে কর্পোরেট সিস্টেম অ্যাডমিনিস্ট্রেটরের পাসওয়ার্ডসহ একটি ডেটাবেস ডাম্প অনলাইনে প্রকাশিত হয়েছে।
- প্রস্তাবিত কৌশল ও সমাধান: সব সক্রিয় অ্যাডমিনিস্ট্রেটর সেশন বাতিল করুন এবং উচ্চ-এন্ট্রপির জেনারেটর দিয়ে ক্রেডেনশিয়াল রিসেট করুন। অ্যাডমিন পোর্টালে ফিশিং-প্রতিরোধী MFA চালু করুন [6], আক্রান্ত API কী বদলে ফেলুন, লগইন লগ পর্যালোচনা করুন, প্রাথমিক উন্মুক্ততার উৎস খুঁজে বের করুন এবং অন্যান্য সুবিধাপ্রাপ্ত অ্যাকাউন্ট পরীক্ষা করুন।

B কেস স্টাডি 2: পাসওয়ার্ড হ্যাশিং মান বাস্তবায়ন

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি এন্টারপ্রাইজ ডেটাবেস বর্তমানে ক্রিপ্টোগ্রাফিক সল্ট ছাড়া পুরোনো MD5 হ্যাশ ব্যবহার করে ব্যবহারকারীর পাসওয়ার্ড সংরক্ষণ করে, ফলে সেগুলো দ্রুত বের করে নেওয়ার ঝুঁকিতে রয়েছে।
- প্রস্তাবিত কৌশল ও সমাধান: প্রতিটি ব্যবহারকারীর জন্য আলাদা সল্টসহ Argon2id (বা পুরোনো সিস্টেমে bcrypt) গ্রহণ করুন [2]। বিদ্যমান MD5 হ্যাশগুলো এখনই নতুন অ্যালগরিদমে মুড়ে দিন, প্রতিটি ব্যবহারকারীর পরবর্তী লগইনে সরাসরি পুনরায় হ্যাশ করুন এবং দীর্ঘদিন নিষ্ক্রিয় অ্যাকাউন্টে রিসেট বাধ্যতামূলক করুন।