Họ tên: _____ Ngày: _____ Điểm: _____

Rò rỉ mật khẩu và bảo mật thông tin đăng nhập

Nhồi thông tin đăng nhập, rò rỉ dữ liệu, thuật toán băm, xác thực đa yếu tố và bảo mật mật khẩu.

TỔNG QUAN BÀI HỌC VỀ RÒ RỈ MẬT KHẨU

ĐÃ BẢO MẬT
MÃ HÓA DỮ LIỆU
Chuẩn AES 256 bit

TUÂN THỦ
TIÊU CHUẨN TOÀN CẦU
Khung GDPR và CCPA

ZERO TRUST
CHÍNH SÁCH TRUY CẬP
Xác thực đa yếu tố

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về rò rỉ mật khẩu và an ninh thông tin xác thực. Bạn sẽ khám phá tấn công nhồi thông tin xác thực (credential stuffing), vi phạm dữ liệu, thuật toán băm, xác thực đa yếu tố và trình quản lý mật khẩu.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- [ ] **Phần 1-4: Nắm vững an ninh mạng và phòng chống mối đe dọa.**
- [ ] **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- [ ] **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- [ ] **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- [ ] **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- [ ] **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn an ninh mạng của VPN.com

URL: https://www.vpn.com/vi/an-ninh-mang/mat-khau-bi-ro-ri/

Lộ trình học về bảo mật mật khẩu của bạn

- Hiểu về rủi ro lộ thông tin đăng nhập trên các diễn đàn dark web.
- Triển khai xác thực đa yếu tố (MFA) và giám sát thông tin đăng nhập bị xâm phạm.
- Thiết kế các biện pháp phòng thủ an ninh doanh nghiệp trước các chiêu lừa đảo kỹ thuật xã hội có chủ đích.

HƯỚNG DẪN VỀ RÒ RỈ MẬT KHẨU

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về việc bảo vệ thông tin đăng nhập. Kết thúc với hoạt động thưởng Nghĩ nhanh.

RÒ RỈ MẬT KHẨU & BẢO MẬT THÔNG TIN ĐĂNG NHẬP (GIỚI THIỆU)

Rò rỉ mật khẩu làm lộ thông tin đăng nhập của người dùng trên các trang web công khai và dark web. Mật khẩu duy nhất từ trình quản lý mật khẩu, sàng lọc mật khẩu bị lộ và xác thực đa yếu tố (MFA) giúp giảm rủi ro nhồi thông tin đăng nhập (credential stuffing), còn băm mật khẩu có salt và chậm sẽ hạn chế thiệt hại nếu cơ sở dữ liệu mật khẩu bị đánh cắp.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG.

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **Credential stuffing là gì?**
   - A. Dùng tự động hóa để thử các tổ hợp tên người dùng/mật khẩu bị lộ trên nhiều trang web
   - B. Mã hóa các tệp lưu trữ cơ sở dữ liệu cục bộ
   - C. Làm quá tải máy chủ web bằng các yêu cầu lưu lượng mạng
   - D. Giám sát thao tác bàn phím một cách bí mật

2. **Hiện nay OWASP liệt kê thuật toán nào là lựa chọn đầu tiên để lưu trữ mật khẩu?**
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. **Xác thực đa yếu tố (MFA) giảm thiểu rủi ro rò rỉ mật khẩu như thế nào?**
   - A. Nó yêu cầu thêm một yếu tố xác minh, nên chỉ riêng mật khẩu bị đánh cắp là không đủ
   - B. Nó tự động đổi mật khẩu mỗi giờ
   - C. Nó mã hóa tên người dùng trong quá trình truyền
   - D. Nó cảnh báo văn phòng tín dụng về các yêu cầu gian lận

4. **Bãi dữ liệu bị rò rỉ (data breach dump) là gì?**
   - A. Tập hợp thông tin xác thực người dùng bị lộ được đăng công khai trực tuyến hoặc bán trên các diễn đàn tin tặc
   - B. Bản sao lưu các tệp cơ sở dữ liệu được lưu ở nơi khác
   - C. Bộ đệm tạm thời của nhật ký máy chủ web
   - D. Một công cụ quản trị dùng để đặt lại mật khẩu người dùng

5. **Vai trò của trình quản lý mật khẩu là gì?**
   - A. Tạo và lưu trữ mật khẩu mạnh, duy nhất cho mọi tài khoản
   - B. Giám sát lưu lượng mạng để phát hiện rò rỉ mật khẩu
   - C. Chặn các cuộc tấn công dò mật khẩu tự động tại cổng
   - D. Quét các khối lưu trữ cơ sở dữ liệu để tìm mật khẩu chưa mã hóa

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Dùng lại mật khẩu trên nhiều tài khoản làm tăng rủi ro tấn công nhồi thông tin xác thực (credential stuffing).

○ Đúng ○ Sai

7 Câu hỏi 7

7. SHA-1 là hàm băm được khuyến nghị để lưu mật khẩu hiện đại.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Chỉ áp dụng độ phức tạp mật khẩu (không có MFA) là chặn đứng hoàn toàn việc nhồi thông tin đăng nhập.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Các công cụ giám sát web tối quét internet để tìm thông tin đăng nhập doanh nghiệp bị lộ.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Băm có muối thêm dữ liệu ngẫu nhiên duy nhất vào mật khẩu trước khi băm để chống tấn công bảng cầu vồng (rainbow table).

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Việc thử thông tin xác thực bị rò rỉ trên nhiều ứng dụng web là hình thức _____ đăng nhập.

2. Một thuật toán băm mật khẩu chậm, thích ứng mà OWASP vẫn chấp nhận là _____ .

3. Việc lộ các tệp cơ sở dữ liệu mật trên internet là một vụ _____ .

4. Việc chèn các giá trị ngẫu nhiên vào mật khẩu trước khi băm được gọi là _____ .

5. Một cơ sở dữ liệu cục bộ an toàn cho thông tin đăng nhập của người dùng là một _____ mật khẩu.

6. Bổ sung bước xác minh đăng nhập thứ hai là dùng _____ .

NGÂN HÀNG TỪ VỰNG

BẢNG CẦU VỒNG | BCRYPT | NHỒI THÔNG TIN | PHISHING | THÊM MUỐI
TRÌNH QUẢN LÝ | VI PHẠM DỮ LIỆU | XÁC THỰC MFA

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

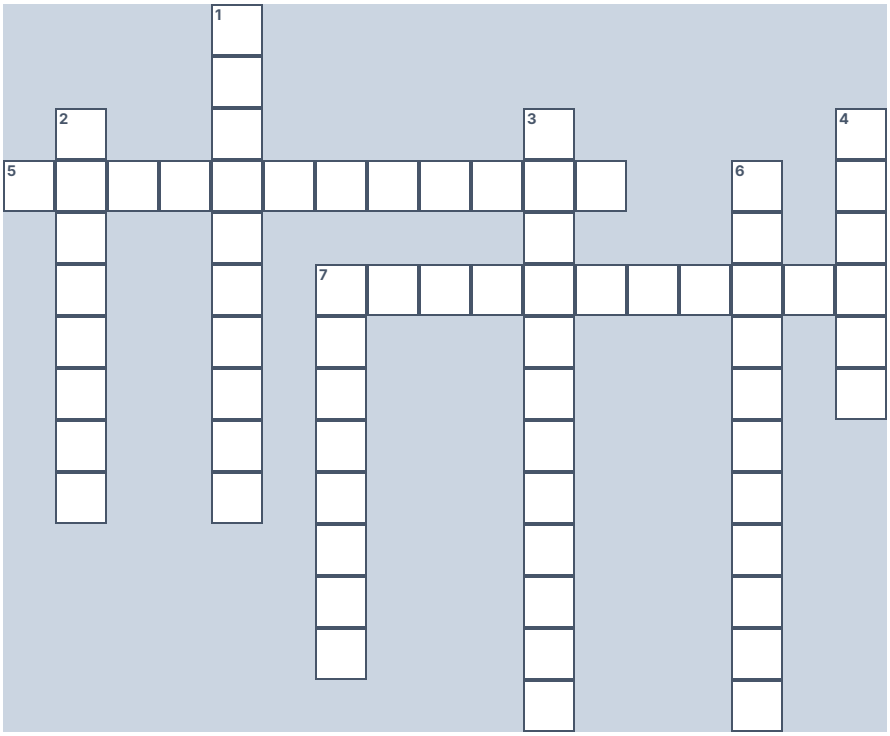
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. NHỒI NHÉT	A	Bảng băm mật khẩu được tính trước.
☐	2. BCRYPT	B	Kiểm tra đăng nhập đa yếu tố.
☐	3. VI PHẠM DỮ LIỆU	C	Công cụ lưu trữ thông tin đăng nhập.
☐	4. THÊM MUỐI	D	Lộ cơ sở dữ liệu trái phép.
☐	5. TRÌNH QUẢN LÝ	E	Kỹ thuật xã hội để đánh cắp thông tin đăng nhập.
☐	6. MFA	F	Thử nghiệm thông tin đăng nhập bị rò rỉ.
☐	7. CẦU VỒNG	G	Thêm salt ngẫu nhiên vào băm mật khẩu.
☐	8. PHISHING	H	Thuật toán băm mật khẩu chậm.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

5. Thử các thông tin đăng nhập bị rò rỉ (12)

7. Công cụ lưu trữ thông tin đăng nhập (11)

HÀNG DỌC

1. Kiểm tra đăng nhập đa yếu tố (10)

2. Thủ thuật tác động tâm lý để đánh cắp thông tin đăng nhập (8)

3. Cơ sở dữ liệu bị lộ trái phép (12)

4. Thuật toán băm mật khẩu chậm (6)

6. Bảng mã băm mật khẩu tính toán trước (11)

7. Thêm giá trị ngẫu nhiên vào mã băm mật khẩu (8)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

5 hàng ngang: Thử các thông tin đăng nhập bị rò rỉ (12 chữ cái):

7 hàng ngang: Công cụ lưu trữ thông tin đăng nhập (11 chữ cái):

HÀNG DỌC

1 hàng dọc: Kiểm tra đăng nhập đa yếu tố (10 chữ cái):

2 hàng dọc: Thủ thuật tác động tâm lý để đánh cắp thông tin đăng nhập (8 chữ cái):

3 hàng dọc: Cơ sở dữ liệu bị lộ trái phép (12 chữ cái):

4 hàng dọc: Thuật toán băm mật khẩu chậm (6 chữ cái):

6 hàng dọc: Bảng mã băm mật khẩu tính toán trước (11 chữ cái):

7 hàng dọc: Thêm giá trị ngẫu nhiên vào mã băm mật khẩu (8 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

U T I P Ă Ư Y V L P Ơ V G O C

Ê A A F M C Ư H T C A X B B P

I I Ơ U Ư Ư K H Ê S Ê Đ C H Ă

L D G I T R Q U P Y D R I Ê D

Ư Q Â A H K Ô Â Y L Y S I T U

D P S A Ê Q Ư H L P H L E R Ê

M M Ê P M Đ K R T I K P Ư I Ê

A Ă S Đ M X N X N Ư Q Ê R N V

H A Ô T U N N G Y O G Ô R H Ê

P Ô T S Ô O S S I A D O M Q K

I N H Ô I T H Ô N G T I N U Ă

V N T Đ E Ô Ơ Ư X H I T H A X

U V B A N G C Â U V Ô N G N Ô

I G Y G H M A D G Ă R A H L D

U D I Y I C K Ơ M H A Đ O Y I

DANH SÁCH TỪ VỰNG

NHÔITHÔNGTIN BCRYPT VIPHAMDỮLIÊU THÊMMUÔI TRINHQUANLY
XACTHƯCMFA BANGCÂUVÔNG PHISHING

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG

A. NHÔITHÔNGTIN

B. BCRYPT

C. VIPHAMDƯLIÊU

D. THÊMMUÔI

E. TRINHQUANLY

F. XACTHƯCMFA

G. BANGCÂUVÔNG

H. PHISHING

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP

_____ 1. Thủ thuật tác động tâm lý để đánh cắp thông tin đăng nhập.

_____ 2. Cơ sở dữ liệu bị lộ trái phép.

_____ 3. Thuật toán băm mật khẩu chậm.

_____ 4. Bảng mã băm mật khẩu tính toán trước.

_____ 5. Thử các thông tin đăng nhập bị rò rỉ.

_____ 6. Thêm giá trị ngẫu nhiên vào mã băm mật khẩu.

_____ 7. Công cụ lưu trữ thông tin đăng nhập.

_____ 8. Kiểm tra đăng nhập đa yếu tố.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về an ninh mạng. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. GHNTHÔTNIÔNI
2. UIAMVIÊPƯLDH
3. TUQAIRLYHNN
4. UNGÂNCÔVBAG
5. YRTBPC
6. ÔIMUTMHÊ
7. ATXCƯMFAHC
8. SHHGPNII

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
2	Những quy tắc cho một mật khẩu mạnh			
3	Những trình quản lý mật khẩu bạn biết			
4	Những công cụ bảo mật bạn biết			
5	Những dấu hiệu cảnh báo trong một email			
6	Những từ vui cho một cụm mật khẩu dài			
7	Những cách đăng nhập không cần mật khẩu			
8	Những thông tin bạn không bao giờ nên chia sẻ			
9	Lý do cập nhật phần mềm			
10	Những việc cần làm khi mật khẩu bị rò rỉ			
11	Những tài khoản cần MFA			
12	Những nơi không bao giờ nên lưu mật khẩu			
13	Những dấu hiệu máy tính bị nhiễm			
14	Những mật khẩu yếu mọi người dùng			
15	Những thứ bạn sao lưu			

Điểm kiểm tra 8: Nghiên cứu tình huống về an ninh mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: XỬ LÝ RÒ RỈ THÔNG TIN ĐĂNG NHẬP CỦA DOANH NGHIỆP

👷

Tình huống: Một dịch vụ giám sát dark web cảnh báo một tổ chức rằng một bản dữ liệu rò rỉ chứa mật khẩu của quản trị viên hệ thống công ty đã được đăng công khai trên mạng.

Câu hỏi thảo luận: Hãy phân tích các rủi ro rò rỉ thông tin đăng nhập, và đề xuất một chiến lược đặt lại về mặt quản trị.

NGHIÊN CỨU TÌNH HUỐNG 2: ÁP DỤNG TIÊU CHUẨN BĂM MẬT KHẨU

👷

Tình huống: Một cơ sở dữ liệu doanh nghiệp hiện lưu mật khẩu người dùng bằng các hàm băm MD5 lỗi thời mà không có salt mật mã, khiến chúng dễ bị trích xuất nhanh chóng.

Câu hỏi thảo luận: Hãy thiết kế một chiến lược di chuyển để nâng cấp thuật toán băm của cơ sở dữ liệu.

Điểm kiểm tra 9: Giải mã mật thư

Chuyên gia an ninh mạng bảo vệ tài sản mạng khỏi các tác nhân đe dọa trực tuyến. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

4	1	17		27	9		15	3	24		13	11	3	25		4	12		14	18
4	2	16	10		7	2	16	10		16	11	3	20		7	1		29	9	25
										24	18									

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q1: Rò rỉ mật khẩu là gì?

Rò rỉ mật khẩu xảy ra khi thông tin đăng nhập của người dùng bị lộ qua các vụ xâm phạm dữ liệu hoặc cấu hình sai máy chủ.

Q2: Tin tặc tìm mật khẩu bị rò rỉ như thế nào?

Tin tặc quét các diễn đàn dark web, các bản sao cơ sở dữ liệu công khai và các trang dán nội dung nơi dữ liệu bị lộ được đăng tải [8].

Q3: Dùng lại mật khẩu có nguy hiểm không?

Có, vì nếu một trang web bị xâm phạm, tin tặc có thể thử cùng thông tin đăng nhập đó trên hàng nghìn nền tảng khác [3].

Q4: Salt mật mã là gì?

Salt là dữ liệu ngẫu nhiên được thêm vào mật khẩu trước khi băm, làm cho các tấn công tra cứu tính toán trước trở nên vô hiệu [2].

Q5: Vì sao MD5 đã lỗi thời?

MD5 là hàm băm đa dụng nhanh và đã lỗi thời, nên kẻ tấn công có thể thử đoán mật khẩu cực nhanh, đặc biệt khi mã băm không có muối [2].

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q6: Trình quản lý mật khẩu bảo vệ người dùng như thế nào?

Nó tự động tạo thông tin đăng nhập phức tạp, duy nhất cho mọi trang, giảm lỗi ghi nhớ của con người và việc dùng lại.

Q7: Tấn công vét cạn (brute force) là gì?

Cuộc tấn công thử một cách có hệ thống mọi tổ hợp ký tự có thể cho đến khi tìm ra mật khẩu đúng [4].

Q8: Khóa tài khoản giúp ích như thế nào?

Khóa tài khoản hoặc giới hạn tốc độ làm chậm việc đoán mật khẩu trực tuyến lặp lại và, khi kết hợp với giám sát và MFA, giúp giảm rủi ro tấn công vét cạn [4].

Q9: Mật khẩu chính có an toàn không?

Chúng an toàn nếu là các cụm mật khẩu có entropy cao và không bao giờ dùng lại trên các hệ thống web khác.

Q10: Có nên đổi mật khẩu thường xuyên không?

NIST nêu rằng không nên buộc đổi mật khẩu định kỳ; hãy đổi khi có bằng chứng bị xâm phạm và ưu tiên độ dài, danh sách chặn và MFA [1].

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q1: Argon2 so với bcrypt như thế nào?

OWASP liệt kê Argon2id là lựa chọn hàng đầu; các thiết lập tốn nhiều bộ nhớ của nó chống bẻ khóa bằng GPU và ASIC tốt hơn bcrypt [2].

Q2: Kéo giãn khóa (key stretching) là gì?

Kỹ thuật lặp thuật toán băm hàng nghìn lần để làm chậm quá trình xác minh mật khẩu, khiến việc bẻ khóa tốn kém [2].

Q3: Bảng cầu vồng hoạt động như thế nào?

Đó là các bảng tra cứu tính toán sẵn liên kết mật khẩu văn bản thuần với giá trị băm của chúng, dùng để đảo ngược nhanh các giá trị băm không có salt [2].

Q4: Tái sử dụng thông tin đăng nhập là gì?

Dùng lại các cặp tên người dùng/mật khẩu bị đánh cắp từ một vụ vi phạm để thử truy cập các dịch vụ khác, đặc biệt khi mọi người dùng lại mật khẩu [3].

Q5: Trình quản lý mật khẩu có thể bị tấn công không?

Có. Nhiều dịch vụ dùng mã hóa zero-knowledge, nên vi phạm máy chủ chỉ làm lộ các kho đã mã hóa, nhưng mật khẩu chính yếu vẫn có thể bị bẻ khóa ngoại tuyến.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q6: Tấn công từ điển là gì?

Biến thể của tấn công vét cạn thử các từ thông dụng, cụm từ và mật khẩu từng bị lộ trước đây thay vì các chữ cái ngẫu nhiên.

Q7: Vì sao cụm từ mật khẩu (passphrase) được ưu tiên hơn?

Cụm từ mật khẩu dùng nhiều từ ngẫu nhiên, tạo độ ngẫu nhiên (entropy) cao, dễ nhớ với con người nhưng tốn kém về tính toán để bẻ khóa [1].

Q8: Đăng nhập một lần (SSO) ảnh hưởng thế nào đến việc rò rỉ mật khẩu?

SSO giảm tình trạng nhiều mật khẩu tràn lan, nhưng nhà cung cấp danh tính trở thành mục tiêu giá trị cao cần MFA mạnh, tốt nhất là chống lừa đảo trực tuyến (phishing) [6].

Q9: Chiếm quyền phiên là gì?

Kẻ tấn công lấy hoặc lạm dụng mã thông báo phiên hợp lệ để mạo danh người dùng đã đăng nhập mà không cần mật khẩu nữa [5].

Q10: Làm thế nào để phát hiện tấn công dò mật khẩu hàng loạt (password spraying)?

Bằng cách tìm kiếm việc cùng một vài mật khẩu được thử trên nhiều tài khoản, thường là thử chậm để nằm dưới ngưỡng khóa tài khoản [7].

Phần 11: 10 sự thật và hiểu biết thực tế về an ninh mạng

Xem lại các sự thật thực tế về vi phạm bảo mật, cơ chế phòng thủ và tiêu chuẩn tuân thủ.

1. THÔNG TIN VỀ AN NINH

NIST SP 800-63B yêu cầu mật khẩu mới phải được kiểm tra đối chiếu với danh sách chặn các mật khẩu phổ biến và đã bị lộ [1].

2. THÔNG TIN VỀ AN NINH

Bản kết xuất 'Collection #1' năm 2019 đã gộp dữ liệu từ nhiều vụ vi phạm trước đó thành một tệp khổng lồ gồm các cặp email và mật khẩu [8].

3. THÔNG TIN VỀ AN NINH

NIST hiện yêu cầu mật khẩu được dùng làm yếu tố xác thực duy nhất phải dài ít nhất 15 ký tự [1].

4. THÔNG TIN VỀ AN NINH

Phần cứng ASIC có thể tính hàng tỷ giá trị băm SHA-256 mỗi giây, khiến việc băm SHA thô không an toàn cho mật khẩu người dùng [2].

5. THÔNG TIN VỀ AN NINH

Salt duy nhất nghĩa là hai người dùng có cùng một mật khẩu vẫn có giá trị băm khác nhau trong cơ sở dữ liệu [2].

6. THÔNG TIN VỀ AN NINH

Nhiều trình quản lý mật khẩu mã hóa dữ liệu kho ở máy cục bộ bằng mật mã mạnh bắt nguồn từ mật khẩu chính của người dùng.

7. THÔNG TIN VỀ BẢO MẬT

Tấn công nhồi thông tin đăng nhập hiệu quả vì nhiều người dùng lại cùng một mật khẩu cho các tài khoản thương mại điện tử, ngân hàng và email [3].

8. THÔNG TIN VỀ BẢO MẬT

NIST SP 800-63B nêu rằng bên xác minh không được yêu cầu đổi mật khẩu định kỳ, chỉ đổi khi có bằng chứng bị xâm phạm [1].

9. THÔNG TIN VỀ BẢO MẬT

Thêm một chữ cái viết hoa và một ký hiệu vào mật khẩu ngắn không ngăn được các tấn công từ điển bằng GPU tự động hiện đại [1].

10. THÔNG TIN VỀ AN NINH

MFA có thể chặn nhiều nỗ lực nhồi thông tin đăng nhập ngay cả sau khi mật khẩu bị rò rỉ; MFA chống lừa đảo trực tuyến (phishing) mạnh hơn mã SMS [3].

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn toàn cầu của NIST, OWASP và tuân thủ quyền riêng tư dữ liệu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[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/

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 **Câu hỏi 1** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Nhồi thông tin đăng nhập dùng tự động hóa để thử các cặp tên người dùng/mật khẩu bị rò rỉ trên các trang web khác [3].

2 **Câu hỏi 2** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

OWASP khuyến nghị Argon2id trước tiên; bcrypt chủ yếu dành cho các hệ thống cũ không có Argon2id hoặc scrypt [2].

3 **Câu hỏi 3** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

MFA yêu cầu thêm một yếu tố, nên chỉ riêng mật khẩu bị đánh cắp không thể mở khóa tài khoản [3].

4 **Câu hỏi 4** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Các bộ dữ liệu rò rỉ là tập hợp thông tin đăng nhập bị lộ, chẳng hạn bản tổng hợp Collection #1 năm 2019 [8].

5 **Câu hỏi 5** — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Trình quản lý mật khẩu tạo và lưu một mật khẩu mạnh, duy nhất cho mọi tài khoản, ngăn việc dùng lại [3].

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Đúng: mật khẩu dùng lại cho phép kẻ tấn công phát lại thông tin đăng nhập bị rò rỉ từ một trang web sang các trang web khác [3].

7 **Câu hỏi 7** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: SHA-1 là hàm băm nhanh; thay vào đó OWASP khuyến nghị Argon2id, scrypt, bcrypt hoặc PBKDF2 [2].

8 **Câu hỏi 8** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sai: chỉ riêng các quy tắc về độ phức tạp không thể ngăn việc nhồi các mật khẩu bị rò rỉ được dùng lại; cần có MFA [3].

9 **Câu hỏi 9** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Đúng: các dịch vụ giám sát tìm kiếm trong các bộ dữ liệu rò rỉ và các nguồn dark web để phát hiện thông tin đăng nhập bị lộ [8].

10 **Câu hỏi 10** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Đúng: một salt duy nhất cho mỗi mật khẩu khiến các bảng cầu vồng tính toán trước trở nên vô hiệu [2].

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

F 1. NHỒI NHÉT	H 2. BCRYPT	D 3. VI PHẠM DỮ LIỆU	G 4. THÊM MUỐI
C 5. TRÌNH QUẢN LÝ	B 6. MFA	A 7. CẦU VỒNG	E 8. PHISHING

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 NHỒI THÔNG TIN	2 BCRYPT	3 VI PHẠM DỮ LIỆU	4 THÊM MUỐI
5 TRÌNH QUẢN LÝ	6 XÁC THỰC MFA		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 H – PHISHING	2 C – VIPHAMDỮLIỆU	3 B – BCRYPT	4 G – BANGCÂUVÔNG
5 A – NHỒITHÔNGTIN	6 D – THÊMMUỐI	7 E – TRINHQUANLY	8 F – XACTHỰCMFA

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được NHỒI NHÉT, BCRYPT và VI PHẠM DỮ LIỆU bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

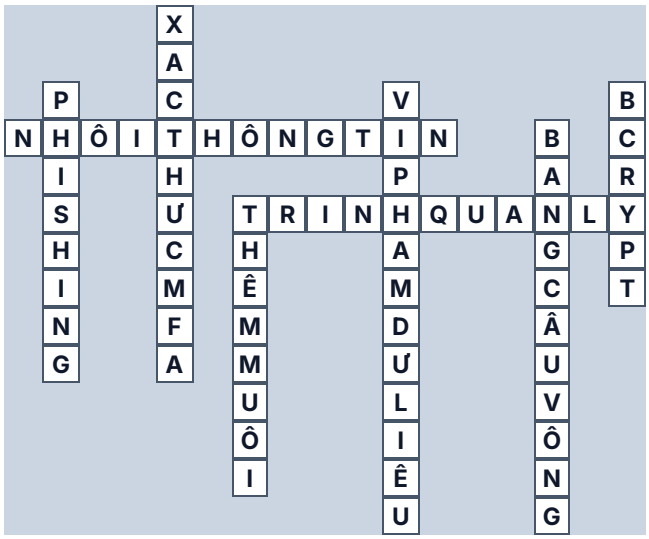
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

U	T	I	P	Ă	Ư	Y	V	L	P	Ơ	V	G	O	C
Ê	A	A	F	M	C	Ư	H	T	C	A	X	B	B	P
I	I	Ơ	U	Ư	Ư	K	H	Ê	S	Ê	Đ	C	H	Ă
L	D	G	I	T	R	Q	U	P	Y	D	R	I	Ê	D
Ư	Q	Â	A	H	K	Ô	Â	Y	L	Y	S	I	T	U
D	P	S	A	Ê	Q	Ư	H	L	P	H	L	E	R	Ê
M	M	Ê	P	M	Đ	K	R	T	I	K	P	Ư	I	Ê
A	Ă	S	Đ	M	X	N	X	N	Ư	Q	Ê	R	N	V
H	A	Ô	T	U	N	N	G	Y	O	G	Ô	R	H	Ê
P	Ô	T	S	Ô	O	S	S	I	A	D	O	M	Q	K
I	N	H	Ô	I	T	H	Ô	N	G	T	I	N	U	Ă
V	N	T	Đ	E	Ô	Ơ	Ư	X	H	I	T	H	A	X
U	V	B	A	N	G	C	Â	U	V	Ô	N	G	N	Ô
I	G	Y	G	H	M	A	D	G	Ă	R	A	H	L	D
U	D	I	Y	I	C	K	Ơ	M	H	A	Đ	O	Y	I

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

5 hàng ngang: NHÔITHÔNGTIN Thử các thông tin đăng nhập bị rò rỉ (12 chữ cái)

7 hàng ngang: TRINHQUANLY Công cụ lưu trữ thông tin đăng nhập (11 chữ cái)

HÀNG DỌC

1 hàng dọc: XACTHƯCMFA Kiểm tra đăng nhập đa yếu tố (10 chữ cái)

2 hàng dọc: PHISHING Thủ thuật tác động tâm lý để đánh cắp thông tin đăng nhập (8 chữ cái)

3 hàng dọc: VIPHAMDƯLIÊU Cơ sở dữ liệu bị lộ trái phép (12 chữ cái)

4 hàng dọc: BCRYPT Thuật toán băm mật khẩu chậm (6 chữ cái)

6 hàng dọc: BANGCÂUVÔNG Bảng mã băm mật khẩu tính toán trước (11 chữ cái)

7 hàng dọc: THÊMMUÔI Thêm giá trị ngẫu nhiên vào mã băm mật khẩu (8 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1. GHNTHÔTNIÔNI — **NHÔITHÔNGTIN**
2. UIAMVIÊPƯLDH — **VIPHAMDƯLIÊU**
3. TUQAIRLYHNN — **TRINHQUANLY**
4. UNGÂNCÔVBAG — **BANGCÂUVÔNG**
5. YRTBPC — **BCRYPT**
6. ÔIMUTMHÊ — **THÊMMUÔI**
7. ATXCƯMFAHC — **XACTHƯCMFA**
8. SHHGPNII — **PHISHING**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"BAO VÊ MÂT KHÂU BI LÔ BĂNG ĐĂNG NHÂP ĐA YÊU TÔ"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Xử lý rò rỉ thông tin đăng nhập của doanh nghiệp

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một dịch vụ giám sát dark web cảnh báo một tổ chức rằng một bản sao cơ sở dữ liệu chứa mật khẩu quản trị viên hệ thống của doanh nghiệp đã bị công bố trực tuyến.
- Chiến lược và giải pháp đề xuất: Thu hồi mọi phiên quản trị viên đang hoạt động và đặt lại thông tin xác thực bằng trình tạo có độ ngẫu nhiên cao. Áp dụng MFA chống lừa đảo trực tuyến (phishing) trên các cổng quản trị [6], xoay vòng các khóa API bị ảnh hưởng, xem lại nhật ký đăng nhập, tìm ra điểm bị lộ ban đầu và kiểm tra các tài khoản đặc quyền khác.

B Nghiên cứu tình huống 2: Áp dụng tiêu chuẩn băm mật khẩu

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một cơ sở dữ liệu doanh nghiệp hiện lưu mật khẩu người dùng bằng mã băm MD5 lỗi thời và không có salt mật mã, khiến chúng dễ bị trích xuất nhanh chóng.
- Chiến lược và giải pháp đề xuất: Áp dụng Argon2id (hoặc bcrypt trên các hệ thống cũ) với salt riêng cho từng người dùng [2]. Bọc ngay các mã băm MD5 hiện có trong thuật toán mới, băm lại trực tiếp ở lần đăng nhập tiếp theo của mỗi người dùng và buộc đặt lại mật khẩu đối với các tài khoản không hoạt động lâu ngày.