이름: _____ 날짜: _____ 점수: _____

비밀번호 유출과 자격 증명 보안

자격 증명 스터핑, 데이터 침해, 해시 알고리즘, 다단계 인증, 비밀번호 보안.

비밀번호 유출 학습 개요

보호됨
데이터 암호화
256비트 AES 표준

규정 준수
글로벌 표준
GDPR 및 CCPA 규정 체계

제로 트러스트
접근 정책
다중 요소 인증

환영합니다! 이 활동 자료집은 비밀번호 유출과 자격 증명 보안을 안내합니다. 크리덴셜 스터핑, 데이터 침해, 해시 알고리즘, 다중 인증, 비밀번호 관리자를 살펴봅니다.

워크시트 체크포인트

- [ ] **파트 1-4: 사이버 보안과 위협 예방을 익힙니다.**
- [ ] **파트 5-7: 십자말풀이와 단어 찾기 퍼즐을 풉니다.**
- [ ] **파트 8-9: 사례 연구와 암호 도전 과제를 풉니다.**
- [ ] **파트 10: 기초 및 심화 FAQ 페이지를 살펴봅니다.**
- [ ] **파트 11: 흥미로운 실제 사실 10가지를 살펴봅니다.**
- [ ] **보너스: 빠르게 생각하기 도전**

VPN.com 사이버 보안 가이드 열기

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

나의 비밀번호 보안 학습 로드맵

- 다크 웹 포럼에서 자격 증명이 노출될 위험을 이해합니다.
- 다중 인증(MFA)과 유출된 인증 정보 모니터링을 도입하세요.
- 표적형 사회공학 사기에 대비한 기업 보안 방어 체계를 설계하세요.

비밀번호 유출 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 자격 증명 보호에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

비밀번호 유출과 자격 증명 보안(소개)

비밀번호 유출은 공개 웹과 다크 웹 사이트에 사용자 자격 증명을 노출합니다. 비밀번호 관리자의 고유한 비밀번호, 유출된 비밀번호 검사, 다단계 인증(MFA)은 크리덴셜 스터핑의 위험을 줄이고, 솔트를 적용한 느린 비밀번호 해싱은 비밀번호 데이터베이스가 도난당했을 때의 피해를 제한합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 크리덴셜 스터핑이란 무엇입니까?

- A. 자동화를 사용해 유출된 사용자 이름/비밀번호 조합을 여러 사이트에서 시험함
- B. 로컬 데이터베이스 저장 파일 암호화하기
- C. 웹 서버에 네트워크 트래픽 요청을 폭주시키기
- D. 키보드 입력을 몰래 감시하기

2 2. OWASP가 현재 비밀번호 저장에 첫 번째로 권장하는 알고리즘은 무엇입니까?

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

3 3. 다중 인증(MFA)은 비밀번호 유출의 위험을 어떻게 줄입니까?

- A. 추가 인증 요소를 요구하므로 도난당한 비밀번호만으로는 충분하지 않다
- B. 비밀번호를 한 시간마다 자동으로 변경한다
- C. 전송 중에 사용자 이름을 암호화한다
- D. 신용 평가 기관에 사기성 요청을 알린다

4 4. 데이터 유출 덤프란 무엇입니까?

- A. 온라인에 게시되거나 해커 포럼에서 판매되는 유출된 사용자 자격 증명 모음
- B. 외부에 보관된 데이터베이스 파일 백업본
- C. 웹 서버 로그의 임시 캐시
- D. 사용자 비밀번호를 재설정하는 데 쓰는 관리 도구

5 5. 비밀번호 관리자의 역할은 무엇입니까?

- A. 계정마다 고유하고 강력한 비밀번호를 생성하고 저장함
- B. 비밀번호 유출이 있는지 네트워크 트래픽 모니터링하기
- C. 게이트웨이에서 자동화된 무차별 대입 공격 차단하기
- D. 데이터베이스 저장 블록에서 암호화되지 않은 비밀번호 검색하기

체크포인트 2: 참/거짓 도전

6 질문 6

6. 여러 계정에 같은 비밀번호를 재사용하면 크리덴셜 스터핑 위험이 커집니다.

○ 참 ○ 거짓

7 질문 7

7. SHA-1은 최신 비밀번호 저장에 권장되는 해시 함수입니다.

○ 참 ○ 거짓

8 질문 8

8. 비밀번호 복잡성만 강제하면(MFA 없이) 크리덴셜 스터핑을 완전히 막을 수 있습니다.

○ 참 ○ 거짓

9 질문 9

9. 다크웹 모니터링 도구는 인터넷을 검색하여 유출된 기업 인증 정보를 찾습니다.

○ 참 ○ 거짓

10 질문 10

10. 솔트가 적용된 해시는 해시하기 전에 비밀번호에 고유한 무작위 데이터를 더해 레인보우 테이블 공격을 무력화합니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

아래 각 문장을 읽고 단어 목록에서 알맞은 용어를 골라 빈칸을 채우세요.

1. 유출된 자격 증명을 여러 웹 애플리케이션에 시도하는 공격을 크리덴셜 _____ (이)라고 합니다.

2. OWASP가 여전히 인정하는 느리고 적응형인 비밀번호 해시 알고리즘은 _____ 입니다.

3. 기밀 데이터베이스 파일이 인터넷에 노출되는 것을 데이터 _____ (이)라고 합니다.

4. 해시하기 전에 비밀번호에 무작위 값을 더하는 것을 _____ (이)라고 합니다.

5. 사용자 자격 증명을 보관하는 안전한 로컬 데이터베이스는 비밀번호 _____ 입니다.

6. 두 번째 로그인 확인 단계를 추가하는 방법은 _____ 입니다.

어휘 단어 목록

관리자 | 다단계 인증 | 레인보우 | 사전 공격 | 솔팅 | 스터핑 | 침해 | bcrypt

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

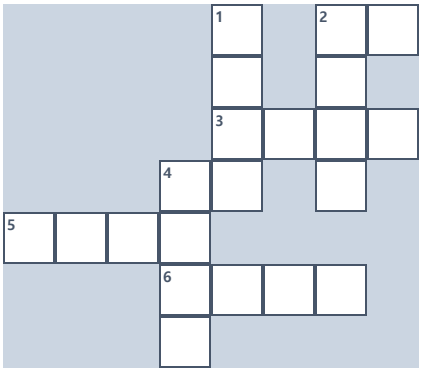
정의 연결하기

왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. 스터핑**	**A**	미리 계산된 비밀번호 해시 표.
☐	**2. bcrypt**	**B**	다중 요소 로그인 확인.
☐	**3. 침해**	**C**	자격 증명 저장 도구.
☐	**4. 솔팅**	**D**	무단 데이터베이스 노출.
☐	**5. 관리자**	**E**	로그인 정보를 훔치는 사회공학.
☐	**6. MFA**	**F**	유출된 로그인 정보를 시험해 보는 행위.
☐	**7. 레인보우**	**G**	비밀번호 해시에 무작위 솔트를 추가함.
☐	**8. 피싱**	**H**	느린 비밀번호 해싱 알고리즘.

체크포인트 5: 십자말풀이

활성화된 흰색 칸에 글자를 입력해 십자말풀이를 푸세요. 숫자는 아래 열쇠에 해당합니다.



가로

2. 남을 속여 돈이나 이익을 가로채는 범죄 (2)

3. 자주 쓰는 단어를 하나씩 넣어 비밀번호를 알아내려는 공격 (4)

4. 범죄나 피해 사실을 관계 기관에 알리는 일 (2)

5. 남의 이름이나 정보를 허락 없이 사용하는 범죄 (4)

6. 개인 정보가 허가 없이 외부로 새어 나가는 일 (4)

세로

1. 해킹 등으로 정보 시스템이 뚫려 정보가 노출된 사건 (4)

2. 사람의 심리를 이용해 정보를 빼내는 수법 (4)

4. 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

화면 낭독기와 키보드 사용자는 아래 입력란에 십자말풀이 정답을 직접 입력할 수 있습니다.

가로

2 가로: 남을 속여 돈이나 이익을 가로채는 범죄 (2 글자):

3 가로: 자주 쓰는 단어를 하나씩 넣어 비밀번호를 알아내려는 공격 (4 글자):

4 가로: 범죄나 피해 사실을 관계 기관에 알리는 일 (2 글자):

5 가로: 남의 이름이나 정보를 허락 없이 사용하는 범죄 (4 글자):

6 가로: 개인 정보가 허가 없이 외부로 새어 나가는 일 (4 글자):

세로

1 세로: 해킹 등으로 정보 시스템이 뚫려 정보가 노출된 사건 (4 글자):

2 세로: 사람의 심리를 이용해 정보를 빼내는 수법 (4 글자):

4 세로: 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보 (4 글자):

체크포인트 6: 숨은 단어 찾기

아래 격자에 숨어 있는 핵심 어휘 8개를 찾으세요. 단어는 가로, 세로, 대각선으로 배치될 수 있습니다.

청 템 해 라 인 소 다 서 색 하 크 유 메 고 템
타 비 속 결 방 트 공 비 사 라 메 카 다 리 방
접 학 워 학 카 파 라 이 워 기 기 템 이 안 송
보 공 공 터 타 바 시 회 다 트 인 요 술 호 회
연 회 시 검 다 정 위 터 파 터 신 번 침 공 명
버 사 개 비 자 보 리 침 기 버 전 험 밀 신 고
개 신 격 연 아 유 소 스 해 도 하 벽 인 바 가
마 사 접 명 벽 출 터 의 화 사 신 주 방 타 위
격 번 터 카 기 이 데 방 격 속 고 트 데 데 격
공 관 스 주 메 네 사 스 공 연 호 리 바 검 카
전 신 용 정 보 템 해 청 아 회 검 서 방 크 학
사 카 데 타 명 위 출 속 사 요 마 가 학 송 카
화 나 타 연 의 타 안 워 기 차 관 격 번 하 기
리 회 템 안 도 위 답 보 나 다 험 접 이 개 주
명 격 터 리 용 주 시 자 이 침 마 버 리 신 유

어휘 단어 목록

정보유출 신용정보 사기 명의도용 신고 침해사고 사회공학 사전공격

체크포인트 6 대체 활동: 접근성을 고려한 어휘 연결

단어 찾기의 8개 어휘를 각각 알맞은 설명과 연결하고, 빈칸에 글자(A-H)를 쓰세요.

어휘 용어
A. 정보유출
B. 신용정보
C. 사기
D. 명의도용
E. 신고
F. 침해사고
G. 사회공학
H. 사전공격

정의 및 연결 항목
____ 1. 자주 쓰는 단어를 하나씩 넣어 비밀번호를 알아내려는 공격.
____ 2. 남을 속여 돈이나 이익을 가로채는 범죄.
____ 3. 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보.
____ 4. 사람의 심리를 이용해 정보를 빼내는 수법.
____ 5. 개인 정보가 허가 없이 외부로 새어 나가는 일.
____ 6. 남의 이름이나 정보를 허락 없이 사용하는 범죄.
____ 7. 범죄나 피해 사실을 관계 기관에 알리는 일.
____ 8. 해킹 등으로 정보 시스템이 뚫려 정보가 노출된 사건.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 사이버 보안 개념과 용어를 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 유 정 출 보 _____
2. 기 사 _____
3. 고 신 _____
4. 학 공 사 회 _____
5. 보 신 정 용 _____
6. 도 용 명 의 _____
7. 사 침 고 해 _____
8. 사 격 공 전 _____

보너스 활동: 빠르게 생각하기

각 범주마다 답을 3개씩 쓰세요. 목록을 가장 먼저 채운 사람이 이깁니다.

1	오늘부터 시작할 수 있는 안전 습관			
2	강력한 비밀번호를 위한 규칙			
3	알고 있는 비밀번호 관리자			
4	알고 있는 보안 도구			
5	이메일의 경고 신호			
6	긴 암호문에 쓸 재미있는 단어			
7	비밀번호 없이 로그인하는 방법			
8	절대 공유하면 안 되는 정보			
9	소프트웨어를 업데이트하는 이유			
10	비밀번호가 유출되었을 때 할 일			
11	MFA가 필요한 계정			
12	비밀번호를 절대 저장하면 안 되는 곳			
13	컴퓨터가 감염되었다는 신호			
14	사람들이 사용하는 나쁜 비밀번호			
15	백업하는 것			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 기업 자격 증명 유출 대응

👷

상황: 다크 웹 모니터링 서비스가 한 조직에 회사 시스템 관리자의 비밀번호가 담긴 데이터베이스 유출본이 온라인에 게시되었다고 알립니다.

토론 질문: 자격 증명 유출 위험을 분석하고, 관리 차원의 초기화 전략을 제안하세요.

사례 연구 2: 비밀번호 해싱 표준 적용하기

👷

상황: 한 기업 데이터베이스가 현재 암호화 솔트 없이 오래된 MD5 해시로 사용자 비밀번호를 저장하고 있어 빠르게 추출될 수 있습니다.

토론 질문: 데이터베이스 해싱 알고리즘을 업그레이드하기 위한 마이그레이션 전략을 설계하세요.

체크포인트 9: 암호 해독하기

사이버 보안 전문가는 온라인 위협 행위자로부터 네트워크 자산을 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 메시지를 해독하세요.

자모-숫자 암호화 키

ㄱ=1 ㄲ=2 ㄴ=3 ㄷ=4 ㄸ=5 ㄹ=6 ㅁ=7 ㅂ=8 ㅃ=9 ㅅ=10
ㅆ=11 ㅇ=12 ㅈ=13 ㅉ=14 ㅊ=15 ㅋ=16 ㅌ=17 ㅍ=18 ㅎ=19 ㅏ=20
ㅐ=21 ㅑ=22 ㅒ=23 ㅓ=24 ㅔ=25 ㅕ=26 ㅖ=27 ㅗ=28 ㅘ=29 ㅙ=30
ㅚ=31 ㅛ=32 ㅜ=33 ㅝ=34 ㅞ=35 ㅟ=36 ㅠ=37 ㅡ=38 ㅢ=39 ㅣ=40

4	20	4	20	3	1	27		12	40	3	13	38	12	12	38	6	28

6	28	1	38	12	40	3		8	28	19	28

해독된 메시지:

팁: 각 숫자는 아래 키의 한글 자모 하나를 나타냅니다. 자모를 차례로 모아 글자를 만드세요(예: ㅂ+ㅗ = 보).

체크포인트 10: 기초 사이버 보안 FAQ (파트 A)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q1: 비밀번호 유출이란 무엇인가요?

비밀번호 유출은 데이터 침해나 서버 구성 오류로 사용자 로그인 자격 증명이 노출될 때 발생합니다.

Q2: 해커는 유출된 비밀번호를 어떻게 찾나요?

해커는 유출 데이터가 게시되는 다크 웹 포럼, 공개 데이터베이스 덤프, 페이스트 사이트를 검색합니다 [8].

Q3: 비밀번호를 재사용하면 위험한가요?

예, 한 사이트가 침해되면 해커가 같은 자격 증명을 수천 개의 다른 플랫폼에서 시도해 볼 수 있기 때문입니다 [3].

Q4: 암호학적 솔트(salt)란 무엇인가요?

솔트는 해시하기 전에 비밀번호에 더하는 무작위 데이터로, 미리 계산한 조회 공격을 무력화합니다 [2].

Q5: MD5가 더 이상 쓰이지 않는 이유는 무엇인가요?

MD5는 빠르지만 이미 구식이 된 범용 해시이므로, 특히 해시에 솔트가 없으면 공격자가 비밀번호 추측을 매우 빠르게 시험해 볼 수 있습니다 [2].

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 비밀번호 관리자는 사용자를 어떻게 보호하나요?

사이트마다 복잡하고 고유한 인증 정보를 자동으로 생성하여 사람의 기억 오류와 재사용을 줄입니다.

Q7: 무차별 대입 공격이란 무엇인가요?

올바른 비밀번호를 찾을 때까지 가능한 모든 문자 조합을 체계적으로 시험하는 공격 [4].

Q8: 계정 잠금은 어떤 도움이 되나요?

잠금 또는 속도 제한은 반복적인 온라인 추측을 늦추며, 모니터링 및 MFA와 함께 사용하면 무차별 대입 공격의 위험을 줄입니다 [4].

Q9: 마스터 비밀번호는 안전한가요?

다른 웹 시스템에서 재사용하지 않는 엔트로피가 높은 암호문(패스프레이즈)이라면 안전합니다.

Q10: 비밀번호를 정기적으로 바꿔야 하나요?

NIST는 주기적인 변경을 강제하지 말고 유출 증거가 있을 때 변경하며 길이, 차단 목록, MFA를 우선하라고 말합니다 [1].

체크포인트 10: 심화 보안 FAQ (파트 C)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q1: Argon2는 bcrypt와 어떻게 비교되나요?

OWASP는 Argon2id를 첫 번째 선택지로 꼽습니다. 메모리 하드 설정 덕분에 bcrypt보다 GPU 및 ASIC 크래킹에 더 잘 견딥니다 [2].

Q2: 키 스트레칭이란 무엇인가요?

해시 알고리즘을 수천 번 반복해 비밀번호 검증 과정을 늦춤으로써 크래킹 비용을 높이는 기법 [2].

Q3: 레인보우 테이블은 어떻게 작동하나요?

평문 비밀번호와 그 해시를 연결한 미리 계산된 조회 표로, 솔트가 없는 해시를 빠르게 되돌리는 데 사용됩니다 [2].

Q4: 자격 증명 재활용이란 무엇인가요?

한 번의 정보 유출에서 도난당한 사용자 이름과 비밀번호 쌍을 다른 서비스에 대입해 접근을 시도하는 것으로, 특히 비밀번호를 재사용한 경우에 효과적입니다 [3].

Q5: 비밀번호 관리자도 해킹당할 수 있나요?

예. 많은 곳이 제로 지식 암호화를 사용하므로 서버가 침해돼도 암호화된 보관함만 노출되지만, 약한 마스터 비밀번호는 오프라인에서 여전히 뚫릴 수 있습니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q6: 사전 공격이란 무엇인가요?

무작위 글자가 아니라 흔한 단어, 문구, 과거에 유출된 비밀번호를 대입해 보는 무차별 대입 공격의 변형.

Q7: 패스프레이즈가 선호되는 이유는 무엇인가요?

패스프레이즈는 무작위 단어 여러 개를 사용해 엔트로피가 높으며, 사람이 기억하기 쉽지만 컴퓨터가 크래킹하는 데는 많은 연산이 필요합니다 [1].

Q8: 싱글 사인온(SSO)은 비밀번호 유출에 어떤 영향을 주나요?

SSO는 비밀번호가 난립하는 문제를 줄이지만, ID 제공자가 가치가 높은 공격 대상이 되므로 강력하고 가급적 피싱에 강한 MFA가 필요합니다 [6].

Q9: 세션 하이재킹이란 무엇인가요?

공격자가 유효한 세션 토큰을 얻거나 악용해 비밀번호 없이도 로그인한 사용자를 사칭합니다 [5].

Q10: 패스워드 스프레이 공격은 어떻게 탐지하나요?

여러 계정에 같은 몇 가지 비밀번호를 대입하는 패턴을 찾음으로써. 계정 잠금 임계값을 넘지 않으려고 대개 천천히 시도합니다 [7].

파트 11: 실제 사이버 보안 사실 10가지와 시사점

보안 침해, 방어 메커니즘, 규정 준수 표준에 관한 실제 사실을 살펴보세요.

1. 보안 인사이트

NIST SP 800-63B는 새 비밀번호를 흔하거나 유출된 비밀번호의 차단 목록과 대조해 확인하도록 요구합니다 [1].

2. 보안 인사이트

2019년 'Collection #1' 유출본은 이전의 여러 침해 사고에서 나온 데이터를 이메일과 비밀번호 쌍으로 이루어진 하나의 거대한 파일로 합친 것입니다 [8].

3. 보안 인사이트

NIST는 이제 유일한 인증 요소로 사용하는 비밀번호는 최소 15자 이상이어야 한다고 요구합니다 [1].

4. 보안 인사이트

ASIC 하드웨어는 초당 수십억 개의 SHA-256 해시를 계산할 수 있어, 원시 SHA 해싱은 사용자 비밀번호에 안전하지 않습니다 [2].

5. 보안 인사이트

솔트가 고유하면 비밀번호가 완전히 같은 두 사용자도 서로 다른 데이터베이스 해시를 갖게 됩니다 [2].

6. 보안 인사이트

많은 비밀번호 관리자는 사용자의 마스터 비밀번호에서 파생된 강력한 암호화로 보관함 데이터를 로컬에서 암호화합니다.

7. 보안 인사이트

많은 사람이 전자상거래, 은행, 이메일 계정에 같은 비밀번호를 재사용하기 때문에 자격 증명 스터핑이 통합니다 [3].

8. 보안 인사이트

NIST SP 800-63B는 검증자가 주기적인 비밀번호 변경을 요구해서는 안 되며, 유출 증거가 있을 때만 변경하게 해야 한다고 말합니다 [1].

9. 보안 인사이트

짧은 비밀번호에 대문자 하나와 기호 하나를 더해도 최신 자동화 GPU 사전 공격을 막지 못합니다 [1].

10. 보안 인사이트

MFA는 비밀번호가 유출된 뒤에도 많은 크리덴셜 스터핑 시도를 차단할 수 있으며, 피싱에 강한 MFA가 SMS 코드보다 더 강력합니다 [3].

기술 참고 자료 및 출처

이 학습 가이드와 인터랙티브 퍼즐은 전 세계 NIST, OWASP, 개인정보 보호 규정 준수 표준을 바탕으로 만들었습니다.

학술 및 업계 참고 자료

[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/

답안: 체크포인트 1 – 객관식

1 질문 1 정답: A

교사용 참고

크리덴셜 스터핑은 자동화를 사용하여 유출된 사용자 이름과 비밀번호 쌍을 다른 사이트에 시도하는 방식입니다 [3].

2 질문 2 정답: A

교사용 참고

OWASP는 Argon2id를 가장 먼저 권장하며, bcrypt는 주로 Argon2id나 scrypt를 사용할 수 없는 레거시 시스템을 위한 것입니다 [2].

3 질문 3 정답: A

교사용 참고

MFA는 추가 요소를 요구하므로, 도난당한 비밀번호만으로는 계정을 열 수 없습니다 [3].

4 질문 4 정답: A

교사용 참고

유출 데이터 모음은 2019년 Collection #1 모음처럼 유출된 자격 증명을 모아 놓은 것입니다 [8].

5 질문 5 정답: A

교사용 참고

비밀번호 관리자는 모든 계정에 고유하고 강력한 비밀번호를 생성하고 저장하여 재사용을 막아 줍니다 [3].

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 — 정답: 참

교사용 참고

참: 재사용한 비밀번호가 있으면 공격자가 한 사이트에서 유출된 자격 증명을 다른 사이트에 다시 시도할 수 있습니다 [3].

7 질문 7 — 정답: 거짓

교사용 참고

거짓: SHA-1은 빠른 해시이며, OWASP는 대신 Argon2id, scrypt, bcrypt, PBKDF2를 권장합니다 [2].

8 질문 8 — 정답: 거짓

교사용 참고

거짓: 복잡성 규칙만으로는 재사용된 유출 비밀번호를 이용한 스터핑을 막을 수 없으며, MFA가 필요합니다 [3].

9 질문 9 — 정답: 참

교사용 참고

참: 모니터링 서비스는 유출 데이터 모음과 다크 웹 출처에서 노출된 자격 증명을 검색합니다 [8].

10 질문 10 — 정답: 참

교사용 참고

참: 비밀번호마다 고유한 솔트를 사용하면 미리 계산된 레인보우 테이블이 소용없어집니다 [2].

어휘 정답 및 채점 기준표

교사용 채점 기준: 정확하게 연결한 항목마다 1점(총 8점), 문맥 용어마다 1점(총 6점)을 줍니다.

체크포인트 4: 답안 – 개념 연결

F 1. 스터핑	H 2. bcrypt	D 3. 침해	G 4. 솔팅
C 5. 관리자	B 6. MFA	A 7. 레인보우	E 8. 피싱

체크포인트 3: 답안 – 핵심 용어

1 스터핑	2 bcrypt	3 침해	4 솔팅
5 관리자	6 다단계 인증		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 H – 사전공격	2 C – 사기	3 B – 신용정보	4 G – 사회공학
5 A – 정보유출	6 D – 명의도용	7 E – 신고	8 F – 침해사고

교사를 위한 토론 참고

핵심 용어:
학생들이 스터핑, bcrypt, 침해를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

사례 연구:
학생들이 의견이 아니라 워크시트의 사실을 근거로 권고안을 제시하게 하세요.

출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

청	템	해	라	인	소	다	서	색	하	크	유	메	고	템
타	비	속	결	방	트	공	비	사	라	메	카	다	리	방
접	학	워	학	카	파	라	이	워	기	기	템	이	안	송
보	공	공	터	타	바	시	회	다	트	인	요	술	호	회
연	회	시	검	다	정	위	터	파	터	신	번	침	공	명
버	사	개	비	자	보	리	침	기	버	전	험	밀	신	고
개	신	격	연	아	유	소	스	해	도	하	벽	인	바	가
마	사	접	명	벽	출	터	의	화	사	신	주	방	타	위
격	번	터	카	기	이	데	방	격	속	고	트	데	데	격
공	관	스	주	메	네	사	스	공	연	호	리	바	검	카
전	신	용	정	보	템	해	청	아	회	검	서	방	크	학
사	카	데	타	명	위	출	속	사	요	마	가	학	송	카
화	나	타	연	의	타	안	워	기	차	관	격	번	하	기
리	회	템	안	도	위	답	보	나	다	험	접	이	개	주
명	격	터	리	용	주	시	자	이	침	마	버	리	신	유

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

2 가로: 사기 남을 속여 돈이나 이익을 가로채는 범죄 (2 글자)

3 가로: 사전공격 자주 쓰는 단어를 하나씩 넣어 비밀번호를 알아내려는 공격 (4 글자)

4 가로: 신고 범죄나 피해 사실을 관계 기관에 알리는 일 (2 글자)

5 가로: 명의도용 남의 이름이나 정보를 허락 없이 사용하는 범죄 (4 글자)

6 가로: 정보유출 개인 정보가 허가 없이 외부로 새어 나가는 일 (4 글자)

세로

1 세로: 침해사고 해킹 등으로 정보 시스템이 뚫려 정보가 노출된 사건 (4 글자)

2 세로: 사회공학 사람의 심리를 이용해 정보를 빼내는 수법 (4 글자)

4 세로: 신용정보 대출 이력 등 개인의 금융 거래 신뢰도를 보여 주는 정보 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 유정출보 — **정보유출**
2. 기사 — **사기**
3. 고신 — **신고**
4. 학공사회 — **사회공학**
5. 보신정용 — **신용정보**
6. 도용명의 — **명의도용**
7. 사침고해 — **침해사고**
8. 사격공전 — **사전공격**

비밀 암호 도전 정답

"다단계 인증으로 로그인 보호"

사례 연구 답안

A 사례 연구 1: 기업 자격 증명 유출 대응

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 다크 웹 모니터링 서비스가 한 조직에 회사 시스템 관리자 비밀번호가 담긴 데이터베이스 덤프가 온라인에 공개되었다고 알립니다.
- 권장 전략 및 해결책: 활성 상태인 모든 관리자 세션을 해지하고 고엔트로피 생성기로 자격 증명을 재설정하세요. 관리자 포털에 피싱에 강한 MFA를 적용하고 [6], 영향을 받은 API 키를 교체하며, 로그인 로그를 검토하고 최초 노출 지점을 찾아 다른 권한 계정도 확인합니다.

B 사례 연구 2: 비밀번호 해싱 표준 적용하기

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 기업의 데이터베이스가 암호학적 솔트 없이 오래된 MD5 해시로 사용자 비밀번호를 저장하고 있어, 빠르게 탈취당할 수 있습니다.
- 권장 전략 및 해결책: 사용자별 고유 솔트와 함께 Argon2id(구형 시스템에서는 bcrypt)를 도입합니다 [2]. 기존 MD5 해시를 지금 새 알고리즘으로 감싸고, 각 사용자의 다음 로그인 때 바로 다시 해시하며, 오랫동안 사용하지 않은 계정은 재설정을 강제합니다.