Nome: _____ Data: _____ Pontuação: _____

Fugas de palavras-passe e segurança das credenciais

Credential stuffing, violações de dados, algoritmos de hash, autenticação multifator e segurança das palavras-passe.

VISÃO GERAL DA APRENDIZAGEM SOBRE FUGAS DE PALAVRAS-PASSE

PROTEGIDO
ENCRIPTAÇÃO DE DADOS
Norma AES de 256 bits

CONFORME
NORMAS GLOBAIS
Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST
POLÍTICA DE ACESSO
Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te pelas fugas de palavras-passe e pela segurança de credenciais. Vais explorar o credential stuffing, violações de dados, algoritmos de hash, autenticação multifator e gestores de palavras-passe.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/cibersegurança/vazamento-senhas/

O teu roteiro de aprendizagem sobre segurança de palavras-passe

- Compreender os riscos de exposição de credenciais em fóruns da dark web.
- Implementa a autenticação multifator (MFA) e a monitorização de credenciais comprometidas.
- Concebe defesas de segurança empresariais contra burlas de engenharia social direcionadas.

INSTRUÇÕES DO GUIA SOBRE FUGAS DE PALAVRAS-PASSE

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à proteção de credenciais. Termina com a atividade bónus Pensa rápido.

FUGAS DE PALAVRAS-PASSE E SEGURANÇA DAS CREDENCIAIS (INTRODUÇÃO)

As fugas de palavras-passe expõem credenciais de utilizadores em sites públicos e da dark web. Palavras-passe únicas geradas por um gestor de palavras-passe, a verificação de palavras-passe comprometidas e a autenticação multifator (MFA) reduzem o risco de credential stuffing, enquanto o hashing lento e com salt das palavras-passe limita os danos se uma base de dados de palavras-passe for roubada.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1 **1. O que é o credential stuffing?**

- A. Usar automatização para testar combinações de nome de utilizador/palavra-passe divulgadas em vários sítios
- B. Encriptar os ficheiros de armazenamento de bases de dados locais
- C. Sobrecarregar servidores web com pedidos de tráfego de rede
- D. Monitorizar secretamente as introduções do teclado

2 **2. Que algoritmo indica a OWASP como primeira escolha para armazenar palavras-passe atualmente?**

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

3 **3. Como atenua a autenticação multifator (MFA) o risco de fugas de palavras-passe?**

- A. Exige um fator de verificação adicional, pelo que uma palavra-passe roubada, por si só, não é suficiente
- B. Altera automaticamente a palavra-passe a cada hora
- C. Encripta o nome de utilizador durante a transmissão
- D. Alerta a agência de crédito sobre pedidos fraudulentos

4 **4. O que é um despejo de dados de uma violação de dados?**

- A. Um conjunto de credenciais de utilizadores divulgadas, publicado online ou vendido em fóruns de hackers
- B. Uma cópia de segurança dos ficheiros da base de dados guardada fora do local
- C. Uma cache temporária de registos de servidores web
- D. Uma ferramenta administrativa usada para repor palavras-passe de utilizadores

5 **5. Qual é o papel de um gestor de palavras-passe?**

- A. Gerar e guardar palavras-passe únicas e fortes para cada conta
- B. Monitorizar o tráfego de rede para detetar fugas de palavras-passe
- C. Bloquear ataques automatizados de força bruta na gateway
- D. Analisar os blocos de armazenamento da base de dados à procura de palavras-passe não encriptadas

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Reutilizar palavras-passe em várias contas aumenta o risco de credential stuffing.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta 7

7. O SHA-1 é uma função de hash recomendada para o armazenamento moderno de palavras-passe.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta 8

8. Impor apenas a complexidade das palavras-passe (sem MFA) impede totalmente o credential stuffing.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta 9

9. As ferramentas de monitorização da dark web analisam a internet à procura de credenciais empresariais comprometidas.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta 10

10. Os hashes com salt acrescentam dados aleatórios únicos às palavras-passe antes do hashing para derrotar ataques com rainbow tables.

- ◯ Verdadeiro
- ◯ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Testar credenciais divulgadas em muitas aplicações web designa-se credential _____ .

2. Um algoritmo lento e adaptativo de hash de palavras-passe, ainda aceite pela OWASP, é o _____ .

3. A exposição de ficheiros confidenciais de bases de dados na internet é uma _____ de dados.

4. Acrescentar valores aleatórios às palavras-passe antes do hash chama-se _____ .

5. Uma base de dados local segura para as credenciais dos utilizadores é um _____ de palavras-passe.

6. Acrescentar um segundo passo de verificação no início de sessão recorre a _____ .

BANCO DE PALAVRAS DE VOCABULÁRIO

BCRYPT GESTOR MFA PHISHING SALTING STUFFING TABELA ARCO-ÍRIS VIOLAÇÃO

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos de segurança

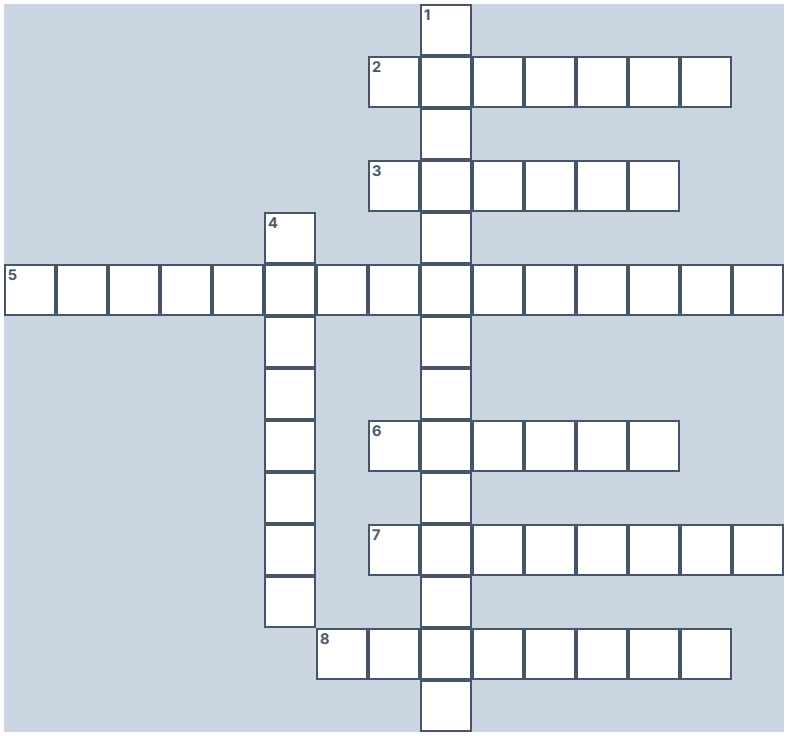
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. STUFFING	A	Tabela pré-calculada de hashes de palavras-passe.
☐	2. BCRYPT	B	Verificação de início de sessão multifator.
☐	3. VIOLAÇÃO	C	Ferramenta de armazenamento de credenciais.
☐	4. ADIÇÃO DE SALT	D	Exposição não autorizada de bases de dados.
☐	5. GESTOR	E	Engenharia social para roubar credenciais de início de sessão.
☐	6. MFA	F	Testar credenciais divulgadas.
☐	7. ARCO-ÍRIS	G	Adicionar um salt aleatório ao hash da palavra-passe.
☐	8. PHISHING	H	Algoritmo lento de hashing de palavras-passe.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

2. Acrescentar um sal aleatório ao hash da palavra-passe. (7)

3. Ferramenta de armazenamento de credenciais. (6)

5. Verificação de início de sessão com vários fatores. (15)

6. Algoritmo lento de hash de palavras-passe. (6)

7. Exposição não autorizada de uma base de dados. (8)

8. Engenharia social para roubar credenciais de acesso. (8)

VERTICAIS

1. Tabela pré-calculada de hashes de palavras-passe. (14)

4. Testar credenciais divulgadas. (8)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

2 horizontal: Acrescentar um sal aleatório ao hash da palavra-passe. (7 letras):

3 horizontal: Ferramenta de armazenamento de credenciais. (6 letras):

5 horizontal: Verificação de início de sessão com vários fatores. (15 letras):

6 horizontal: Algoritmo lento de hash de palavras-passe. (6 letras):

7 horizontal: Exposição não autorizada de uma base de dados. (8 letras):

8 horizontal: Engenharia social para roubar credenciais de acesso. (8 letras):

VERTICAIS

1 vertical: Tabela pré-calculada de hashes de palavras-passe. (14 letras):

4 vertical: Testar credenciais divulgadas. (8 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

B C R Y P T C A Z W F K H Z D
N G D Q X P C U U B T A Z N D
K N A D O D F T H I A D R Q M
E I I R Z S F E Q V B F A A Q
O H N P T X Q N K R E U S D N
G S Y B F S X T W J L A R Z Y
N I Y L G S I I M R A J M L T
I H O H Q A Q C H V A Z A O V
F P G U B L Y A R I R Y B H L
F Z G J O T P C N O C W R C M
U Z Y G Y I O A W L O U O K V
T P B N V N T O M A I G T V D
S Y U K R G B M X C R Z S Y M
R Q X I P D A F D A I J E Q V
W W L J H T H A G O S B G E I

LISTA DE PALAVRAS DE VOCABULÁRIO

STUFFING BCRYPT VIOLACAO SALTING GESTOR AUTENTICACAOMFA TABELAARCOIRIS PHISHING

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO	DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO
A. STUFFING	_____ 1. Engenharia social para roubar credenciais de acesso.
B. BCRYPT	_____ 2. Exposição não autorizada de uma base de dados.
C. VIOLACAO	_____ 3. Algoritmo lento de hash de palavras-passe.
D. SALTING	_____ 4. Tabela pré-calculada de hashes de palavras-passe.
E. GESTOR	_____ 5. Testar credenciais divulgadas.
F. AUTENTICACAOMFA	_____ 6. Acrescentar um sal aleatório ao hash da palavra-passe.
G. TABELAARCOIRIS	_____ 7. Ferramenta de armazenamento de credenciais.
H. PHISHING	_____ 8. Verificação de início de sessão com vários fatores.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. NFFSITGU
2. LVOIACAO
3. GSTROE
4. AAIOECASRRI TBL
5. YRTBPC
6. NLISTGA
7. CAIAAOUTAT MFECN
8. SHHGPNII

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Hábitos seguros que podes começar hoje			
2	Regras para uma palavra-passe forte			
3	Gestores de palavras-passe que conheces			
4	Ferramentas de segurança que conheces			
5	Sinais de alerta num email			
6	Palavras divertidas para uma frase-passe longa			
7	Formas de iniciar sessão sem palavra-passe			
8	Informações que nunca deves partilhar			
9	Razões para atualizar o software			
10	Coisas a fazer quando uma palavra-passe é divulgada			
11	Contas que precisam de MFA			
12	Locais onde as palavras-passe nunca devem ser guardadas			
13	Sinais de que um computador está infetado			
14	Palavras-passe fracas que as pessoas usam			
15	Coisas de que fazes cópia de segurança			

Ponto de controlo 8: Estudos de caso de cibersegurança

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

ESTUDO DE CASO 1: CORREÇÃO DE FUGA DE CREDENCIAIS EMPRESARIAIS

👷

Cenário: Um serviço de monitorização da dark web alerta uma organização de que foi publicada online uma fuga de base de dados com palavras-passe de administradores de sistemas da empresa.

Questão para debate: Analisa os riscos da fuga de credenciais e propõe uma estratégia administrativa de redefinição.

ESTUDO DE CASO 2: IMPLEMENTAR NORMAS DE HASH DE PALAVRAS-PASSE

👷

Cenário: Uma base de dados empresarial guarda atualmente as palavras-passe dos utilizadores com hashes MD5 desatualizados e sem salt criptográfico, o que as torna vulneráveis a extração rápida.

Questão para debate: Cria uma estratégia de migração para atualizar o algoritmo de hash da base de dados.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

16	1	12	1	22	18	1	19		16	1	19	19	5	
5	24	16	15	19	20	1	19		16	5	4	5	13	
1	21	20	5	14	20	9	3	1	3	1	15	13	6	1

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: O que é uma fuga de palavras-passe?

Uma fuga de palavras-passe ocorre quando as credenciais de início de sessão dos utilizadores são expostas por violações de dados ou configurações incorretas de servidores.

Q2: Como encontram os hackers as palavras-passe divulgadas?

Os hackers vasculham fóruns da dark web, despejos públicos de bases de dados e sites de paste onde os dados de violações são publicados [8].

Q3: Reutilizar palavras-passe é perigoso?

Sim, porque se um site for comprometido, os piratas informáticos podem testar as mesmas credenciais em milhares de outras plataformas [3].

Q4: O que é um sal criptográfico?

Um salt são dados aleatórios adicionados a uma palavra-passe antes do hashing, tornando ineficazes os ataques de consulta pré-calculados [2].

Q5: Porque está o MD5 obsoleto?

O MD5 é um hash genérico rápido e obsoleto, pelo que os atacantes podem testar tentativas de palavras-passe extremamente depressa, sobretudo quando os hashes não têm sal [2].

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte B)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: Como protege um gestor de palavras-passe os utilizadores?

Gera automaticamente credenciais complexas e únicas para cada site, reduzindo os erros de memória humana e a reutilização.

Q7: O que é um ataque de força bruta?

Um ataque que testa sistematicamente todas as combinações possíveis de caracteres até encontrar a palavra-passe correta [4].

Q8: Como ajuda o bloqueio de contas?

O bloqueio de conta ou a limitação de tentativas abranda as tentativas repetidas de adivinhação online e, em conjunto com a monitorização e a MFA, reduz o risco de ataques de força bruta [4].

Q9: As palavras-passe mestras são seguras?

São seguras se forem frases-passe de elevada entropia que nunca são reutilizadas noutros sistemas web.

Q10: As palavras-passe devem ser alteradas regularmente?

O NIST recomenda não forçar alterações periódicas; devem alterar-se perante provas de comprometimento e dar prioridade ao comprimento, às listas de bloqueio e à MFA [1].

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte C)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como se compara o Argon2 com o bcrypt?

A OWASP indica o Argon2id como primeira escolha; as suas definições resistentes por uso intensivo de memória resistem melhor ao cracking por GPU e ASIC do que o bcrypt [2].

Q2: O que é o key stretching?

Uma técnica que repete um algoritmo de hashing milhares de vezes para abrandar o processo de verificação de palavras-passe, tornando dispendioso o seu desbloqueio [2].

Q3: Como funcionam as rainbow tables?

São tabelas de consulta pré-calculadas que associam palavras-passe em texto simples aos seus hashes, usadas para reverter rapidamente hashes sem salt [2].

Q4: O que é a reciclagem de credenciais?

Reutilizar pares de nome de utilizador/palavra-passe roubados numa violação de dados para tentar aceder a outros serviços, sobretudo quando as pessoas reutilizaram palavras-passe [3].

Q5: Os gestores de palavras-passe podem ser pirateados?

Sim. Muitos usam encriptação de conhecimento zero, pelo que uma violação do servidor expõe apenas cofres cifrados, mas palavras-passe mestras fracas ainda podem ser descobertas offline.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte D)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: O que é um ataque de dicionário?

Uma variante de força bruta que testa palavras comuns, expressões e palavras-passe divulgadas anteriormente em fugas, em vez de letras aleatórias.

Q7: Porque são preferidas as frases-passe?

As frases-passe usam várias palavras aleatórias, criando uma entropia elevada que é fácil de memorizar para os humanos, mas computacionalmente dispendiosa de quebrar [1].

Q8: Como afeta o início de sessão único (SSO) as fugas de palavras-passe?

O SSO reduz a proliferação de palavras-passe, mas o fornecedor de identidade passa a ser um alvo de grande valor que precisa de MFA robusta, de preferência resistente a phishing [6].

Q9: O que é o sequestro de sessão?

Um atacante obtém ou abusa de um token de sessão válido para se fazer passar por um utilizador com sessão iniciada sem precisar novamente da palavra-passe [5].

Q10: Como detetar password spraying?

Procurando as mesmas poucas palavras-passe experimentadas em muitas contas, muitas vezes devagar para ficar abaixo dos limiares de bloqueio [7].

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

A NIST SP 800-63B exige que as palavras-passe novas sejam verificadas em listas de bloqueio de palavras-passe comuns e comprometidas [1].

2. PERSPETIVA SOBRE SEGURANÇA

A fuga «Collection #1» de 2019 fundiu dados de muitas violações anteriores num único ficheiro enorme de pares de email e palavra-passe [8].

3. PERSPETIVA SOBRE SEGURANÇA

O NIST exige agora que as palavras-passe usadas como único fator de autenticação tenham pelo menos 15 caracteres [1].

4. PERSPETIVA SOBRE SEGURANÇA

O hardware ASIC consegue calcular milhares de milhões de hashes SHA-256 por segundo, tornando o hashing SHA em bruto inseguro para palavras-passe de utilizadores [2].

5. PERSPETIVA SOBRE SEGURANÇA

Salts únicos significam que dois utilizadores com exatamente a mesma palavra-passe obtêm hashes diferentes na base de dados [2].

6. PERSPETIVA SOBRE SEGURANÇA

Muitos gestores de palavras-passe encriptam localmente os dados do cofre com criptografia robusta derivada da palavra-passe mestra do utilizador.

7. PERSPETIVA SOBRE SEGURANÇA

O credential stuffing funciona porque muitas pessoas reutilizam a mesma palavra-passe em contas de comércio eletrónico, bancárias e de e-mail [3].

8. PERSPETIVA SOBRE SEGURANÇA

A NIST SP 800-63B afirma que os verificadores não devem exigir alterações periódicas de palavra-passe, apenas alterações após provas de comprometimento [1].

9. PERSPETIVA SOBRE SEGURANÇA

Acrescentar uma única letra maiúscula e um símbolo a uma palavra-passe curta não impede os ataques modernos de dicionário automatizados com GPU [1].

10. PERSPETIVA SOBRE SEGURANÇA

A MFA pode bloquear muitas tentativas de credential stuffing mesmo depois de uma palavra-passe ser divulgada; a MFA resistente a phishing é mais forte do que os códigos por SMS [3].

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[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/

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

Resposta correta: A

NOTA PARA O PROFESSOR

O credential stuffing usa automatização para experimentar pares de nome de utilizador e palavra-passe divulgados noutros sites [3].

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

A OWASP recomenda primeiro o Argon2id; o bcrypt serve sobretudo para sistemas legados em que o Argon2id ou o scrypt não estão disponíveis [2].

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

A MFA exige um fator adicional, pelo que uma palavra-passe roubada, por si só, não consegue desbloquear a conta [3].

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

As fugas de dados (breach dumps) são coleções de credenciais divulgadas, como a compilação Collection #1 de 2019 [8].

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

Um gestor de palavras-passe gera e guarda uma palavra-passe única e forte para cada conta, evitando a reutilização [3].

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 Pergunta 6

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Verdadeiro: as palavras-passe reutilizadas permitem aos atacantes reutilizar credenciais divulgadas num site noutros sites [3].

7 Pergunta 7

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: o SHA-1 é um hash rápido; a OWASP recomenda antes Argon2id, scrypt, bcrypt ou PBKDF2 [2].

8 Pergunta 8

Resposta correta: Falso

NOTA PARA O PROFESSOR

Falso: as regras de complexidade, por si só, não conseguem impedir o stuffing com palavras-passe divulgadas e reutilizadas; é preciso MFA [3].

9 Pergunta 9

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Verdadeiro: os serviços de monitorização pesquisam fugas de dados e fontes da dark web à procura de credenciais expostas [8].

10 Pergunta 10

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Verdadeiro: um salt único por palavra-passe torna ineficazes as rainbow tables pré-calculadas [2].

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

F 1. STUFFING	H 2. BCRYPT	D 3. VIOLAÇÃO	G 4. ADIÇÃO DE SALT
C 5. GESTOR	B 6. MFA	A 7. ARCO-ÍRIS	E 8. PHISHING

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 STUFFING	2 BCRYPT	3 VIOLAÇÃO	4 SALTING
5 GESTOR	6 MFA		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 H – PHISHING	2 C – VIOLACAO	3 B – BCRYPT	4 G – TABELAARCOIRIS
5 A – STUFFING	6 D – SALTING	7 E – GESTOR	8 F – AUTENTICACAOMFA

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar STUFFING, BCRYPT e VIOLAÇÃO por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

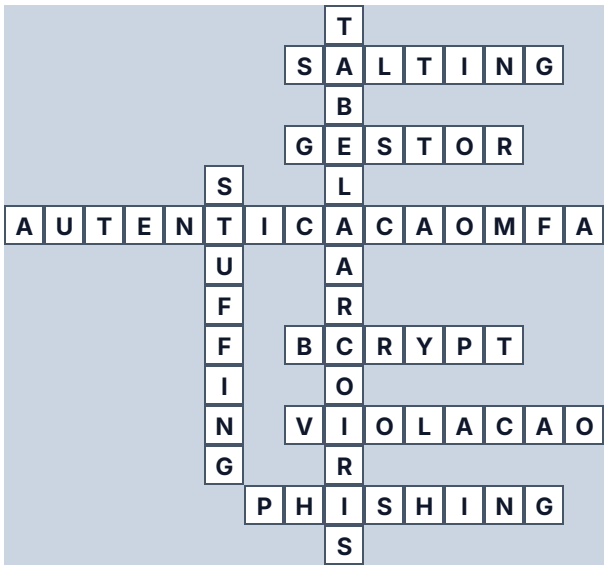
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

B	C	R	Y	P	T	C	A	Z	W	F	K	H	Z	D
N	G	D	Q	X	P	C	U	U	B	T	A	Z	N	D
K	N	A	D	O	D	F	T	H	I	A	D	R	Q	M
E	I	I	R	Z	S	F	E	Q	V	B	F	A	A	Q
O	H	N	P	T	X	Q	N	K	R	E	U	S	D	N
G	S	Y	B	F	S	X	T	W	J	L	A	R	Z	Y
N	I	Y	L	G	S	I	I	M	R	A	J	M	L	T
I	H	O	H	Q	A	Q	C	H	V	A	Z	A	O	V
F	P	G	U	B	L	Y	A	R	I	R	Y	B	H	L
F	Z	G	J	O	T	P	C	N	O	C	W	R	C	M
U	Z	Y	G	Y	I	O	A	W	L	O	U	O	K	V
T	P	B	N	V	N	T	O	M	A	I	G	T	V	D
S	Y	U	K	R	G	B	M	X	C	R	Z	S	Y	M
R	Q	X	I	P	D	A	F	D	A	I	J	E	Q	V
W	W	L	J	H	T	H	A	G	O	S	B	G	E	I

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: SALTING Acrescentar um sal aleatório ao hash da palavra-passe. (7 letras)

3 horizontal: GESTOR Ferramenta de armazenamento de credenciais. (6 letras)

5 horizontal: AUTENTICACAOMFA Verificação de início de sessão com vários fatores. (15 letras)

6 horizontal: BCRYPT Algoritmo lento de hash de palavras-passe. (6 letras)

7 horizontal: VIOLACAO Exposição não autorizada de uma base de dados. (8 letras)

8 horizontal: PHISHING Engenharia social para roubar credenciais de acesso. (8 letras)

VERTICAIS

1 vertical: TABELAARCOIRIS Tabela pré-calculada de hashes de palavras-passe. (14 letras)

4 vertical: STUFFING Testar credenciais divulgadas. (8 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. NFFSITGU — **STUFFING**
2. LVOIACAO — **VIOLACAO**
3. GSTROE — **GESTOR**
4. AAIOECASRRITBL — **TABELAARCOIRIS**
5. YRTBPC — **BCRYPT**
6. NLISTGA — **SALTING**
7. CAIAAOUTATMFECN — **AUTENTICACAOMFA**
8. SHHGPNII — **PHISHING**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"PALAVRAS PASSE EXPOSTAS PEDEM AUTENTICACAO MFA"

Soluções dos estudos de caso

A Estudo de caso 1: Correção de fuga de credenciais empresariais

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um serviço de monitorização da dark web alerta uma organização de que uma fuga de base de dados com palavras-passe de administradores de sistemas da empresa foi publicada online.
- Estratégia e solução recomendadas: Revogar todas as sessões de administrador ativas e repor as credenciais com um gerador de elevada entropia. Aplicar MFA resistente a phishing nos portais de administração [6], rodar as chaves de API afetadas, rever os registos de início de sessão, encontrar a exposição inicial e verificar as outras contas privilegiadas.

B Estudo de caso 2: Implementar normas de hash de palavras-passe

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise de cenário: Uma base de dados empresarial guarda atualmente as palavras-passe dos utilizadores com hashes MD5 desatualizados e sem salt criptográfico, o que as torna vulneráveis a uma extração rápida.
- Estratégia e solução recomendadas: Adotar o Argon2id (ou o bcrypt em sistemas antigos) com um sal único por utilizador [2]. Envolver já os hashes MD5 existentes no novo algoritmo, voltar a gerar o hash diretamente no próximo início de sessão de cada utilizador e forçar a reposição nas contas inativas há muito tempo.