姓名: _____ 日期: _____ 得分: _____

密码泄露与凭据安全

凭据填充、数据泄露、哈希算法、多因素认证和密码安全。

密码泄露学习概览

受保护
数据加密
256 位 AES 标准

合规的
全球标准
GDPR 与 CCPA 框架

零信任
访问策略
多重身份验证

欢迎！ 本活动手册将带你了解密码泄露和凭据安全。你将探索撞库攻击、数据泄露、哈希算法、多因素身份验证和密码管理器。

练习单检查点

- [ ] **第 1-4 部分: 掌握网络安全和威胁防范。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com 网络安全指南

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

你的密码安全学习路线图

- 了解暗网论坛上的凭据暴露风险。
- 实施多因素身份验证（MFA）和泄露凭据监控。
- 设计企业安全防御措施，抵御有针对性的社会工程诈骗。

密码泄露指南说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于凭据保护。 最后完成附加活动: 快速思考。

密码泄露与凭据安全（简介）

密码泄露会在公共网站和暗网网站上暴露用户凭据。使用密码管理器生成的唯一密码、泄露密码筛查和多因素身份验证（MFA）可降低撞库攻击的风险，而加盐的慢速密码哈希则可在密码数据库被盗时限制损失。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 1. 什么是撞库攻击?
   - A. 使用自动化手段在多个网站上测试泄露的用户名/密码组合
   - B. 加密本地数据库存储文件
   - C. 用大量网络流量请求压垮网络服务器
   - D. 秘密监控键盘输入

2. 2. OWASP 目前把哪种算法列为存储密码的首选?
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. 3. 多因素认证（MFA）如何降低密码泄露的风险?
   - A. 它需要额外的验证因素，因此仅凭被盗的密码是不够的
   - B. 它每小时自动更改密码
   - C. 它在传输过程中加密用户名
   - D. 它向征信机构通报欺诈请求

4. 4. 什么是数据泄露转储?
   - A. 在网上公布或在黑客论坛出售的泄露用户凭据集合
   - B. 存放在异地的数据库文件备份副本
   - C. Web 服务器日志的临时缓存
   - D. 用于重置用户密码的管理工具

5. 5. 密码管理器的作用是什么?
   - A. 为每个账户生成并存储唯一的强密码
   - B. 监控网络流量以发现密码泄露
   - C. 在网关处阻止自动化暴力破解攻击
   - D. 扫描数据库存储块中的未加密密码

检查点 2: 判断正误挑战

6 问题 6

6. 在多个账户中重复使用密码会增加撞库攻击的风险。

○ 正确 ○ 错误

7 问题 7

7. SHA-1 是现代密码存储的推荐哈希函数。

○ 正确 ○ 错误

8 问题 8

8. 仅强制执行密码复杂度（不使用 MFA）就能完全阻止撞库攻击。

○ 正确 ○ 错误

9 问题 9

9. 暗网监控工具会扫描互联网，查找被泄露的企业凭据。

○ 正确 ○ 错误

10 问题 10

10. 加盐哈希会在哈希之前向密码添加唯一的随机数据，以击败彩虹表攻击。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 在多个网络应用中测试泄漏的凭证称为凭证 _____ 。
2. OWASP 仍然认可的一种缓慢、自适应的密码哈希算法是 _____ 。
3. 机密数据库文件在互联网上暴露属于数据 _____ 。
4. 在哈希之前向密码添加随机值称为 _____ 。
5. 用于用户凭证的安全本地数据库是密码 _____ 。
6. 增加第二道登录验证步骤使用的是 _____ 。

词汇词库

彩虹表　多因素验证　管理器　哈希表　加盐　泄漏　撞库攻击　bcrypt

在此写下你的答案:

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

检查点 4: 安全概念配对

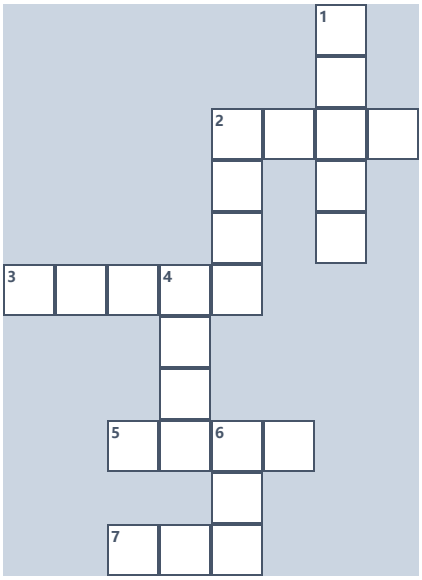
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

	1. 撞库	A	预先计算的密码哈希表。
	2. bcrypt	B	多重登录验证检查。（F）
	3. 数据泄露	C	凭据存储工具。
	4. 加盐	D	未经授权的数据库暴露。
	5. 管理器	E	通过社会工程学窃取登录信息。
	6. MFA	F	测试泄露的凭据。
	7. 彩虹	G	为密码哈希添加随机盐值。
	8. 网络钓鱼	H	慢速密码哈希算法。

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

2. 管理用户身份信息及其访问权限 (4)

3. 多重因素的登录检查 (5)

5. 把密码经单向算法转换后再保存的做法 (4)

7. 预先计算好的密码哈希对照表 (3)

纵向

1. 凭证存储工具 (5)

2. 确认用户确实是其所声称的那个人 (4)

4. 核对用户输入的密码是否正确 (4)

6. 把键通过哈希函数映射到存储位置的数据结构 (3)

检查点 5 替代活动: 无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

2 横向: 管理用户身份信息及其访问权限 (4 字):

3 横向: 多重因素的登录检查 (5 字):

5 横向: 把密码经单向算法转换后再保存的做法 (4 字):

7 横向: 预先计算好的密码哈希对照表 (3 字):

纵向

1 纵向: 凭证存储工具 (5 字):

2 纵向: 确认用户确实是其所声称的那个人 (4 字):

4 纵向: 核对用户输入的密码是否正确 (4 字):

6 纵向: 把键通过哈希函数映射到存储位置的数据结构 (3 字):

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

全 地 哈 道 输 多 全 址 人 安 信 录 用 私 彩
公 希 输 务 火 击 攻 协 哈 护 统 火 全 共 服
安 码 管 名 击 私 素 证 服 希 器 安 身 私 访
输 密 身 户 风 户 统 验 域 务 表 数 理 因 络
护 证 址 隧 问 密 访 份 因 险 理 记 安 件 域
器 验 域 虹 认 码 多 身 统 表 息 系 火 密 管
访 保 份 设 认 管 统 表 份 软 险 加 人 传 输
用 议 地 数 网 理 数 加 击 管 哈 议 域 哈 协
表 共 名 务 件 器 认 址 服 访 理 身 证 协 软
表 系 隐 证 证 件 备 理 共 公 护 据 传 软 险
虹 多 因 素 验 证 接 管 据 记 服 输 多 道 加
彩 因 记 息 密 名 私 素 服 证 务 设 虹 系 据
隧 全 网 素 码 份 服 协 络 务 险 务 信 隐 访
服 备 件 认 哈 用 访 管 因 传 信 设 览 户 络
络 设 攻 身 希 系 共 表 软 域 管 人 理 码 身

词汇列表

彩虹表 **哈希表** **密码哈希** **密码管理器** **身份管理** **身份验证** **多因素验证** **验证密码**

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 彩虹表
B. 哈希表
C. 密码哈希
D. 密码管理器
E. 身份管理
F. 身份验证
G. 多因素验证
H. 验证密码

定义与配对字段
1. 核对用户输入的密码是否正确。
2. 把密码经单向算法转换后再保存的做法。
3. 把键通过哈希函数映射到存储位置的数据结构。
4. 多重因素的登录检查。
5. 预先计算好的密码哈希对照表。
6. 凭证存储工具。
7. 管理用户身份信息及其访问权限。
8. 确认用户确实是其所声称的那个人。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的网络安全概念和术语。把答案写在提供的输入框中。

1. 虹 表 彩 _____

2. 密 哈 希 码 _____

3. 理 身 管 份 _____

4. 素 证 验 多 因 _____

5. 表 希 哈 _____

6. 理 密 管 器 码 _____

7. 验 身 证 份 _____

8. 验 码 密 证 _____

附加活动: 快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	你今天就可以开始的安全习惯			
2	强密码的规则			
3	你知道的密码管理器			
4	你知道的安全工具			
5	电子邮件中的警示信号			
6	适合做长密码短语的有趣词语			
7	无需密码登录的方法			
8	你绝不应分享的信息			
9	更新软件的原因			
10	密码泄露后要做的事			
11	需要多因素认证（MFA）的账户			
12	绝不应存放密码的地方			
13	电脑被感染的迹象			
14	人们使用的弱密码			
15	你要备份的内容			

检查点 8: 网络安全案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 企业凭据泄露的补救



情景: 一项暗网监控服务向某组织发出警报，称包含企业系统管理员密码的数据库转储文件已在网上公开。

讨论问题: 分析凭据泄露风险，并提出管理员重置策略。

案例研究 2: 落实密码哈希标准



情景: 一个企业数据库目前使用过时的 MD5 哈希值存储用户密码，且没有加密盐值，容易被快速提取。

讨论问题: 设计一个迁移策略来升级数据库的哈希算法。

检查点 9: 破解密码

网络安全专业人员保护网络资产免受网络威胁行为者的攻击。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

理=1 素=2 漏=3 护=4 多=5 登=6 络=7 证=8 身=9 因=10

虹=11 全=12 哈=13 管=14 码=15 器=16 份=17 密=18 安=19 验=20

录=21 彩=22 数=23 据=24 泄=25 保=26 表=27 网=28 用=29 希=30

29	5	10	2	6	21		26	4		25	3	18	15

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

检查点 10: 基础网络安全常见问题 (A 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q1: 什么是密码泄露?

当用户登录凭据因数据泄露或服务器配置错误而暴露时，就会发生密码泄露。

Q2: 黑客如何找到泄露的密码?

黑客会扫描暗网论坛、公开的数据库转储文件以及发布泄露数据的粘贴网站 [8]。

Q3: 重复使用密码危险吗?

是的，因为如果一个网站被攻破，黑客可以在数千个其他平台上测试相同的凭据 [3]。

Q4: 什么是加密盐值?

盐值是在哈希之前添加到密码中的随机数据，使预先计算的查表攻击失效 [2]。

Q5: MD5 为什么已经过时?

MD5 是一种快速且已过时的通用哈希算法，因此攻击者可以极快地测试密码猜测，尤其是在哈希值未加盐时 [2]。

检查点 10: 基础网络安全常见问题 (B 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q6: 密码管理器如何保护用户?

它会为每个网站自动生成复杂且唯一的凭据，减少人为记忆错误和重复使用。

Q7: 什么是暴力破解攻击?

一种系统地测试每种可能的字符组合直到找到正确密码的攻击 [4]。

Q8: 账户锁定有什么帮助?

锁定或速率限制可减缓反复的在线猜测，与监控和 MFA 结合使用时可降低暴力破解风险 [4]。

Q9: 主密码安全吗?

如果是高熵口令短语，并且从不在其他网络系统中重复使用，它们就是安全的。

Q10: 密码应该定期更换吗?

NIST 指出不要强制定期更改；应在有证据表明密码已泄露时才更改，并优先考虑长度、黑名单和 MFA [1]。

检查点 10: 高级安全常见问题 (C 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q1: Argon2 与 bcrypt 相比如何?

OWASP 将 Argon2id 列为首选；其内存困难型设置比 bcrypt 更能抵御 GPU 和 ASIC 破解 [2]。

Q2: 什么是密钥拉伸?

一种将哈希算法循环数千次以减慢密码验证过程的技术，使破解成本高昂 [2]。

Q3: 彩虹表是如何工作的?

它们是预先计算好的查找表，将明文密码与其哈希值对应起来，用于快速还原未加盐的哈希 [2]。

Q4: 什么是凭据回收利用?

重复使用从一次数据泄露中窃取的用户名/密码组合去尝试访问其他服务，尤其是在人们重复使用密码的情况下 [3]。

Q5: 密码管理器会被黑客攻破吗?

是的。许多采用零知识加密，因此服务器遭入侵时只会泄露加密的保险库，但薄弱的主密码仍可能被离线破解。

检查点 10: 高级安全常见问题 (D 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q6: 什么是字典攻击?

一种暴力破解变体，测试常用单词、短语和历史泄露的密码，而不是随机字母。

Q7: 为什么更推荐使用口令短语?

密码短语使用多个随机单词，形成易于人记忆、但破解计算成本很高的高熵值 [1]。

Q8: 单点登录 (SSO) 如何影响密码泄露?

SSO 减少了密码泛滥，但身份提供商会成为高价值目标，需要强大的、最好是抗网络钓鱼的 MFA [6]。

Q9: 什么是会话劫持?

攻击者获取或滥用有效的会话令牌来冒充已登录的用户，而无需再次输入密码 [5]。

Q10: 你如何检测密码喷洒攻击?

通过寻找在许多账户上尝试的少数相同密码，这类尝试通常进行得很慢，以保持在锁定阈值之下 [7]。

第 11 部分: 10 个现实中的网络安全事实与洞察

回顾有关安全漏洞、防御机制和合规标准的真实事实。

1. 安全洞察

NIST SP 800-63B 要求将新密码与常见密码和已泄露密码的黑名单进行比对检查 [1]。

2. 安全洞察

2019 年的“Collection #1”泄露文件将许多早期数据泄露事件的数据合并成一个包含电子邮箱和密码组合的巨大文件 [8]。

3. 安全洞察

NIST 现在要求，用作唯一身份验证因素的密码长度至少为 15 个字符 [1]。

4. 安全洞察

ASIC 硬件每秒可计算数十亿个 SHA-256 哈希，使原始 SHA 哈希对用户密码来说并不安全 [2]。

5. 安全洞察

唯一的盐值意味着两个使用完全相同密码的用户在数据库中会得到不同的哈希值 [2]。

6. 安全洞察

许多密码管理器使用由用户主密码派生的强加密算法，在本地加密保险库数据。

7. 安全洞察

凭据填充之所以有效，是因为许多人在电商、银行和电子邮件账户中重复使用同一个密码 [3]。

8. 安全洞察

NIST SP 800-63B 指出，验证方不应要求定期更改密码，仅应在有证据表明密码已泄露后才更改 [1]。

9. 安全洞察

在短密码中添加一个大写字母和符号，并不能阻止现代自动化 GPU 字典攻击 [1]。

10. 安全洞察

即使密码已泄露，MFA 也能阻止许多撞库尝试；抗网络钓鱼的 MFA 比短信验证码更强 [3]。

技术参考资料与来源

本学习指南和互动谜题根据全球 NIST、OWASP 以及数据隐私合规标准编写。

学术与行业参考资料

[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/

答案: 检查点 1 – 单项选择

1 问题 1

正确答案: A

教学提示

撞库使用自动化手段，在其他网站上尝试已泄露的用户名/密码组合 [3]。

2 问题 2

正确答案: A

教学提示

OWASP 首先推荐 Argon2id；bcrypt 主要用于无法使用 Argon2id 或 scrypt 的旧系统 [2]。

3 问题 3

正确答案: A

教学提示

MFA 需要额外的验证因素，因此仅凭被盗的密码无法解锁账户 [3]。

4 问题 4

正确答案: A

教学提示

泄露数据转储是已泄露的凭据集合，例如 2019 年的 Collection #1 合集 [8]。

5 问题 5

正确答案: A

教学提示

密码管理器会为每个账户生成并存储唯一的强密码，防止重复使用 [3]。

答案: 检查点 2 – 判断题（正确或错误）

6 问题 6

正确答案: 正确

教学提示

正确: 重复使用的密码让攻击者可以把从一个网站泄露的凭据在其他网站上重放 [3]。

7 问题 7

正确答案: 错误

教学提示

错误: SHA-1 是一种快速哈希；OWASP 推荐改用 Argon2id、scrypt、bcrypt 或 PBKDF2 [2]。

8 问题 8

正确答案: 错误

教学提示

错误: 仅靠复杂性规则无法阻止使用重复的已泄露密码的撞库；需要 MFA [3]。

9 问题 9

正确答案: 正确

教学提示

正确: 监控服务会在泄露数据转储和暗网来源中搜索暴露的凭据 [8]。

10 问题 10

正确答案: 正确

教学提示

正确: 每个密码使用唯一的盐值，会使预先计算的彩虹表失效 [2]。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

F 1. 撞库	H 2. bcrypt	D 3. 数据泄露	G 4. 加盐
C 5. 管理器	B 6. MFA	A 7. 彩虹	E 8. 网络钓鱼

检查点 3: 答案 – 关键术语

1 撞库攻击	2 bcrypt	3 泄漏	4 加盐
5 管理器	6 多因素验证		

检查点 6 替代活动: 答案 – 词语配对

1 H – 验证密码	2 C – 密码哈希	3 B – 哈希表	4 G – 多因素验证
5 A – 彩虹表	6 D – 密码管理器	7 E – 身份管理	8 F – 身份验证

教师讨论提示

关键术语:
检查学生能否用自己的话解释撞库、bcrypt和数据泄露，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

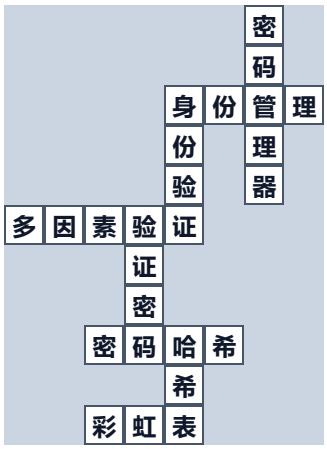
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	地	哈	道	输	多	全	址	人	安	信	录	用	私	彩
公	希	输	务	火	击	攻	协	哈	护	统	火	全	共	服
安	码	管	名	击	私	素	证	服	希	器	安	身	私	访
输	密	身	户	风	户	统	验	域	务	表	数	理	因	络
护	证	址	隧	问	密	访	份	因	险	理	记	安	件	域
器	验	域	虹	认	码	多	身	统	表	息	系	火	密	管
访	保	份	设	认	管	统	表	份	软	险	加	人	传	输
用	议	地	数	网	理	数	加	击	管	哈	议	域	哈	协
表	共	名	务	件	器	认	址	服	访	理	身	证	协	软
表	系	隐	证	证	件	备	理	共	公	护	据	传	软	险
虹	多	因	素	验	证	接	管	据	记	服	输	多	道	加
彩	因	记	息	密	名	私	素	服	证	务	设	虹	系	据
隧	全	网	素	码	份	服	协	络	务	险	务	信	隐	访
服	备	件	认	哈	用	访	管	因	传	信	设	览	户	络
络	设	攻	身	希	系	共	表	软	域	管	人	理	码	身

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 身份管理 管理用户身份信息及其访问权限 (4 字)

3 横向: 多因素验证 多重因素的登录检查 (5 字)

5 横向: 密码哈希 把密码经单向算法转换后再保存的做法 (4 字)

7 横向: 彩虹表 预先计算好的密码哈希对照表 (3 字)

纵向

1 纵向: 密码管理器 凭证存储工具 (5 字)

2 纵向: 身份验证 确认用户确实是其所声称的那个人 (4 字)

4 纵向: 验证密码 核对用户输入的密码是否正确 (4 字)

6 纵向: 哈希表 把键通过哈希函数映射到存储位置的数据结构 (3 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 虹表彩 — **彩虹表**
2. 密哈希码 — **密码哈希**
3. 理身管份 — **身份管理**
4. 素证验多因 — **多因素验证**
5. 表希哈 — **哈希表**
6. 理密管器码 — **密码管理器**
7. 验身证份 — **身份验证**
8. 验码密证 — **验证密码**

秘密密码挑战答案

“用多因素登录保护泄漏密码”

案例研究答案

A 案例研究 1: 企业凭据泄露的补救

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一项暗网监控服务向某组织发出警报，称包含企业系统管理员密码的数据库转储已在网上发布。
- 推荐策略与解决方案: 撤销所有活动的管理员会话，并使用高熵生成器重置凭据。在管理员门户上实施抗网络钓鱼的 MFA [6]，轮换受影响的 API 密钥，检查登录日志，找出最初的暴露点，并检查其他特权账户。

B 案例研究 2: 落实密码哈希标准

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一个企业数据库目前使用过时的 MD5 哈希且没有加密盐值来存储用户密码，因此很容易被快速提取。
- 建议策略与方案: 采用 Argon2id（旧系统上用 bcrypt），并为每个用户使用唯一的盐值 [2]。现在就用新算法包装现有的 MD5 哈希，在每个用户下次登录时直接重新哈希，并强制长期不活跃的账户重置密码。