ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

การรั่วไหลของรหัสผ่านและความปลอดภัยของข้อมูลประจำตัว

Credential Stuffing การละเมิดข้อมูล อัลกอริทึมแฮช การยืนยันตัวตนหลายปัจจัย และความปลอดภัยของรหัสผ่าน

ภาพรวมการเรียนรู้เรื่องการรั่วไหลของรหัสผ่าน

ได้รับการรักษาความปลอดภัย
การเข้ารหัสข้อมูล
มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด
มาตรฐานสากล
กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์
นโยบายการเข้าถึง
การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการรั่วไหลของรหัสผ่านและความปลอดภัยของข้อมูลรับรอง คุณจะได้สำรวจ credential stuffing การละเมิดข้อมูล อัลกอริทึมแฮช การพิสูจน์ตัวตนหลายปัจจัย และตัวจัดการรหัสผ่าน

จุดตรวจสอบของใบงาน

- [ ] **ส่วนที่ 1-4: เรียนรู้ความปลอดภัยไซเบอร์และการป้องกันภัยคุกคามให้เชี่ยวชาญ**
- [ ] **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- [ ] **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- [ ] **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- [ ] **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- [ ] **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือความปลอดภัยไซเบอร์ของ VPN.com

URL: https://www.vpn.com/th/cybersecurity/rathat-phan-rua/

เส้นทางการเรียนรู้ความปลอดภัยของรหัสผ่านของคุณ

- ทำความเข้าใจความเสี่ยงของการเปิดเผยข้อมูลรับรองบนฟอรัมดาร์กเว็บ
- ใช้การยืนยันตัวตนหลายปัจจัย (MFA) และการเฝ้าติดตามข้อมูลเข้าสู่ระบบที่ถูกบุกรุก
- ออกแบบการป้องกันความปลอดภัยขององค์กรจากการหลอกลวงด้วยวิศวกรรมสังคมแบบเจาะจงเป้าหมาย

คำแนะนำคู่มือการรั่วไหลของรหัสผ่าน

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การปกป้องข้อมูลรับรองตัวตน ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การรั่วไหลของรหัสผ่านและความปลอดภัยของข้อมูลประจำตัว (บทนำ)

การรั่วไหลของรหัสผ่านเปิดเผยข้อมูลประจำตัวของผู้ใช้บนเว็บสาธารณะและดาร์กเว็บ การใช้รหัสผ่านที่ไม่ซ้ำกันจากตัวจัดการรหัสผ่าน การตรวจสอบรหัสผ่านที่รั่วไหล และการยืนยันตัวตนหลายปัจจัย (MFA) ช่วยลดความเสี่ยงของ credential stuffing ส่วนการแฮชรหัสผ่านแบบเติมค่าสุ่มและช้าช่วยจำกัดความเสียหายหากฐานข้อมูลรหัสผ่านถูกขโมย

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. 1. การโจมตีแบบ **credential stuffing** คืออะไร?
   - A. การใช้ระบบอัตโนมัติทดสอบชุดชื่อผู้ใช้/รหัสผ่านที่รั่วไหลข้ามหลายเว็บไซต์
   - B. การเข้ารหัสไฟล์จัดเก็บฐานข้อมูลในเครื่อง
   - C. ท่วมเว็บเซิร์ฟเวอร์ด้วยคำขอทราฟฟิกเครือข่ายจำนวนมาก
   - D. การแอบเฝ้าดูการป้อนข้อมูลจากแป้นพิมพ์

2. 2. **OWASP** ระบุอัลกอริทึมใดเป็นตัวเลือกแรกสำหรับการจัดเก็บรหัสผ่านในปัจจุบัน?
   - A. Argon2id
   - B. MD5
   - C. SHA-1
   - D. ROT13

3. 3. การยืนยันตัวตนหลายปัจจัย (MFA) ลดความเสี่ยงจากรหัสผ่านรั่วไหลได้อย่างไร?
   - A. ต้องใช้ปัจจัยยืนยันเพิ่มเติม ดังนั้นรหัสผ่านที่ถูกขโมยเพียงอย่างเดียวจึงไม่เพียงพอ
   - B. เปลี่ยนรหัสผ่านโดยอัตโนมัติทุกชั่วโมง
   - C. เข้ารหัสชื่อผู้ใช้ระหว่างการส่ง
   - D. แจ้งเตือนสำนักงานเครดิตบูโรเกี่ยวกับคำขอที่เป็นการฉ้อโกง

4. 4. ดัมพ์ข้อมูลจากการละเมิดข้อมูลคืออะไร?
   - A. ชุดข้อมูลรับรองผู้ใช้ที่รั่วไหล ซึ่งเผยแพร่ออนไลน์หรือขายในฟอรัมของแฮกเกอร์
   - B. สำเนาสำรองของไฟล์ฐานข้อมูลที่เก็บไว้นอกสถานที่
   - C. แคชชั่วคราวของล็อกเว็บเซิร์ฟเวอร์
   - D. เครื่องมือผู้ดูแลระบบที่ใช้รีเซ็ตรหัสผ่านผู้ใช้

5. 5. ตัวจัดการรหัสผ่านมีบทบาทอะไร?
   - A. การสร้างและจัดเก็บรหัสผ่านที่ไม่ซ้ำกันและรัดกุมสำหรับทุกบัญชี
   - B. การเฝ้าดูทราฟฟิกเครือข่ายเพื่อหารหัสผ่านที่รั่วไหล
   - C. การบล็อกการโจมตีแบบ **brute-force** อัตโนมัติที่เกตเวย์
   - D. การสแกนบล็อกจัดเก็บฐานข้อมูลเพื่อหารหัสผ่านที่ไม่เข้ารหัส

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. การใช้รหัสผ่านซ้ำในหลายบัญชีเพิ่มความเสี่ยงของ credential stuffing

○ จริง ○ เท็จ

7 คำถาม 7

7. SHA-1 เป็นฟังก์ชันแฮชที่แนะนำสำหรับการจัดเก็บรหัสผ่านสมัยใหม่

○ จริง ○ เท็จ

8 คำถาม 8

8. การบังคับใช้ความซับซ้อนของรหัสผ่านเพียงอย่างเดียว (โดยไม่มี MFA) หยุดการโจมตีแบบ credential stuffing ได้ทั้งหมด

○ จริง ○ เท็จ

9 คำถาม 9

9. เครื่องมือเฝ้าระวังเว็บมืดสแกนอินเทอร์เน็ตเพื่อหาข้อมูลรับรองขององค์กรที่ถูกเจาะ

○ จริง ○ เท็จ

10 คำถาม 10

10. แฮชแบบใส่ salt เพิ่มข้อมูลสุ่มที่ไม่ซ้ำกันลงในรหัสผ่านก่อนแฮช เพื่อต้านการโจมตีด้วย rainbow table

○ จริง ○ เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การทดสอบข้อมูลประจำตัวที่รั่วไหลกับเว็บแอปพลิเคชันจำนวนมากคือการ _____ ข้อมูลประจำตัว
2. อัลกอริทึมแฮชรหัสผ่านแบบปรับได้ที่ช้าซึ่ง OWASP ยังยอมรับคือ _____
3. การเปิดเผยไฟล์ฐานข้อมูลลับบนอินเทอร์เน็ตคือข้อมูล _____
4. การเพิ่มค่าสุ่มลงในรหัสผ่านก่อนแฮชเรียกว่า _____
5. ฐานข้อมูลในเครื่องที่ปลอดภัยสำหรับข้อมูลประจำตัวของผู้ใช้คือ _____ รหัสผ่าน
6. การเพิ่มขั้นตอนยืนยันการเข้าสู่ระบบขั้นที่สองใช้ _____

คลังคำศัพท์

การใส่เกลือ | ตารางสายรุ้ง | บีคริปต์ | ผู้จัดการ | ฟิชชิง | ยัดข้อมูล | รั่วไหล | เอ็มเอฟเอ

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

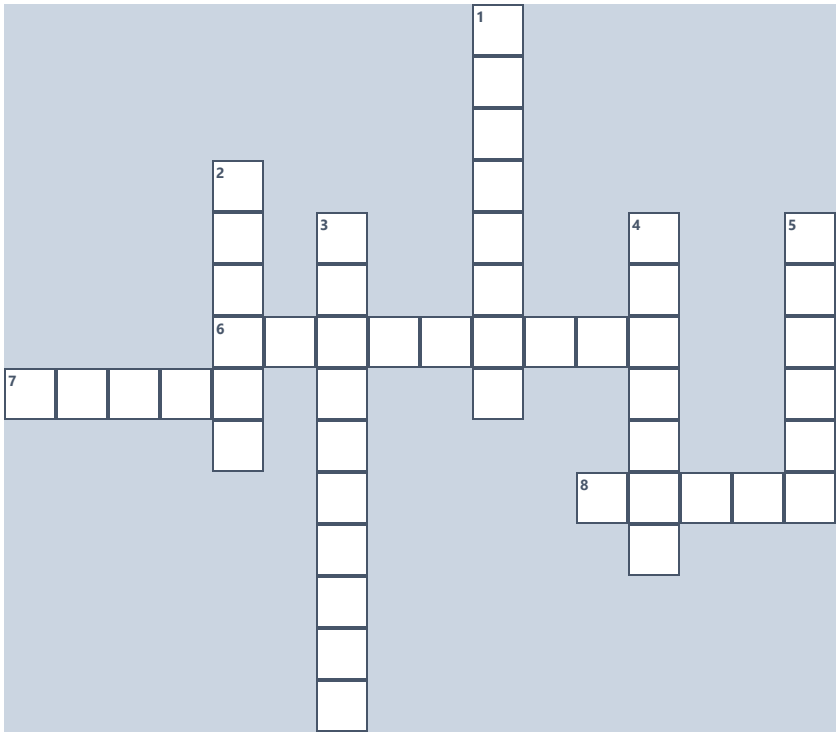
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. การยัด (Stuffing)**	**A**	ตารางแฮชรหัสผ่านที่คำนวณล่วงหน้า
☐	**2. bcrypt**	**B**	การตรวจสอบการเข้าสู่ระบบหลายปัจจัย
☐	**3. การละเมิดข้อมูล**	**C**	เครื่องมือจัดเก็บข้อมูลรับรอง
☐	**4. การใส่ salt**	**D**	การเปิดเผยฐานข้อมูลโดยไม่ได้รับอนุญาต
☐	**5. ตัวจัดการ**	**E**	วิศวกรรมสังคมเพื่อชโมยข้อมูลเข้าสู่ระบบ
☐	**6. MFA**	**F**	การทดสอบข้อมูลรับรองที่รั่วไหล
☐	**7. เรนโบว์**	**G**	การเพิ่ม Salt แบบสุ่มลงในแฮชรหัสผ่าน
☐	**8. ฟิชชิง**	**H**	อัลกอริทึมแฮชรหัสผ่านที่ทำงานช้า

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

6. การเพิ่มค่าเกลือแบบสุ่มลงในแฮชรหัสผ่าน (9)

7. อัลกอริทึมแฮชรหัสผ่านที่ทำงานช้า (5)

8. การเปิดเผยฐานข้อมูลโดยไม่ได้รับอนุญาต (5)

แนวตั้ง

1. การตรวจสอบการเข้าสู่ระบบหลายปัจจัย (8)

2. เครื่องมือจัดเก็บข้อมูลประจำตัว (6)

3. ตารางแฮชรหัสผ่านที่คำนวณไว้ล่วงหน้า (10)

4. วิศวกรรมสังคมเพื่อขโมยข้อมูลเข้าสู่ระบบ (7)

5. การทดสอบข้อมูลประจำตัวที่รั่วไหล (6)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

6 แนวนอน: การเพิ่มค่าเกลือแบบสุ่มลงในแฮชรหัสผ่าน (9 ตัวอักษร):

7 แนวนอน: อัลกอริทึมแฮชรหัสผ่านที่ทำงานช้า (5 ตัวอักษร):

8 แนวนอน: การเปิดเผยฐานข้อมูลโดยไม่ได้รับอนุญาต (5 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: การตรวจสอบการเข้าสู่ระบบหลายปัจจัย (8 ตัวอักษร):

2 แนวตั้ง: เครื่องมือจัดเก็บข้อมูลประจำตัว (6 ตัวอักษร):

3 แนวตั้ง: ตารางแฮชรหัสผ่านที่คำนวณไว้ล่วงหน้า (10 ตัวอักษร):

4 แนวตั้ง: วิศวกรรมสังคมเพื่อขโมยข้อมูลเข้าสู่ระบบ (7 ตัวอักษร):

5 แนวตั้ง: การทดสอบข้อมูลประจำตัวที่รั่วไหล (6 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช มี ฟ บ า า ห ยั นี า ม กี จ า า
รี ต า ว ย ง ก ด ค จ ผู้ น ตี ว ร
ตี ว ช้ า ล ล ด ข้ า อ จั้ ย ซ ฟ ก
อ ก ช ล ม า ป อ อ อ ด ม มี า ล
ลี ล ฮ ป จ ต า มู นี กี ก พ ร เ ง
ก า แ ซ า า า ล ลี จ า ดี า อ็ น
เ ล ผ ดี ซ ร ก ด ห า ร ต า ม จ
ส่ า ค ก ดี า า ซ ล ว ก ด กี เ ด
ใ ท ผ ฟ ซ ง มี ม อ อ ต ฟ ร อ ดี
ร า ท า ส ส รั่ ท ก ข ข า น ฟ ก
า า ล า ม า ว ร ล มี า ร ช เ ก
ก ด ง น ร ย ไ ต ว สี ย ข มี อ ดี
ด ด ว บ ฟ รุ้ ห อ ง า ร ห ห รี น
ผ นี ม ผ ดี ง ล ข กี ส บ ลี ง ด ร
ด ค ผ ห ดี ป ร กี นี า ต จ ห ดี ด

รายการคำศัพท์

ยัดข้อมูล แฮชซ้ำ รั่วไหล การใส่เกลือ ผู้จัดการ เอ็มเอฟเอ ตารางสายรุ้ง หลอกลวง

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. ยัดข้อมูล
B. แฮชช้า
C. รั่วไหล
D. การใส่เกลือ
E. ผู้จัดการ
F. เอ็มเอฟเอ
G. ตารางสายรุ้ง
H. หลอกลวง

คำนิยามและช่องจับคู่
1. วิศวกรรมสังคมเพื่อชโมยข้อมูลเข้าสู่ระบบ
2. การเปิดเผยฐานข้อมูลโดยไม่ได้รับอนุญาต
3. อัลกอริทึมแฮชรหัสผ่านที่ทำงานช้า
4. ตารางแฮชรหัสผ่านที่คำนวณไว้ล่วงหน้า
5. การทดสอบข้อมูลประจำตัวที่รั่วไหล
6. การเพิ่มค่าเกลือแบบสุ่มลงในแฮชรหัสผ่าน
7. เครื่องมือจัดเก็บข้อมูลประจำตัว
8. การตรวจสอบการเข้าสู่ระบบหลายปัจจัย

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. ข้ ย้ อ มู ล ด
2. รั่ ล ห ไ ว
3. ผู้ ด ก ร า จั
4. ส รุ้ ง ง า ย า ต า ร
5. ช า แ ซ้ ฮ
6. ลื ใ า ก เ ก ส่ อ ร
7. เ อ อ ฟ เ อ็ เ ม
8. ล ก ง ห ว ล อ

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
2	กฎสำหรับรหัสผ่านที่รัดกุม			
3	ตัวจัดการรหัสผ่านที่คุณรู้จัก			
4	เครื่องมือด้านความปลอดภัยที่คุณรู้จัก			
5	สัญญาณเตือนในอีเมล			
6	คำสนุก ๆ สำหรับวลีรหัสผ่านที่ยาว			
7	วิธีเข้าสู่ระบบโดยไม่ใช้รหัสผ่าน			
8	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
9	เหตุผลที่ควรอัปเดตซอฟต์แวร์			
10	สิ่งที่ควรทำเมื่อรหัสผ่านรั่วไหล			
11	บัญชีที่ต้องใช้ MFA			
12	สถานที่ที่ไม่ควรเก็บรหัสผ่านเด็ดขาด			
13	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
14	รหัสผ่านที่ไม่ดีที่คนใช้			
15	สิ่งที่คุณสำรองข้อมูล			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การแก้ไขข้อมูลรับรององค์กรรั่วไหล



สถานการณ์: บริการเฝ้าระวัง Dark Web แจ้งองค์กรว่าชุดข้อมูลรั่วไหลที่มีรหัสผ่านของผู้ดูแลระบบองค์กรถูกเผยแพร่ออนไลน์

คำถามอภิปราย: จงวิเคราะห์ความเสี่ยงจากการรั่วไหลของข้อมูลประจำตัว และเสนอกลยุทธ์การรีเซ็ตของผู้ดูแลระบบ

กรณีศึกษาที่ 2: การนำมาตรฐานการแฮชรหัสผ่านมาใช้



สถานการณ์: ฐานข้อมูลองค์กรปัจจุบันจัดเก็บรหัสผ่านผู้ใช้ด้วยแฮช MD5 ที่ล้าสมัยโดยไม่มีซอลต์การเข้ารหัส ทำให้เสี่ยงต่อการถูกดึงข้อมูลออกอย่างรวดเร็ว

คำถามอภิปราย: จงออกแบบกลยุทธ์การย้ายเพื่ออัปเกรดอัลกอริทึมแฮชของฐานข้อมูล

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ปกป้องทรัพย์สินเครือข่ายจากผู้ก่อภัยคุกคามออนไลน์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ โดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง

คีย์เข้ารหัสตัวอักษรเป็นตัวเลข

ก=1 ข=2 ฃ=3 ค=4 ฅ=5 ฆ=6 ง=7 จ=8 ฉ=9 ช=10 ซ=11 ฌ=12
ญ=13 ฎ=14 ฏ=15 ฐ=16 ฑ=17 ฒ=18 ณ=19 ด=20 ต=21 ถ=22 ท=23 ธ=24
น=25 บ=26 ป=27 ผ=28 ฝ=29 พ=30 ฟ=31 ภ=32 ม=33 ย=34 ร=35 ฤ=36
ล=37 ฦ=38 ว=39 ศ=40 ษ=41 ส=42 ห=43 ฬ=44 อ=45 ฮ=46 ะ=47 ◌ั=48
า=49 ◌ำ=50 ◌ิ=51 ◌ี=52 ◌ึ=53 ◌ื=54 ◌ุ=55 ◌ู=56 เ=57 แ=58 โ=59 ใ=60
ไ=61 ◌็=62 ◌่=63 ◌้=64 ◌๊=65 ◌๋=66 ◌์=67

27	1	27	64	45	7		35	43	48	42	28	63	49	25

35	48	63	39	61	43	37		20	64	39	34

43	37	49	34	27	48	8	8	48	34

ข้อความที่ถอดรหัสแล้ว:

คำใบ้: ตัวเลขแต่ละตัวแทนตำแหน่งของตัวอักษรนั้นในตัวอักษรไทย (เช่น 1 = ก, 2 = ข, 67 = ◌์)

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: การรั่วไหลของรหัสผ่านคืออะไร?

การรั่วไหลของรหัสผ่านเกิดขึ้นเมื่อข้อมูลเข้าสู่ระบบของผู้ใช้ถูกเปิดเผยผ่านการละเมิดข้อมูลหรือการกำหนดค่าเซิร์ฟเวอร์ที่ผิดพลาด

Q2: แฮกเกอร์หารหัสผ่านที่รั่วไหลได้อย่างไร?

แฮกเกอร์สแกนฟอรัมดาร์กเว็บ ข้อมูลฐานข้อมูลที่ถูกเปิดเผยต่อสาธารณะ และเว็บไซต์วางข้อความที่มีการเผยแพร่ข้อมูลที่รั่วไหล [8]

Q3: การใช้รหัสผ่านซ้ำอันตรายหรือไม่?

ใช่ เพราะหากเว็บไซต์หนึ่งถูกบุกรุก แฮกเกอร์สามารถลองข้อมูลเข้าสู่ระบบเดียวกันกับแพลตฟอร์มอื่นอีกนับพัน [3]

Q4: ซอลต์เข้ารหัสลับ (cryptographic salt) คืออะไร?

Salt คือข้อมูลสุ่มที่เพิ่มเข้าไปในรหัสผ่านก่อนแฮช ทำให้การโจมตีด้วยการค้นหาจากตารางที่คำนวณไว้ล่วงหน้าไม่ได้ผล [2]

Q5: ทำไม MD5 จึงล้าสมัย?

MD5 เป็นแฮชอเนกประสงค์ที่เร็วและล้าสมัย ผู้โจมตีจึงทดสอบการเดารหัสผ่านได้เร็วมาก โดยเฉพาะเมื่อแฮชไม่มีเกลือ [2]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: โปรแกรมจัดการรหัสผ่านปกป้องผู้ใช้อย่างไร?

สร้างข้อมูลเข้าสู่ระบบที่ซับซ้อนและไม่ซ้ำกันสำหรับทุกเว็บไซต์โดยอัตโนมัติ ลดความผิดพลาดจากความจำของมนุษย์และการใช้ซ้ำ

Q7: การโจมตีแบบ brute force คืออะไร?

การโจมตีที่ทดสอบการผสมอักขระที่เป็นไปได้ทุกแบบอย่างเป็นระบบจนพบรหัสผ่านที่ถูกต้อง [4]

Q8: การล็อกบัญชี (account lockout) ช่วยได้อย่างไร?

การล็อกบัญชีหรือการจำกัดอัตราช่วยชะลอการเดารหัสผ่านออนไลน์ซ้ำ ๆ และเมื่อใช้ร่วมกับการเฝ้าระวังและ MFA จะช่วยลดความเสี่ยงจากการโจมตีแบบ brute-force [4]

Q9: รหัสผ่านหลัก (master password) ปลอดภัยหรือไม่?

ปลอดภัยหากเป็นวลีรหัสผ่านที่มีเอนโทรปีสูงและไม่เคยใช้ซ้ำกับระบบเว็บอื่น

Q10: ควรเปลี่ยนรหัสผ่านเป็นประจำหรือไม่?

NIST ระบุว่าไม่ควรบังคับเปลี่ยนเป็นระยะ ให้เปลี่ยนเมื่อมีหลักฐานว่าถูกบุกรุก และให้ความสำคัญกับความยาว รายการบล็อก และ MFA [1]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: Argon2 เปรียบเทียบกับ bcrypt อย่างไร?

OWASP แนะนำ Argon2id เป็นตัวเลือกแรก การตั้งค่าที่ใช้หน่วยความจำสูงช่วยต้านการถอดรหัสด้วย GPU และ ASIC ได้ดีกว่า bcrypt [2]

Q2: key stretching คืออะไร?

เทคนิคที่วนอัลกอริทึมแฮชซ้ำหลายพันครั้งเพื่อทำให้กระบวนการตรวจสอบรหัสผ่านช้าลง ทำให้การเจาะรหัสมีต้นทุนสูง [2]

Q3: Rainbow table ทำงานอย่างไร?

เป็นตารางค้นหาที่คำนวณไว้ล่วงหน้าซึ่งเชื่อมรหัสผ่านข้อความธรรมดากับแฮช ใช้ย้อนกลับแฮชที่ไม่มี salt ได้อย่างรวดเร็ว [2]

Q4: การนำข้อมูลรับรองกลับมาใช้ซ้ำ (credential recycling) คืออะไร?

การนำคู่ชื่อผู้ใช้/รหัสผ่านที่ถูกขโมยจากการรั่วไหลครั้งหนึ่งไปลองเข้าถึงบริการอื่น โดยเฉพาะเมื่อผู้คนใช้รหัสผ่านซ้ำ [3]

Q5: โปรแกรมจัดการรหัสผ่านถูกแฮกได้หรือไม่?

ได้ หลายรายใช้การเข้ารหัสแบบ zero-knowledge ดังนั้นหากเซิร์ฟเวอร์ถูกเจาะ จะเปิดเผยเฉพาะตู้นิรภัยที่เข้ารหัสไว้ แต่รหัสผ่านหลักที่อ่อนก็ยังถูกถอดรหัสแบบออฟไลน์ได้

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: การโจมตีแบบพจนานุกรม (dictionary attack) คืออะไร?

การโจมตีแบบ Brute-force รูปแบบหนึ่งที่ทดสอบคำทั่วไป วลี และรหัสผ่านที่เคยรั่วไหลในอดีต แทนที่จะสุ่มตัวอักษร

Q7: ทำไมจึงนิยมใช้ passphrase?

วลีรหัสผ่านใช้คำสุ่มหลายคำ ทำให้มีเอนโทรปีสูง มนุษย์จำง่ายแต่ใช้การคำนวณมากในการถอดรหัส [1]

Q8: การลงชื่อเข้าใช้ครั้งเดียว (SSO) ส่งผลต่อการรั่วไหลของรหัสผ่านอย่างไร?

SSO ลดการกระจายของรหัสผ่านหลายชุด แต่ผู้ให้บริการระบุตัวตนกลายเป็นเป้าหมายที่มีมูลค่าสูงซึ่งต้องใช้ MFA ที่แข็งแกร่ง โดยควรเป็นแบบที่ทนต่อฟิชชิง [6]

Q9: การแย่งเซสชัน (session hijacking) คืออะไร?

ผู้โจมตีได้มาหรือใช้โทเค็นเซสชันที่ใช้ได้ในทางที่ผิดเพื่อปลอมเป็นผู้ใช้ที่ลงชื่อเข้าใช้โดยไม่ต้องใช้รหัสผ่านอีก [5]

Q10: คุณตรวจจับ password spraying ได้อย่างไร?

ด้วยการมองหารหัสผ่านชุดเดิมจำนวนน้อยที่ถูกลองกับหลายบัญชี ซึ่งมักทำอย่างช้าๆ เพื่อไม่ให้เกินเกณฑ์การล็อกบัญชี [7]

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

NIST SP 800-63B กำหนดให้ตรวจสอบรหัสผ่านใหม่เทียบกับรายการบล็อกของรหัสผ่านที่พบบ่อยและรหัสผ่านที่ถูกบุกรุก [1]

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ข้อมูลรั่วไหล 'Collection #1' ในปี 2019 รวมข้อมูลจากการละเมิดหลายครั้งก่อนหน้านี้เป็นไฟล์ขนาดใหญ่ไฟล์เดียวที่มีคู่อีเมลและรหัสผ่าน [8]

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ปัจจุบัน NIST กำหนดให้รหัสผ่านที่ใช้เป็นปัจจัยการยืนยันตัวตนเพียงอย่างเดียวต้องยาวอย่างน้อย 15 อักขระ [1]

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ฮาร์ดแวร์ ASIC คำนวณแฮช SHA-256 ได้หลายพันล้านค่าต่อวินาที ทำให้การแฮช SHA แบบดิบไม่ปลอดภัยสำหรับรหัสผ่านของผู้ใช้ [2]

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

salt ที่ไม่ซ้ำกันทำให้ผู้ใช้สองคนที่ใช้รหัสผ่านเดียวกันได้ค่าแฮชในฐานข้อมูลต่างกัน [2]

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ตัวจัดการรหัสผ่านจำนวนมากเข้ารหัสข้อมูลในห้องนิรภัยภายในเครื่องด้วยการเข้ารหัสที่แข็งแกร่งซึ่งสร้างจากรหัสผ่านหลักของผู้ใช้

7. ข้อมูลเชิงลึกด้านความปลอดภัย

Credential Stuffing ได้ผลเพราะหลายคนใช้รหัสผ่านเดิมซ้ำกับบัญชีอีคอมเมิร์ซ ธนาคาร และอีเมล [3]

8. ข้อมูลเชิงลึกด้านความปลอดภัย

NIST SP 800-63B ระบุว่าผู้ตรวจสอบต้องไม่บังคับให้เปลี่ยนรหัสผ่านเป็นระยะ แต่ให้เปลี่ยนเฉพาะเมื่อมีหลักฐานว่าถูกบุกรุก [1]

9. ข้อมูลเชิงลึกด้านความปลอดภัย

การเพิ่มตัวอักษรพิมพ์ใหญ่หนึ่งตัวและสัญลักษณ์หนึ่งตัวในรหัสผ่านสั้นไม่ได้หยุดการโจมตีแบบพจนานุกรมอัตโนมัติด้วย GPU สมัยใหม่ [1]

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

MFA สามารถบล็อกความพยายามแบบ credential stuffing ได้จำนวนมากแม้รหัสผ่านรั่วไหลแล้ว MFA ที่ต้านทานฟิชชิงแข็งแกร่งกว่ารหัส SMS [3]

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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/

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

Credential stuffing ใช้ระบบอัตโนมัติลองใช้คู่ชื่อผู้ใช้/รหัสผ่านที่รั่วไหลกับเว็บไซต์อื่น [3]

2 คำถาม 2

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

OWASP แนะนำ Argon2id เป็นอันดับแรก ส่วน bcrypt ใช้เป็นหลักกับระบบรุ่นเก่าที่ไม่มี Argon2id หรือ scrypt [2]

3 คำถาม 3

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

MFA ต้องใช้ปัจจัยเพิ่มเติม ดังนั้นรหัสผ่านที่ถูกขโมยเพียงอย่างเดียวจึงปลดล็อกบัญชีไม่ได้ [3]

4 คำถาม 4

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ชุดข้อมูลรั่วไหล (breach dump) คือชุดข้อมูลประจำตัวที่รั่วไหล เช่น ชุดรวม Collection #1 ปี 2019 [8]

5 คำถาม 5

คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ตัวจัดการรหัสผ่านสร้างและจัดเก็บรหัสผ่านที่ไม่ซ้ำกันและคาดเดายากสำหรับทุกบัญชี ป้องกันการใช้ซ้ำ [3]

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

จริง: รหัสผ่านที่ใช้ซ้ำทำให้ผู้โจมตีนำข้อมูลประจำตัวที่รั่วไหลจากเว็บไซต์หนึ่งไปลองใช้กับเว็บไซต์อื่นได้ [3]

7 **คำถาม 7** — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

เท็จ: SHA-1 เป็นแฮชที่เร็ว OWASP แนะนำ Argon2id, scrypt, bcrypt หรือ PBKDF2 แทน [2]

8 **คำถาม 8** — **คำตอบที่ถูกต้อง: เท็จ**

หมายเหตุสำหรับผู้สอน

เท็จ: กฎความซับซ้อนเพียงอย่างเดียวไม่สามารถหยุด stuffing ด้วยรหัสผ่านที่รั่วไหลและใช้ซ้ำได้ จำเป็นต้องใช้ MFA [3]

9 **คำถาม 9** — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

จริง: บริการเฝ้าระวังค้นหาชุดข้อมูลรั่วไหลและแหล่งข้อมูลดาร์กเว็บเพื่อหาข้อมูลประจำตัวที่ถูกเปิดเผย [8]

10 **คำถาม 10** — **คำตอบที่ถูกต้อง: จริง**

หมายเหตุสำหรับผู้สอน

จริง: ค่าซอลต์ที่ไม่ซ้ำกันสำหรับแต่ละรหัสผ่านทำให้ตารางเรนโบว์ที่คำนวณไว้ล่วงหน้าใช้ไม่ได้ผล [2]

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

เกณฑ์การให้คะแนนของผู้สอน: ให้ 1 คะแนนสำหรับการจับคู่ที่ถูกต้องแต่ละข้อ (รวม 8 คะแนน) และคำศัพท์บริบท (รวม 6 คะแนน)

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

F 1. การยัด (Stuffing)	H 2. bcrypt	D 3. การละเมิดข้อมูล	G 4. การใส่ salt
C 5. ตัวจัดการ	B 6. MFA	A 7. เรนโบว์	E 8. ฟิชชิง

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 ยัดข้อมูล	2 บีคริปต์	3 รั่วไหล	4 การใส่เกลือ
5 ผู้จัดการ	6 เอ็มเอฟเอ		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 H – หลอกลวง	2 C – รั่วไหล	3 B – แฮชช้า	4 G – ตารางสายรุ้ง
5 A – ยัดข้อมูล	6 D – การใส่เกลือ	7 E – ผู้จัดการ	8 F – เอ็มเอฟเอ

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย การยัด (Stuffing) bcrypt และ การละเมิดข้อมูล ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

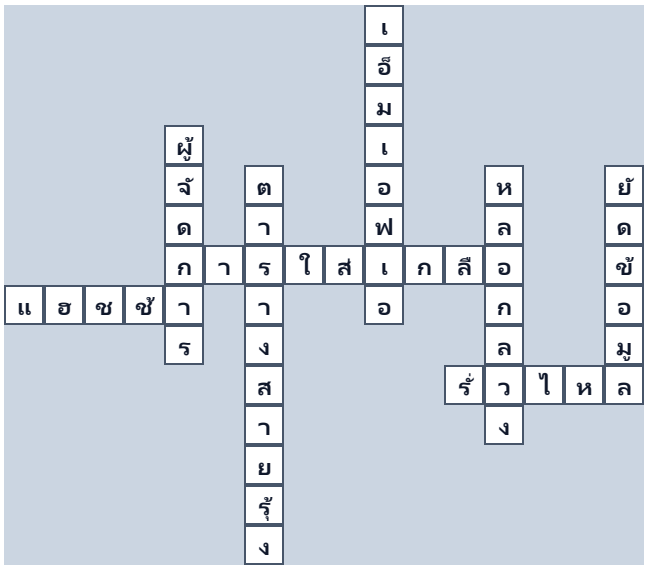
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	ฟ	บ	า	า	ห	ยั	นี	า	ม	กี	จ	า	า
รี	ต	า	ว	ย	ง	ก	ด	ค	จ	ผู้	น	ตี	ว	ร
ดี	ว	ช้	า	ล	ล	ด	ข้	า	อ	จั	ย	ช	ฟ	ก
อ	ก	ช	ล	ม	า	ป	อ	อ	อ	ด	ม	มี	า	ล
ลี	ล	ฮ	ป	จ	ต	า	มู	นี	กี	ก	พ	ร	เ	ง
ก	า	แ	ช	า	า	า	ล	ลี	จ	า	ตี	า	อ็	น
เ	ล	ผ	ดี	ช	ร	ก	ด	ห	า	ร	ต	า	ม	จ
ส่	า	ค	ก	ดี	า	า	ช	ล	ว	ก	ด	กี	เ	ด
ใ	ท	ผ	ฟ	ช	ง	มี	ม	อ	อ	ต	ฟ	ร	อ	ดี
ร	า	ท	า	ส	ส	รั่	ท	ก	ข	ข	า	น	ฟ	ก
า	า	ล	า	ม	า	ว	ร	ล	มี	า	ร	ช	เ	ก
ก	ด	ง	น	ร	ย	ไ	ต	ว	สี	ย	ข	มี	อ	ดี
ด	ด	ว	บ	ฟ	รุ้	ห	อ	ง	า	ร	ห	ห	รี	น
ผ	นี	ม	ผ	ดี	ง	ล	ข	กี	ส	บ	ลี	ง	ด	ร
ด	ค	ผ	ห	ดี	ป	ร	กี	นี	า	ต	จ	ห	ดี	ด

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

6 แนวนอน: การ์ใส่เกลือ การเพิ่มค่าเกลือแบบสุ่มลงในแฮชรหัสผ่าน (9 ตัวอักษร)

7 แนวนอน: แฮชช้า อัลกอริทึมแฮชรหัสผ่านที่ทำงานช้า (5 ตัวอักษร)

8 แนวนอน: รั่วไหล การเปิดเผยฐานข้อมูลโดยไม่ได้รับอนุญาต (5 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: เอ็มเอฟเอ การตรวจสอบการเข้าสู่ระบบหลายปัจจัย (8 ตัวอักษร)

2 แนวตั้ง: ผู้จัดการ เครื่องมือจัดเก็บข้อมูลประจำตัว (6 ตัวอักษร)

3 แนวตั้ง: ตารางสายรุ้ง ตารางแฮชรหัสผ่านที่คำนวณไว้ล่วงหน้า (10 ตัวอักษร)

4 แนวตั้ง: หลอกลวง วิศวกรรมสังคมเพื่อขโมยข้อมูลเข้าสู่ระบบ (7 ตัวอักษร)

5 แนวตั้ง: ยัดข้อมูล การทดสอบข้อมูลประจำตัวที่รั่วไหล (6 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. ข้ยอ้มูลด → ยัดข้อมูล
2. รั่ลหไว → รั่วไหล
3. ผู้ดกราจั → ผู้จัดการ
4. สรุ้งงายาตาร → ตารางสายรุ้ง
5. ชาแซ้ฮ → แฮชช้า
6. ลีใกเกสอร → การใส่เกลือ
7. เออฟเอ็เม → เอ็มเอฟเอ
8. ลกงหวลอ → หลอกลวง

เฉลยภารกิจรหัสลับ

"ปกป้อง รหัสผ่าน รั่วไหล ด้วย หลายปัจจัย"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การแก้ไขข้อมูลรับรององค์กรรั่วไหล

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: บริการเฝ้าระวัง dark web แจ้งองค์กรว่าฐานข้อมูลที่รั่วไหลซึ่งมีรหัสผ่านของผู้ดูแลระบบองค์กรถูกเผยแพร่ออนไลน์
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: เพิกถอนเซสชันผู้ดูแลระบบที่ใช้งานอยู่ทั้งหมดและรีเซ็ตข้อมูลรับรองด้วยตัวสร้างที่มีเอนโทรปีสูง บังคับใช้ MFA ที่ทนต่อฟิชชิงบนพอร์ทัลผู้ดูแลระบบ [6] หมุนเวียนคีย์ API ที่ได้รับผลกระทบ ตรวจสอบบันทึกการล็อกอินหาจุดรั่วไหลแรกเริ่ม และตรวจสอบบัญชีที่มีสิทธิ์พิเศษอื่น

B กรณีศึกษาที่ 2: การนำมาตรฐานการแฮชรหัสผ่านมาใช้

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: ฐานข้อมูลขององค์กรเก็บรหัสผ่านของผู้ใช้โดยใช้แฮช MD5 ที่ล้าสมัยและไม่มีซอลต์เข้ารหัส ทำให้ถูกดึงข้อมูลออกไปได้อย่างรวดเร็ว
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ใช้ Argon2id (หรือ bcrypt บนระบบรุ่นเก่า) พร้อมซอลต์เฉพาะต่อผู้ใช้ [2] ห่อหุ้มแฮช MD5 ที่มีอยู่ด้วยอัลกอริทึมใหม่ในตอนนี้ แฮชใหม่โดยตรงเมื่อผู้ใช้แต่ละคนเข้าสู่ระบบครั้งถัดไป และบังคับรีเซ็ตสำหรับบัญชีที่ไม่ได้ใช้งานมานาน