



20225261

bao.kv225261@sis.hust.edu.vn

1

2

3

4

5

6

7

8

9

10

Quiz 11 - Xác thực danh tính

Homework due Jul 1, 2025 07:00 +07 *Completed*

Question #13d55

1/1 point (graded)

Câu 1. Những nguyên nhân nào sau đây làm giảm tính an toàn và tin cậy của hệ xác thực bằng mật khẩu?

- ☒ Người dùng không thể nhớ được mật khẩu phức tạp
- ☒ Không sử dụng cơ chế mật mã để bảo vệ đường truyền khi người dùng truy cập
- ☒ Người dùng sử dụng mật khẩu giống nhau cho nhiều tài khoản
- ☒ Không có cơ chế để người dùng xác minh đang truy cập vào đúng hệ thống
- ☒ Hệ thống không sử dụng cơ chế hạn chế số lần đăng nhập sai



Submit

Question #6200f

1/1 point (graded)

Câu 2. Mật khẩu là yếu tố xác thực thuộc loại nào?

- ☒ Yếu tố tri thức
- ☐ Yếu tố tài sản
- ☐ Yếu tố sinh trắc



Submit

Question #898c8

1/1 point (graded)

Câu 3. Mục đích chính khi áp dụng hàm băm lên mật khẩu người dùng trước khi lưu trữ là gì?

- ☐ Tiết kiệm dung lượng bộ nhớ để lưu trữ mật khẩu
- ☐ Chống tấn công phát lại
- ☒ Ngăn cản kẻ tấn công biết được mật khẩu dạng bản rõ
- ☐ Giảm độ phức tạp tính toán khi mã hóa bảo vệ mật khẩu bằng hệ mật khóa bất đối xứng



Submit

### Question #8ff84

1/1 point (graded)

Câu 4. Mục đích của việc thêm giá trị salt ngẫu nhiên vào mật khẩu trước khi băm là gì?

- ☐ Giảm thời gian tính toán
- ☐ Giảm thiểu rủi ro tấn công vét cạn
- ☒ Giảm thiểu rủi ro tấn công từ điển/tấn công cầu vồng
- ☐ Giảm tốc độ dò tìm mật khẩu



Submit

### Question #87fbc

1/1 point (graded)

Câu 5. Trong các cách thức sau mật khẩu được lưu trữ như thế nào là an toàn nhất?

- ☐ MD5(Password)
- ☐ MD5(Password, Salt)
- ☐ SHA-1(Password, Salt)
- ☐ SHA-1(SHA-256(Password))
- ☐ SHA-256(Password, Salt)
- ☒ SHA-256(Password, Salt, Pepper)



Submit

### Question #384d8

1/1 point (graded)

Câu 6. Biện pháp nào sau đây được sử dụng để làm giảm tốc độ dò tìm mật khẩu của kẻ tấn công?

- ☐ Quy định độ dài tối thiểu cho mật khẩu
- ☒ Yêu cầu hoàn thành CAPTCHA mỗi khi đăng nhập
- ☐ Quy định các dạng ký tự phải có mặt trong mật khẩu
- ☒ Khóa tài khoản trong một khoảng thời gian nhất định sau một số lần đăng nhập sai
- ☐ Quy định thời hạn sử dụng mật khẩu



Submit

### Question #d0c2e

1/1 point (graded)

Câu 7. Khi sử dụng mã xác thực để khôi phục mật khẩu, biện pháp nào sau đây nên được áp dụng?

- ☐ Kích hoạt sớm các cơ chế chờ xác thực lại nếu người dùng cung cấp mã xác thực sai
- ☐ Thiết lập thời hạn sử dụng ngắn cho mã xác thực
- ☐ Kích hoạt sớm các cơ chế thách thức nếu người dùng cung cấp mã xác thực sai
- ☐ Tạo mã xác thực ngẫu nhiên

☒ Tất cả các biện pháp trên



Submit

---

Question #a58e4

1/1 point (graded)

Câu 8. Tại sao giao thức xác thực CHAP an toàn hơn so với PAP?

- ☐ Sử dụng cơ chế thách thức khi xác thực thất bại
- ☒ Không lộ mật khẩu trên kênh truyền
- ☐ Yêu cầu phải băm mật khẩu cùng salt khi lưu trữ
- ☐ Tất cả đáp án trên đều đúng



Submit

---

Question #8ccf9

1/1 point (graded)

Câu 9. Tại sao sử dụng phương pháp xác thực đa yếu tố nâng cao an toàn cho hệ xác thực bằng mật khẩu?

- ☐ Kẻ tấn công mất nhiều thời gian để vét cạn mật khẩu hơn
- ☐ Mật khẩu được lưu trữ an toàn hơn
- ☐ Tài sản của người dùng khó bị đánh cắp hơn
- ☐ Vân tay khó bị làm giả hơn
- ☒ Kẻ tấn công phải chiếm đoạt được tất cả các yếu tố xác thực



Submit

---

Question #80ca9

1/1 point (graded)

Câu 10. Ưu điểm của TOPT so với HOTP là gì?

- ☒ Tự động sinh và thay đổi OTP theo thời gian
- ☐ Có thể tạo OTP với độ dài tùy ý
- ☒ Khó bị mất đồng bộ hơn
- ☐ Thuật toán sinh OTP đơn giản hơn



Submit