**ÔN TẬP**

**TUẦN 3 – TOP 10 OSWAP**

**Câu 1: Injection trong bảo mật web là gì?**

**a. Việc chèn mã độc vào ứng dụng thông qua đầu vào không được kiểm tra đúng cách**

b. Việc thay đổi quyền truy cập vào hệ thống

c. Việc sử dụng giao thức mã hóa yếu

d. Việc không ghi lại các sự kiện bảo mật

**Câu 2: OWASP Top 10 là danh sách gì?**

**a. Danh sách 10 rủi ro bảo mật phổ biến nhất cho các ứng dụng web**

b. Danh sách 10 ứng dụng bảo mật web hàng đầu

c. Danh sách 10 công cụ bảo mật phổ biến nhất

d. Danh sách 10 biện pháp bảo mật cho website

**Câu 3: Ghép cặp các lỗ hổng bảo mật với vị trí của chúng trong OWASP Top 10.**

**a. Broken Access Control → 1, Security Misconfiguration → 5, Injection → 3, Cryptographic Failures → 2, Insecure Design → 4**

b. Broken Access Control → 6, Security Misconfiguration → 5, Injection → 3, Cryptographic Failures → 2, Insecure Design → 3

c. Broken Access Control → 1, Security Misconfiguration → 5, Injection → 3, Cryptographic Failures → 2, Insecure Design → 6

d. Broken Access Control → 6, Security Misconfiguration → 5, Injection → 4, Cryptographic Failures → 2, Insecure Design → 3

**Câu 4: Broken Access Control là?**

**a. Việc truy cập trái phép vào hệ thống do kiểm soát truy cập không chính xác**

b. Việc sử dụng thuật toán mã hóa yếu

c. Việc tiêm mã độc hại vào hệ thống

d. Việc cấu hình sai hệ thống

**Câu 5: Rủi ro Cryptographic Failures có nghĩa là gì?**

**a. Lỗ hổng bảo mật do sử dụng mã hóa yếu hoặc lỗi thời**

b. Lỗ hổng bảo mật do quyền truy cập không đúng

c. Lỗ hổng bảo mật do tiêm mã độc

d. Lỗ hổng bảo mật do cấu hình sai

**Câu 6: Biện pháp nào sau đây giúp ngăn chặn Security Logging and Monitoring Failures?**

**a. Ghi lại và giám sát tất cả các sự kiện bảo mật đáng ngờ**

b. Tắt chức năng ghi log khi không cần thiết

c. Không ghi lại các giao dịch có giá trị cao

d. Chỉ lưu trữ log cục bộ

**Câu 7: Ví dụ nào sau đây là rủi ro do Vulnerable and Outdated Components?**

**a. Sử dụng phiên bản lỗi thời của thư viện phần mềm**

b. Sử dụng giao thức mã hóa yếu

c. Không ghi log các sự kiện bảo mật

d. Không giới hạn quyền truy cập vào hệ thống

**Câu 8: Ghép cặp các lỗ hổng bảo mật với loại tấn công tương ứng.**

**a.  Injection → Tiêm mã độc vào cơ sở dữ liệu, Vulnerable Components → Tấn công hệ thống sử dụng thành phần lỗi thời, Broken Access Control → Tấn công vượt qua các rào cản xác thực, Cryptographic Failures → Giải mã dữ liệu nhạy cảm trái phép, Cross-Site Scripting → Chèn mã JavaScript độc hại**

b.  Injection → Tiêm mã độc vào cơ sở dữ liệu, Vulnerable Components → Tấn công hệ thống sử dụng thành phần lỗi thời, Broken Access Control → Tấn công vượt qua các rào cản xác thực, Cryptographic Failures → Giải mã dữ liệu nhạy cảm trái phép, Cross-Site Scripting → Chèn mã JavaScript độc hại

c. Cross-Site Scripting → Tiêm mã độc vào cơ sở dữ liệu, Vulnerable Components → Tấn công hệ thống sử dụng thành phần lỗi thời, Broken Access Control → Tấn công vượt qua các rào cản xác thực, Cryptographic Failures → Giải mã dữ liệu nhạy cảm trái phép,  Injection → Chèn mã JavaScript độc hại

d.  Injection → Tiêm mã độc vào cơ sở dữ liệu, Vulnerable Components → Tấn công hệ thống sử dụng thành phần lỗi thời, Broken Access Control → Tấn công vượt qua các rào cản xác thực, Cryptographic Failures → Giải mã dữ liệu nhạy cảm trái phép, Cross-Site Scripting → Chèn mã Assembly độc hại

**Câu 9: Ghép cặp các thuật ngữ bảo mật với định nghĩa của chúng.**

**a. CSRF (Cross-Site Request Forgery) → Kẻ tấn công gửi yêu cầu trái phép thay mặt người dùng hợp lệ, SQL Injection → Lỗ hổng tiêm mã lệnh SQL qua đầu vào không được xác thực, XSS (Cross-Site Scripting) → Chèn mã JavaScript độc hại vào trang web, Multi-Factor Authentication → Xác thực sử dụng nhiều phương pháp khác nhau, SSL/TLS → Giao thức mã hóa dữ liệu truyền tải qua Internet**

b. CFRF (Cross-Site Request Forgery) → Kẻ tấn công gửi yêu cầu trái phép thay mặt người dùng hợp lệ, SQL Injection → Lỗ hổng tiêm mã lệnh SQL qua đầu vào không được xác thực, XSS (Cross-Site Scripting) → Chèn mã JavaScript độc hại vào trang web, Multi-Factor Authentication → Xác thực sử dụng nhiều phương pháp khác nhau, SSL/TLS → Giao thức mã hóa dữ liệu truyền tải qua Internet

c. CSRF (Cross-Site Request Forgery) → Kẻ tấn công gửi yêu cầu trái phép thay mặt người dùng hợp lệ, SQL Injection → Lỗ hổng tiêm mã lệnh SQL qua đầu vào không được xác thực, XLSS (Cross Large Site Scripting) → Chèn mã JavaScript độc hại vào trang web, Multi-Factor Authentication → Xác thực sử dụng nhiều phương pháp khác nhau, SSL/TLS → Giao thức mã hóa dữ liệu truyền tải qua Internet

d. CSRF (Cross-Site Request Forgery) → Kẻ tấn công gửi yêu cầu trái phép thay mặt người dùng hợp lệ, noSQL Injection → Lỗ hổng tiêm mã lệnh noSQL qua đầu vào không được xác thực, XSS (Cross-Site Scripting) → Chèn mã JavaScript độc hại vào trang web, Multi-Factor Authentication → Xác thực sử dụng nhiều phương pháp khác nhau, SSL/TLS → Giao thức mã hóa dữ liệu truyền tải qua Internet

**Câu 10: Ghép cặp các biện pháp phòng ngừa với rủi ro bảo mật tương ứng của chúng.**

**a. Cập nhật phần mềm thường xuyên → Vulnerable and Outdated Components, Kiểm tra đầu vào người dùng → Injection, Mã hóa dữ liệu nhạy cảm → Cryptographic Failures, Giới hạn quyền truy cập tài nguyên → Broken Access Control, Sử dụng xác thực nhiều yếu tố → Identification and Authentication Failures**

b. Cập nhật phần mềm thường xuyên → Vulnerable and Outdated Components, Kiểm tra đầu vào người dùng → Injection, Mã hóa dữ liệu nhạy cảm → Cryptographic Failures, Giới hạn quyền truy cập tài nguyên → Broken Access Control, Sử dụng xác thực nhiều yếu tố → Bcrypt

c. Hạn chế nhật phần mềm thường xuyên → Vulnerable and Outdated Components, Kiểm tra đầu vào người dùng → Injection, Mã hóa dữ liệu nhạy cảm → Cryptographic Failures, Giới hạn quyền truy cập tài nguyên → Broken Access Control, Sử dụng xác thực nhiều yếu tố → Identification and Authentication Failures

d. Cập nhật phần mềm thường xuyên → Vulnerable and Outdated Components, Kiểm tra đầu vào người dùng → Cross-Site Scripting, Mã hóa dữ liệu nhạy cảm → Cryptographic Failures, Giới hạn quyền truy cập tài nguyên → Broken Access Control, Sử dụng xác thực nhiều yếu tố → Identification and Authentication Failures

**Câu 11: Rủi ro bảo mật nào được xếp hạng số 1 trong danh sách OWASP Top 10?**

**a. Broken Access Control**

b. Cryptographic Failures

c. Injection

d. Security Misconfiguration

**Câu 12: Identification and Authentication Failures là?**

**a. Rủi ro liên quan đến việc xác thực và định danh không chính xác**

b. Rủi ro liên quan đến mã hóa không an toàn

c. Rủi ro liên quan đến việc cấu hình sai hệ thống

d. Rủi ro liên quan đến việc không ghi log sự kiện bảo mật

**Câu 13: Biện pháp nào giúp ngăn chặn Software and Data Integrity Failures?**

**a. Sử dụng các thành phần phần mềm từ nguồn tin cậy**

b. Tắt chức năng ghi log

c. Chỉ sử dụng các thư viện mã nguồn mở

d. Sử dụng các khóa mã hóa yếu

**Câu 14: Server-Side Request Forgery (SSRF) là lỗ hổng bảo mật gì?**

**a. Lỗ hổng cho phép kẻ tấn công gửi các yêu cầu trái phép đến các tài nguyên từ xa**

b. Lỗ hổng cho phép kẻ tấn công truy cập không giới hạn vào hệ thống

c. Lỗ hổng cho phép kẻ tấn công thực thi mã trên máy chủ

d. Lỗ hổng cho phép kẻ tấn công đánh cắp dữ liệu từ hệ thống

**Câu 15: Đâu là ví dụ về lỗ hổng Injection?**

**a. SQL Injection**

b. CSRF

c. XSS

d. DDoS

**Câu 16: Ghép cặp các lỗ hổng bảo mật với ví dụ của chúng.**

**a. Insecure Design → Thiết kế hệ thống mà không tính đến các yêu cầu bảo mật, Broken Access Control → Truy cập tệp tin quan trọng mà không có xác thực, Injection → SQL Injection, Vulnerable Components → Sử dụng phiên bản lỗi thời của thư viện phần mềm, Cross-Site Scripting (XSS) → Chèn mã JavaScript độc hại vào trang web**

b. Insecure Design → Thiết kế hệ thống đã tính toán đến các yêu cầu bảo mật, Broken Access Control → Truy cập tệp tin quan trọng mà không có xác thực, Injection → SQL Injection, Vulnerable Components → Sử dụng phiên bản lỗi thời của thư viện phần mềm, Cross-Site Scripting (XSS) → Chèn mã JavaScript độc hại vào trang web

c. Insecure Design → Thiết kế hệ thống mà không tính đến các yêu cầu bảo mật, Broken Access Control → Truy cập tệp tin quan trọng mà không có xác thực, Cross-Site Scripting → Scripting Injection, Vulnerable Components → Sử dụng phiên bản lỗi thời của thư viện phần mềm, Cross Large Site Scripting (XLSS) → Chèn mã JavaScript độc hại vào trang web

d. Insecure System → Thiết kế hệ thống mà không tính đến các yêu cầu bảo mật, Broken Access Control → Truy cập tệp tin quan trọng mà không có xác thực, Injection → SQL Injection, Vulnerable Components → Sử dụng phiên bản lỗi thời của thư viện phần mềm, Cross-Site Scripting (XSS) → Chèn mã JavaScript độc hại vào trang web

**Câu 17: Ghép cặp các lỗ hổng bảo mật với hậu quả của chúng.**

**a. Broken Access Control → Truy cập trái phép vào dữ liệu nhạy cảm, Injection → Thực thi mã độc trên máy chủ, Vulnerable Components → Hệ thống bị khai thác bởi các lỗ hổng đã biết, Identification Failures → Xác thực người dùng không chính xác, Security Misconfiguration → Rò rỉ thông tin nhạy cảm**

b. Broken Access Control → Truy cập trái phép vào dữ liệu nhạy cảm, Injection → Thực thi mã độc trên máy chủ, Vulnerable Components → Hệ thống bị khai thác bởi các lỗ hổng đã biết, Attribute Control Failures → Xác thực người dùng không chính xác, Security Misconfiguration → Rò rỉ thông tin nhạy cảm

c. Broken Access Control → Truy cập trái phép vào dữ liệu nhạy cảm, Injection → Thực thi mã độc trên máy chủ, Vulnerable Items → Hệ thống bị khai thác bởi các lỗ hổng đã biết, Identification Failures → Xác thực người dùng không chính xác, Security Misconfiguration → Rò rỉ thông tin nhạy cảm

d. Access Control List→ Truy cập trái phép vào dữ liệu nhạy cảm, Injection → Thực thi mã độc trên máy chủ, Vulnerable Components → Hệ thống bị khai thác bởi các lỗ hổng đã biết, Identification Failures → Xác thực người dùng không chính xác, Security Misconfiguration → Rò rỉ thông tin nhạy cảm

**Câu 18: Biện pháp nào giúp ngăn chặn các rủi ro Cryptographic Failures?**

**a. Mã hóa dữ liệu nhạy cảm khi lưu trữ và truyền tải**

b. Sử dụng các mật khẩu mặc định

c. Tắt chức năng ghi log

d. Chỉ mã hóa dữ liệu khi cần thiết

**Câu 19: Ghép cặp các biện pháp bảo mật với mục tiêu của chúng.**

**a. Xác thực nhiều yếu tố → Giảm rủi ro về xác thực và định danh sai, Ghi log các sự kiện bảo mật → Giúp phát hiện và xử lý các sự cố bảo mật, Kiểm tra và lọc đầu vào → Ngăn chặn các cuộc tấn công tiêm mã độc, Mã hóa dữ liệu → Bảo vệ tính bảo mật của dữ liệu, Cập nhật phần mềm thường xuyên → Ngăn chặn việc khai thác các lỗ hổng bảo mật đã biết**

b. Xác thực nhiều yếu tố → Giảm rủi ro về xác thực và định danh sai, Ghi log các sự kiện bảo mật → Giúp phát hiện và xử lý các sự cố bảo mật, Kiểm tra và lọc đầu vào → Ngăn chặn các cuộc tấn công tiêm mã độc bằng Assembly, Mã hóa dữ liệu → Bảo vệ tính bảo mật của dữ liệu, Cập nhật phần mềm thường xuyên → Ngăn chặn việc khai thác các lỗ hổng bảo mật đã biết

c. Xác thực một yếu tố → Giảm rủi ro về xác thực và định danh sai, Ghi log các sự kiện bảo mật → Giúp phát hiện và xử lý các sự cố bảo mật, Kiểm tra và lọc đầu vào → Ngăn chặn các cuộc tấn công tiêm mã độc, Mã hóa dữ liệu → Bảo vệ tính bảo mật của dữ liệu, Cập nhật phần mềm thường xuyên → Ngăn chặn việc khai thác các lỗ hổng bảo mật đã biết

d. Xác thực nhiều yếu tố → Giảm rủi ro về xác thực và định danh sai, Ghi log các sự kiện bảo mật → Giúp phát hiện và xử lý các sự cố bảo mật, Kiểm tra và lọc đầu vào → Ngăn chặn các cuộc tấn công tiêm mã độc, Mã hóa dữ liệu bằng DES → Bảo vệ tính bảo mật của dữ liệu, Cập nhật phần mềm thường xuyên → Ngăn chặn việc khai thác các lỗ hổng bảo mật chưa biết

**Câu 20: OWASP Juice Shop là?**

**a. Một ứng dụng web mô phỏng các lỗ hổng bảo mật trong OWASP Top 10**

b. Một công cụ mã hóa

c. Một công cụ kiểm thử bảo mật mạng

d. Một hệ thống phòng thủ tấn công mạng

**Câu 21: Biện pháp nào giúp ngăn chặn SSRF?**

**a. Làm sạch và xác minh tất cả dữ liệu đầu vào của người dùng**

b. Sử dụng mật khẩu mặc định

c. Không ghi lại các sự kiện bảo mật

d. Chỉ cho phép truy cập từ các nguồn không tin cậy

**Câu 22: OWASP Cheat Sheets là gì?**

**a. Các tài liệu hướng dẫn về các biện pháp bảo mật quan trọng**

b. Danh sách các công cụ bảo mật phổ biến

c. Danh sách các ứng dụng bảo mật web

d. Danh sách các lỗ hổng bảo mật web

**Câu 23: Insecure Design trong OWASP Top 10 ám chỉ điều gì?**

**a. Thiết kế không đáp ứng các yêu cầu bảo mật**

b. Thiết kế giao diện không hợp lý

c. Sử dụng giao thức truyền dữ liệu không an toàn

d. Thiếu cơ chế ghi log bảo mật

**Câu 24: Ghép cặp các kiểu tấn công với hạng mục OWASP Top 10 tương ứng.**

**a. Path Traversal → Broken Access Control, SQL Injection → Injection, Unencrypted Data → Cryptographic Failures, Session Hijacking → Identification and Authentication Failures, Unpatched Software → Vulnerable and Outdated Components**

b. Path Traversal → Broken Access Control, SQL Injection → Injection, Encrypted Data → Cryptographic Failures, Session Hijacking → Identification and Authentication Failures, Unpatched Software → Vulnerable and Outdated Components

c. Path Traversal → Broken Access List, SQL Injection → Injection, Unencrypted Data → Cryptographic Failures, Session Hijacking → Identification and Authentication Failures, Unpatched Software → Vulnerable and Outdated Components

d. Path Traversal → Broken Access Control, SQL Scripts → Injection, Unencrypted Data → Cryptographic Failures, Session Hijacking → Identification and Authentication Failures, Unpatched Software → Vulnerable and Outdated Components

**Câu 25: Ghép cặp các kiểu tấn công bảo mật với biện pháp phòng ngừa.**

**a. CSRF → Sử dụng token CSRF để xác thực yêu cầu, Security Misconfiguration → Cập nhật cấu hình và bảo mật hệ thống thường xuyên, Broken Access Control → Giới hạn quyền truy cập tài nguyên dựa trên vai trò người dùng, XSS → Escape các ký tự đặc biệt trong đầu vào người dùng, SQL Injection → Sử dụng câu truy vấn có tham số hóa**

b. CSRF → Sử dụng token CSRF để xác thực yêu cầu, Security Misconfiguration → Cập nhật cấu hình và bảo mật hệ thống thường xuyên, Broken Access Control → Giới hạn quyền truy cập tài nguyên dựa trên vai trò người dùng, XSS → Escape các ký tự đặc biệt trong đầu vào người dùng, SQL Injection → Sử dụng câu truy vấn không có tham số hóa

c. CFRF → Sử dụng token CFRF để xác thực yêu cầu, Security Misconfiguration → Cập nhật cấu hình và bảo mật hệ thống thường xuyên, Broken Access Control → Giới hạn quyền truy cập tài nguyên dựa trên vai trò người dùng, XSS → Escape các ký tự đặc biệt trong đầu vào người dùng, SQL Injection → Sử dụng câu truy vấn có tham số hóa

d. CSRF → Sử dụng token CSRF để xác thực yêu cầu, Security Misconfiguration → Cập nhật cấu hình và bảo mật hệ thống thường xuyên, Broken Access Control → Giới hạn quyền truy cập tài nguyên dựa trên vai trò người dùng, XLSS → Escape các ký tự đặc biệt trong đầu vào người dùng, SQL Injection → Sử dụng câu truy vấn có tham số hóa

**Câu 26: Ghép cặp các nguyên tắc bảo mật OWASP với mô tả của chúng.**

**a. Integrity → Đảm bảo dữ liệu không bị thay đổi bởi các đối tượng không được phép, Confidentiality → Bảo vệ dữ liệu khỏi những truy cập trái phép, Authorization → Quyết định xem người dùng có quyền truy cập tài nguyên hay không, Availability → Đảm bảo hệ thống và dữ liệu luôn sẵn có khi cần thiết, Authentication → Xác thực danh tính của người dùng hoặc hệ thống**

b. Integrity → Đảm bảo dữ liệu không bị thay đổi bởi các đối tượng được phép, Confidentiality → Bảo vệ dữ liệu khỏi những truy cập trái phép, Authorization → Quyết định xem người dùng có quyền truy cập tài nguyên hay không, Availability → Đảm bảo hệ thống và dữ liệu luôn sẵn có khi cần thiết, Authentication → Xác thực danh tính của người dùng hoặc hệ thống

c. Integrity → Đảm bảo dữ liệu không bị thay đổi bởi các đối tượng không được phép, Confidentiality → Bảo vệ dữ liệu khỏi những truy cập trái phép, Authorization → Quyết định xem người dùng có quyền truy cập tài nguyên hay không, Availability → Đảm bảo hệ thống và dữ liệu luôn sẵn có khi không cần thiết, Authentication → Xác thực danh tính của người dùng hoặc hệ thống

d. Integrity → Đảm bảo dữ liệu không bị thay đổi bởi các đối tượng không được phép, Confidentiality → Bảo vệ dữ liệu khỏi những truy cập trái phép, Authentication → Quyết định xem người dùng có quyền truy cập tài nguyên hay không, Availability → Đảm bảo hệ thống và dữ liệu luôn sẵn có khi cần thiết, Authorization → Xác thực danh tính của người dùng hoặc hệ thống

**Câu 27: Software and Data Integrity Failures ám chỉ điều gì?**

**a. Rủi ro do không đảm bảo tính toàn vẹn của phần mềm và dữ liệu**

b. Rủi ro do quyền truy cập không đúng

c. Rủi ro do mã hóa yếu

d. Rủi ro do cấu hình sai hệ thống

**Câu 28: Ghép cặp các dự án OWASP với mục tiêu của chúng.**

**a. OWASP ZAP → Công cụ kiểm thử bảo mật ứng dụng web tự động, OWASP ASVS → Cung cấp các yêu cầu kiểm thử bảo mật ứng dụng, OWASP Top 10 → Xác định 10 rủi ro bảo mật phổ biến nhất cho ứng dụng web, OWASP Juice Shop → Mô phỏng các lỗ hổng bảo mật trong ứng dụng web, OWASP SAMM → Cung cấp mô hình để đánh giá và cải thiện an ninh phần mềm**

b. OWASP ASVS → Công cụ kiểm thử bảo mật ứng dụng web tự động, OWASP ZAP → Cung cấp các yêu cầu kiểm thử bảo mật ứng dụng, OWASP Top 10 → Xác định 10 rủi ro bảo mật phổ biến nhất cho ứng dụng web, OWASP Juice Shop → Mô phỏng các lỗ hổng bảo mật trong ứng dụng web, OWASP SAMM → Cung cấp mô hình để đánh giá và cải thiện an ninh phần mềm

c. OWASP ZAP → Công cụ kiểm thử bảo mật ứng dụng web tự động, OWASP ASVS → Cung cấp các yêu cầu kiểm thử bảo mật ứng dụng, OWASP Top 10 → Xác định 10 rủi ro bảo mật phổ biến nhất cho ứng dụng web, OWASP SAMM Juice Shop → Mô phỏng các lỗ hổng bảo mật trong ứng dụng web, OWASP Software→ Cung cấp mô hình để đánh giá và cải thiện an ninh phần mềm

d. OWASP ZAP 10→ Công cụ kiểm thử bảo mật ứng dụng web tự động dựa trên TOP 10 OWASP Mobile, OWASP ASVS → Cung cấp các yêu cầu kiểm thử bảo mật ứng dụng, OWASP Top 10 → Xác định 10 rủi ro bảo mật phổ biến nhất cho ứng dụng web, OWASP SAMM Juice Shop → Mô phỏng các lỗ hổng bảo mật trong ứng dụng web, OWASP Software→ Cung cấp mô hình để đánh giá và cải thiện an ninh phần mềm

**Câu 29: Biện pháp nào dưới đây không giúp giảm thiểu Cryptographic Failures?**

**a. Sử dụng các giao thức truyền tải dữ liệu không an toàn**

b. Phân loại dữ liệu nhạy cảm và mã hóa khi cần thiết

c. Không lưu trữ dữ liệu nhạy cảm khi không cần thiết

d. Sử dụng giao thức TLS để mã hóa dữ liệu

**Câu 30: OWASP là viết tắt của?**

**a. Open Web Application Security Project**

b. Open Wide Application Security Program

c. Open Web Application Security Platform

d. Online Web Application Secure Program

**Câu 31: Security Logging and Monitoring Failures là rủi ro gì?**

**a. Rủi ro do không ghi lại hoặc không giám sát các sự kiện bảo mật**

b. Rủi ro do cấu hình sai hệ thống

c. Rủi ro do tiêm mã độc hại vào hệ thống

d. Rủi ro do không mã hóa dữ liệu nhạy cảm

**Câu 32: Ví dụ nào dưới đây là ví dụ về Security Misconfiguration?**

**a. Ứng dụng cho phép liệt kê các thư mục trên hệ thống**

b. Ứng dụng sử dụng mật khẩu mặc định

c. Ứng dụng lưu trữ dữ liệu không mã hóa

d. Ứng dụng không ghi log các sự kiện bảo mật

**Câu 33: Ghép cặp các ví dụ với rủi ro bảo mật tương ứng.**

**a. Không kiểm tra đầu vào người dùng → Injection, Không cập nhật phần mềm → Vulnerable and Outdated Components, Sử dụng mật khẩu dễ đoán → Identification and Authentication Failures, Cho phép truy cập tệp tin quan trọng mà không có quyền → Broken Access Control, Không mã hóa dữ liệu nhạy cảm → Cryptographic Failures**

b. Không kiểm tra đầu vào người dùng → Injection, Không cập nhật phần mềm → Vulnerable and Outdated Components, Sử dụng mật khẩu dễ đoán → Cryptographic Failures, Cho phép truy cập tệp tin quan trọng mà không có quyền → Broken Access Control, Không mã hóa dữ liệu nhạy cảm → Identification and Authentication Failures

c. Không kiểm tra đầu vào người dùng → Injection, Không cập nhật phần mềm → Vulnerable and Outdated Components, Sử dụng mật khẩu dễ đoán → Identification and Authentication Failures, Cho phép truy cập tệp tin quan trọng mà không có quyền → Broken Role Control, Không mã hóa dữ liệu nhạy cảm → Cryptographic Failures

d. Không kiểm tra đầu vào người dùng → Injection, Luôn cập nhật phần mềm → Vulnerable and Outdated Components, Sử dụng mật khẩu dễ đoán → Identification and Authentication Failures, Cho phép truy cập tệp tin quan trọng mà không có quyền → Broken Access Control, Không mã hóa dữ liệu nhạy cảm → Cryptographic Failures

**Câu 34: Biện pháp nào không giúp ngăn chặn Security Misconfiguration?**

**a. Cho phép bật các tính năng không cần thiết**

b. Gỡ bỏ các tính năng và thành phần không cần thiết

c. Cập nhật phần mềm và bản vá kịp thời

d. Xem xét cấu hình và bảo mật hệ thống thường xuyên

**Câu 35: Ghép cặp các cấu hình bảo mật sai với hậu quả của chúng.**

**a. Sử dụng mật khẩu mặc định → Nguy cơ bị tấn công bởi mật khẩu dễ đoán, Không cập nhật phần mềm → Hệ thống dễ bị tấn công bởi các lỗ hổng đã biết, Không ghi log sự kiện bảo mật → Không thể phát hiện tấn công hoặc sự cố kịp thời, Bật các tính năng không cần thiết → Lỗ hổng dễ bị khai thác do các tính năng không sử dụng, Cấu hình sai quyền truy cập → Truy cập không được phép vào tài nguyên nhạy cảm**

b. Sử dụng mật khẩu rất mạnh→ Nguy cơ bị tấn công bởi mật khẩu dễ đoán, Không cập nhật phần mềm → Hệ thống dễ bị tấn công bởi các lỗ hổng đã biết, Không ghi log sự kiện bảo mật → Không thể phát hiện tấn công hoặc sự cố kịp thời, Bật các tính năng không cần thiết → Lỗ hổng dễ bị khai thác do các tính năng không sử dụng, Cấu hình sai quyền truy cập → Truy cập không được phép vào tài nguyên nhạy cảm

c. Sử dụng mật khẩu mặc định → Nguy cơ bị tấn công bởi mật khẩu dễ đoán, Không cập nhật phần mềm → Hệ thống dễ bị tấn công bởi các lỗ hổng đã biết, Không ghi log sự kiện bảo mật → Không thể phát hiện tấn công hoặc sự cố kịp thời, Bật các tính năng không cần thiết → Lỗ hổng dễ bị khai thác do các tính năng không sử dụng, Cấu hình đúng quyền truy cập → Truy cập không được phép vào tài nguyên nhạy cảm

d. Sử dụng mật khẩu mặc định → Nguy cơ bị tấn công bởi mật khẩu dễ đoán, Luôn cập nhật phần mềm → Hệ thống dễ bị tấn công bởi các lỗ hổng đã biết, Không ghi log sự kiện bảo mật → Không thể phát hiện tấn công hoặc sự cố kịp thời, Bật các tính năng không cần thiết → Lỗ hổng dễ bị khai thác do các tính năng không sử dụng, Cấu hình sai quyền truy cập → Truy cập không được phép vào tài nguyên nhạy cảm

**Câu 36: Ghép cặp các lỗ hổng bảo mật với các biện pháp phòng ngừa của chúng.**

**a. Vulnerable and Outdated Components → Cập nhật phần mềm và các thành phần thường xuyên, Broken Access Control → Giới hạn truy cập mặc định, chỉ cho phép quyền cần thiết, Cryptographic Failures → Mã hóa dữ liệu nhạy cảm khi lưu trữ và truyền tải, Security Misconfiguration → Loại bỏ các tính năng không cần thiết và cập nhật hệ thống thường xuyên, Injection → Kiểm tra và xác thực tất cả dữ liệu đầu vào người dùng**

b. Vulnerable and Outdated Components → Cập nhật phần mềm và các thành phần thường xuyên, Broken Access Control → Giới hạn truy cập mặc định, chỉ cho phép quyền cần thiết, Cryptographic Failures → Không cần mã hóa dữ liệu nhạy cảm khi lưu trữ và truyền tải, Security Misconfiguration → Loại bỏ các tính năng không cần thiết và cập nhật hệ thống thường xuyên, Injection → Kiểm tra và xác thực tất cả dữ liệu đầu vào người dùng

c. Vulnerable and Outdated Components → Cập nhật phần mềm và các thành phần thường xuyên, Broken Access Control → Giới hạn truy cập mặc định, chỉ cho phép quyền cần thiết, Cryptographic Failures → Mã hóa dữ liệu nhạy cảm khi lưu trữ và truyền tải, Security Misconfiguration → Loại bỏ các tính năng không cần thiết và cập nhật hệ thống thường xuyên, Injection → Không cần kiểm tra và xác thực tất cả dữ liệu đầu vào người dùng

d. Vulnerable and Outdated System → Cập nhật phần mềm và các thành phần thường xuyên, Broken Access Control → Giới hạn truy cập mặc định, chỉ cho phép quyền cần thiết, Cryptographic Failures → Mã hóa dữ liệu nhạy cảm khi lưu trữ và truyền tải, Security Misconfiguration → Loại bỏ các tính năng không cần thiết và cập nhật hệ thống thường xuyên, Injection → Kiểm tra và xác thực tất cả dữ liệu đầu vào người dùng

**Câu 37: Biện pháp nào sau đây giúp ngăn chặn Insecure Design?**

**a. Sử dụng vòng đời phát triển an toàn (secure development lifecycle)**

b. Sử dụng mật khẩu mặc định

c. Chỉ mã hóa dữ liệu khi được yêu cầu

d. Ghi log tất cả các sự kiện bảo mật

**Câu 38: Security Misconfiguration là?**

**a. Việc cấu hình sai hệ thống dẫn đến lỗ hổng bảo mật**

b. Việc sử dụng thuật toán mã hóa yếu

c. Việc tiêm mã độc hại vào hệ thống

d. Việc không ghi log sự kiện bảo mật

**Câu 39: Biện pháp nào giúp ngăn chặn Vulnerable and Outdated Components?**

**a. Cập nhật phần mềm và thành phần hệ thống thường xuyên**

b. Chỉ sử dụng các thành phần mã nguồn mở

c. Không sử dụng mã hóa cho dữ liệu nhạy cảm

d. Cho phép truy cập không giới hạn

**Câu 40: Rủi ro Vulnerable and Outdated Components ám chỉ điều gì?**

**a. Việc sử dụng các thành phần phần mềm lỗi thời và có lỗ hổng bảo mật**

b. Việc tiêm mã độc vào hệ thống

c. Việc không ghi log các sự kiện bảo mật

d. Việc cấu hình sai hệ thống

**Câu 41: Injection xảy ra khi?**

**a. Ứng dụng chấp nhận dữ liệu đầu vào mà không kiểm tra đúng cách**

b. Người dùng cố tình thay đổi mật khẩu

c. Dữ liệu được truyền đi dưới dạng cleartext

d. Ứng dụng ghi log sai

**Câu 42: Biện pháp nào giúp ngăn chặn rủi ro Identification and Authentication Failures?**

**a. Sử dụng xác thực nhiều yếu tố (multi-factor authentication)**

b. Không yêu cầu mật khẩu khi đăng nhập

c. Sử dụng mật khẩu mặc định

d. Chỉ mã hóa dữ liệu không nhạy cảm

**Câu 43: Ghép cặp các lỗ hổng bảo mật trong OWASP Top 10 với mô tả của chúng.**

**a. Security Misconfiguration → Hệ thống cấu hình sai dẫn đến lỗ hổng bảo mật, Injection → Chèn mã độc hại vào hệ thống qua đầu vào không được kiểm tra, Cryptographic Failures → Lỗi liên quan đến việc sử dụng mã hóa yếu hoặc không đúng cách, Identification and Authentication Failures → Xác thực và định danh người dùng không chính xác, Broken Access Control → Truy cập trái phép do kiểm soát truy cập không đúng cách**

b. Security Misconfiguration → Hệ thống cấu hình đúng dẫn đến lỗ hổng bảo mật, Injection → Chèn mã độc hại vào hệ thống qua đầu vào không được kiểm tra, Cryptographic Failures → Lỗi liên quan đến việc sử dụng mã hóa yếu hoặc không đúng cách, Identification and Authentication Failures → Xác thực và định danh người dùng không chính xác, Broken Access Control → Truy cập trái phép do kiểm soát truy cập không đúng cách

c. Security Misconfiguration → Hệ thống cấu hình sai dẫn đến lỗ hổng bảo mật, Injection → Chèn mã độc hại vào hệ thống qua đầu vào không được kiểm tra, Cryptographic Failures → Lỗi liên quan đến việc sử dụng mã hóa mạnh hoặc đúng cách, Identification and Authentication Failures → Xác thực và định danh người dùng không chính xác, Broken Access Control → Truy cập trái phép do kiểm soát truy cập không đúng cách

d. Security Misconfiguration → Hệ thống cấu hình sai dẫn đến lỗ hổng bảo mật, Injection → Chèn mã độc hại vào hệ thống qua đầu vào không được kiểm tra, Cryptographic Failures → Lỗi liên quan đến việc sử dụng mã hóa yếu hoặc không đúng cách, Identification and Authentication Failures → Xác thực và định danh người dùng không chính xác, Broken Access Control → Truy cập trái phép do kiểm soát truy cập đúng cách

**Câu 44: Biện pháp nào không phải là cách ngăn chặn Broken Access Control?**

**a. Sử dụng mã hóa yếu để giảm tải cho hệ thống**

b. Ghi log và cảnh báo người quản trị khi cần thiết

c. Giới hạn tốc độ truy cập API để ngăn chặn tấn công tự động

d. Chặn truy cập mặc định và chỉ cho phép những tài nguyên công cộng

**Câu 45: Yếu tố nào dưới đây không nằm trong danh sách OWASP Top 10?**

**a. Cross-Site Request Forgery (CSRF)**

b. Security Misconfiguration

c. Broken Access Control