**ÔN TẬP**

**TUẦN 10 - ANDROID SECURITY**

**Câu 1: Ghép các kỹ thuật kiểm thử ứng dụng Android với công cụ phù hợp:**

**a. Static Analysis → SonarQube, Fuzzy Testing → OWASP ZAP, Dynamic Analysis → Burp Suite**

b. Static Analysis → OWASP ZAP, Fuzzy Testing → SonarQube, Dynamic Analysis → Burp Suite

c. Static Analysis → Burp Suite, Fuzzy Testing → OWASP ZAP, Dynamic Analysis → SonarQube

**Câu 2: Ghép các thuật ngữ bảo mật với định nghĩa phù hợp:**

**a. Static Analysis → Phân tích mã nguồn mà không thực thi, Dynamic Analysis → Kiểm tra hành vi ứng dụng trong runtime, Penetration Testing → Xác định và khai thác lỗ hổng bảo mật**

b. Static Analysis → Phân tích mã nguồn được thực thi, Dynamic Analysis → Kiểm tra hành vi ứng dụng trong runtime, Penetration Testing → Xác định và khai thác lỗ hổng bảo mật

c. Static Analysis → Phân tích mã nguồn mà không thực thi, Dynamic Checking → Kiểm tra hành vi ứng dụng trong runtime, Penetration Testing → Xác định và khai thác lỗ hổng bảo mật

**Câu 3: Certificate Pinning đảm bảo điều gì?**

**a. Ứng dụng chỉ kết nối với máy chủ đáng tin cậy**

b. Chặn các kết nối mạng không mã hóa

c. Mã hóa dữ liệu người dùng trên thiết bị

d. Kiểm tra cấu trúc giao diện

**Câu 4: Ghép các kỹ thuật kiểm thử ứng dụng với mục đích tương ứng:**

**a. Penetration Testing → Xác định và khai thác lỗ hổng bảo mật, Dynamic Analysis → Kiểm thử ứng dụng trong runtime, Fuzzy Testing → Đưa dữ liệu không hợp lệ hoặc ngẫu nhiên để kiểm thử**

b. Penetration Testing → Xác định và khai thác lỗ hổng bảo mật, Dynamic Analysis → Kiểm thử ứng dụng trong runtime, Fuzzy Testing → Đưa dữ liệu không hợp lệ hoặc ngẫu nhiên để kiểm thử hợp đồng thông minh

c. Fuzzy Testing → Xác định và khai thác lỗ hổng bảo mật, Dynamic Analysis → Kiểm thử ứng dụng trong runtime, Penetration Testing → Đưa dữ liệu không hợp lệ hoặc ngẫu nhiên để kiểm thử

**Câu 5: Mục tiêu chính của Penetration Testing trên ứng dụng di động là gì?**

**a. Xác định và khai thác các lỗ hổng bảo mật**

b. Tăng tốc độ xử lý của ứng dụng

c. Quản lý tài nguyên mạng

d. Mã hóa toàn bộ dữ liệu ứng dụng

**Câu 6: Fuzzy Testing là gì?**

**a. Kỹ thuật kiểm thử bằng cách đưa dữ liệu không hợp lệ hoặc ngẫu nhiên vào hệ thống**

b. Phương pháp mã hóa dữ liệu

c. Công cụ phát hiện phần mềm độc hại

d. Cách kiểm tra xác thực 2 yếu tố

**Câu 7: Ghép các lỗ hổng bảo mật với công cụ kiểm tra tương ứng:**

**a. SQL Injection → Burp Suite, Buffer Overflow → Fuzzy Testing, Reverse Engineering → JADX**

b. SQL Injection → Fuzzy Testing, Buffer Overflow → Burp Suite, Reverse Engineering → JADX

c. SQL Injection → JADX, Buffer Overflow → Fuzzy Testing, Reverse Engineering → Burp Suite

**Câu 8: Kỹ thuật nào thường được sử dụng để thực hiện reverse engineering trên ứng dụng Android?**

**a. Dịch ngược mã bytecode bằng công cụ như JADX**

b. Phân tích giao diện người dùng

c. Mã hóa dữ liệu người dùng

d. Chặn lưu lượng mạng

**Câu 9: Mục tiêu chính của Security Testing là gì?**

**a. Phát hiện và giảm thiểu các lỗ hổng bảo mật**

b. Đảm bảo giao diện người dùng trực quan

c. Tăng tốc độ xử lý của ứng dụng

d. Lưu trữ dữ liệu không mã hóa

**Câu 10: Làm thế nào để phát hiện lỗ hổng Buffer Overflow trong ứng dụng di động?**

**a. Kiểm tra dữ liệu đầu vào và giới hạn kích thước bộ nhớ**

b. Mã hóa dữ liệu truyền qua mạng

c. Sử dụng các thuật toán hash

d. Phân tích mã nguồn bằng SonarQube

**Câu 11: Nguyên nhân chính của Insecure Data Storage là gì?**

**a. Lưu trữ dữ liệu không an toàn hoặc không bảo vệ đúng cách**

b. Sử dụng thuật toán mã hóa lỗi thời

c. Không xác thực người dùng

d. Không xác minh hostname trong giao thức SSL/TLS

**Câu 12: Ghép các kỹ thuật mã hóa trong Android với mục đích tương ứng:**

**a. RSA → Mã hóa bất đối xứng, SHA-256 → Kỹ thuật Hash, AES → Mã hóa đối xứng**

b. RSA → Mã hóa đối xứng, ABE → Kỹ thuật Hash, AES → Mã hóa bất đối xứng

c. RSA → Mã hóa bất đối xứng, BcryptWithSHA512 → Kỹ thuật Encdoe, AES → Mã hóa đối xứng

**Câu 13: Lỗ hổng M10 liên quan đến điều gì? (TOP OWASP Mobile 10 – 2016)**

**a. Các chức năng ẩn hoặc không cần thiết trong mã nguồn**

b. Quản lý quyền không đúng cách

c. Không mã hóa dữ liệu nhạy cảm

d. Lỗi trong giao tiếp mạng

**Câu 14: HostnameVerifier có chức năng gì trong bảo mật SSL/TLS?**

**a. So khớp hostname của server với chứng chỉ được cung cấp**

b. Mã hóa dữ liệu trên máy chủ

c. Tăng tốc độ kết nối

d. Lưu trữ dữ liệu truyền qua mạng

**Câu 15: Phương pháp nào hiệu quả hơn trong kiểm tra dữ liệu đầu vào?**

**a. Accept-Known-Good**

b. Reject-Known-Bad

c. Mã hóa dữ liệu đầu vào

d. Xác thực hostname

**Câu 16: Biện pháp nào hiệu quả nhất để bảo vệ ứng dụng khỏi Command Injection?**

**a. Xác thực và kiểm tra dữ liệu đầu vào**

b. Mã hóa toàn bộ dữ liệu người dùng

c. Tăng quyền truy cập của người dùng

d. Sử dụng thuật toán hash

**Câu 17: Salt được sử dụng trong mã hóa có tác dụng gì?**

**a. Tăng độ khó của việc tìm ra khóa**

b. Mã hóa toàn bộ dữ liệu

c. Lưu trữ thông tin người dùng

d. Xác thực máy chủ

**Câu 18: Ghép các thành phần của SSL/TLS trong Android với chức năng tương ứng:**

**a. HttpsURLConnection → Tạo kết nối HTTPS đến server, SSLContext → Thiết lập cấu hình SSL/TLS, HostnameVerifier → Xác minh hostname của server**

b. HttpsURLConnection → Tạo kết nối HTTP đến server, SSLContext → Thiết lập cấu hình SSL/TLS, HostnameVerifier → Xác minh hostname của server

c. HttpsURLConnection → Tạo kết nối HTTPS đến server, SSLContext → Thiết lập cấu hình SSL/TLS, HostnameVerifier → Xác minh hostname của client

**Câu 19: M1: Improper Platform Usage đề cập đến vấn đề gì?**

**a. Sử dụng không đúng các cơ chế kiểm soát bảo mật nền tảng**

b. Truyền dữ liệu không an toàn

c. Phân quyền không hợp lý

d. Dữ liệu lưu trữ không được mã hóa

**Câu 20: Biện pháp nào sau đây giúp phát hiện việc sửa đổi mã nguồn (Code Tampering)?**

**a. Kiểm tra tính toàn vẹn của ứng dụng bằng checksum**

**b.** Mã hóa dữ liệu người dùng

c. Chặn các kết nối không an toàn

d. Sử dụng static analysis

**Câu 21: Thách thức chính khi thực hiện Dynamic Analysis là gì?**

**a. Ứng dụng có thể phát hiện môi trường giả lập**

b. Dữ liệu không được mã hóa

c. Mã nguồn không có lỗi

d. Tăng kích thước của ứng dụng

**Câu 22: M3: Insecure Communication xảy ra khi nào?**

**a. Khi giao tiếp dữ liệu không được mã hóa hoặc xác thực**

b. Khi dữ liệu bị rò rỉ trong quá trình lưu trữ

c. Khi mã nguồn chứa backdoor

d. Khi có lỗi trong quản lý phiên đăng nhập

**Câu 23: Tại sao self-signed certificate được sử dụng với server riêng tư?**

**a. Không cần chứng chỉ từ CA thương mại**

b. Dữ liệu được mã hóa mạnh hơn

c. Giảm chi phí vận hành

d. Hỗ trợ nhiều client đồng thời

**Câu 24: Biện pháp nào giúp phát hiện lỗ hổng Command Injection?**

**a. Sử dụng dữ liệu đầu vào độc hại để kiểm tra phản hồi**

b. Mã hóa toàn bộ dữ liệu người dùng

c. Phân tích mã nguồn ứng dụng

d. Xác minh hostname của máy chủ

**Câu 25: M5: Insufficient Cryptography liên quan đến điều gì?**

**a. Sử dụng thuật toán mã hóa yếu hoặc lỗi thời**

b. Dữ liệu lưu trữ không được bảo vệ

c. Lạm dụng quyền trên thiết bị

d. Không có sự kiểm tra xác thực trong giao tiếp mạng

**Câu 26: Lỗi M6: Insecure Authorization thường liên quan đến?**

**a. Phân quyền sai hoặc không phân quyền**

b. Dữ liệu truyền qua mạng không được mã hóa

c. Lỗ hổng quản lý phiên đăng nhập

d. Không thực hiện mã hóa dữ liệu đầu cuối

**Câu 27: Lỗ hổng M4 có thể được khai thác như thế nào?**

**a. Bằng cách brute force mã xác thực 2 yếu tố (2FA)**

b. Bằng cách khai thác dữ liệu cleartext trong giao tiếp

c. Bằng cách vượt qua sandbox ứng dụng

d. Bằng cách phân tích mã binary của ứng dụng

**Câu 28: OWASP Mobile Top 10 là gì?**

**a. Một danh sách các lỗ hổng bảo mật phổ biến trên ứng dụng di động**

b. Hướng dẫn phát triển giao diện người dùng

c. Một công cụ kiểm thử ứng dụng

d. Danh sách các công cụ mã hóa phổ biến

**Câu 29: Ghép các lỗ hổng OWASP Mobile Top 10 với mô tả tương ứng:**

**a. M1: Improper Platform Usage → Lạm dụng các cơ chế bảo mật nền tảng, M3: Insecure Communication → Truyền dữ liệu không được mã hóa, M4: Insecure Authentication → Lỗi trong xác thực người dùng và quản lý phiên, M2: Insecure Data Storage → Dữ liệu lưu trữ không an toàn**

b. M2: Improper Platform Usage → Lạm dụng các cơ chế bảo mật nền tảng, M3: Insecure Communication → Truyền dữ liệu không được mã hóa, M4: Insecure Authentication → Lỗi trong xác thực người dùng và quản lý phiên, M1: Insecure Data Storage → Dữ liệu lưu trữ không an toàn

c. M1: Improper Platform Usage → Lạm dụng các cơ chế bảo mật nền tảng, M4: Insecure Communication → Truyền dữ liệu không được mã hóa, M3: Insecure Authentication → Lỗi trong xác thực người dùng và quản lý phiên, M2: Insecure Data Storage → Dữ liệu lưu trữ không an toàn

**Câu 30: SSL/TLS Configuration giúp bảo vệ điều gì trong ứng dụng?**

**a. Dữ liệu truyền qua mạng**

b. Dữ liệu lưu trữ trên thiết bị

c. Cấu trúc giao diện người dùng

d. Tài nguyên bộ nhớ