

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC MỎ - ĐỊA CHẤT
BỘ MÔN MẠNG MÁY TÍNH
=====:

BÁO CÁO HỌC THUẬT

TÌM HIỂU VỀ KIỂM THỬ BẢO MẬT

Người thực hiện: ThS. Đỗ Như Hải

Đơn vị: Bộ môn Mạng máy tính

Hà Nội - 12/2025

MỤC LỤC

Contents

MỤC LỤC	2
A. TÓM TẮT BÁO CÁO	3
B . NỘI DUNG BÁO CÁO.....	4
1. Giới thiệu	4
2. Phân loại các công cụ kiểm thử Security	6
3. Xây dựng một checklist kiểm thử bảo mật	12

A. TÓM TẮT BÁO CÁO

Tên báo cáo: Tìm hiểu về kiểm thử bảo mật

Trong bối cảnh công nghệ thông tin phát triển mạnh mẽ và các hệ thống phần mềm ngày càng đóng vai trò quan trọng trong mọi lĩnh vực, vấn đề bảo mật thông tin trở thành mối quan tâm hàng đầu. Các lỗ hổng bảo mật có thể gây ra những hậu quả nghiêm trọng như rò rỉ dữ liệu, gián đoạn dịch vụ hoặc thiệt hại về kinh tế và uy tín. Vì vậy, kiểm thử bảo mật được xem là một hoạt động thiết yếu nhằm phát hiện, đánh giá và khắc phục các điểm yếu trong hệ thống trước khi chúng bị khai thác. Báo cáo này tập trung tìm hiểu về kiểm thử bảo mật, bao gồm khái niệm, mục tiêu, vai trò cũng như tầm quan trọng của kiểm thử bảo mật trong quá trình phát triển và vận hành hệ thống công nghệ thông tin.

Mục tiêu của báo cáo: Trình bày về kiểm thử bảo mật, các loại chính, các công cụ phổ biến và đưa ra checklist kiểm thử bảo mật cho một tổ chức hoặc doanh nghiệp.

B . NỘI DUNG BÁO CÁO

1. Giới thiệu

Kiểm thử bảo mật giúp phát hiện và đánh giá lỗ hổng bảo mật trong hệ thống và ứng dụng. Nó có vai trò quan trọng và then chốt trong việc bảo vệ tài sản và uy tín của doanh nghiệp. Kiểm thử bảo mật nhằm bảo vệ dữ liệu và hệ thống khỏi bị tấn công, đảm bảo tuân thủ các quy định pháp lý, tăng cường uy tín của tổ chức và tạo niềm tin cho khách hàng, giảm thiểu thiệt hại tài chính, phát hiện và khắc phục lỗ hổng sớm.



Xét về quy trình kiểm thử bảo mật bao gồm các bước:

Xác định phạm vi kiểm thử.

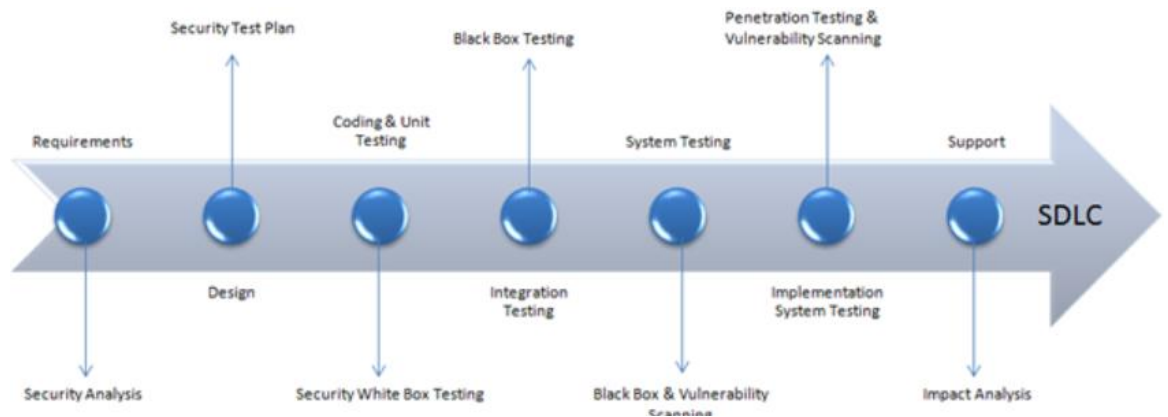
Thu thập thông tin.

Xác định lỗ hổng.

Phân tích rủi ro.

Khắc phục và kiểm tra lại.

Báo cáo kết quả kiểm thử.



Xét về phương pháp sẽ có ba phương pháp kiểm thử chính là:

Kiểm thử hộp đen.

Là phương pháp kiểm tra hệ thống tập trung vào chức năng, đầu vào và đầu ra mà không cần biết cấu trúc hay logic bên trong, giống như người dùng cuối tương tác với một "hộp đen". Tester chỉ quan tâm đến việc liệu hệ thống có hoạt động đúng theo yêu cầu hay không (Input -> Output).

Kiểm thử hộp trắng.

Là phương pháp kiểm tra hệ thống tập trung vào cấu trúc, logic và mã nguồn bên trong, cho phép người kiểm thử "nhìn xuyên qua" để xác minh các đường dẫn, câu lệnh, điều kiện và luồng dữ liệu hoạt động đúng như thiết kế, nhằm tìm ra lỗi logic, lỗ hổng bảo mật và tối ưu hóa mã, thường được thực hiện bởi lập trình viên ở cấp độ đơn vị.

Kiểm thử hộp xám.

Là kỹ thuật kết hợp giữa kiểm thử hộp đen (không biết nội bộ) và hộp trắng (biết toàn bộ nội bộ), trong đó người kiểm thử có **một phần kiến thức** về cấu trúc bên trong hệ thống (như luồng dữ liệu, kiến trúc, hoặc một phần mã nguồn) để thiết kế các trường hợp kiểm thử hiệu quả hơn, nhắm mục tiêu vào các lỗi logic, lỗ hổng bảo mật và sự cố chức năng mà không cần hiểu sâu như hộp trắng, đồng thời mang lại góc nhìn từ người dùng cuối như hộp đen.

Có nhiều loại kiểm thử bảo mật - từ xác thực, ứng dụng web, hạ tầng (infrastructure), đến xâm nhập (penetration), ủy quyền. Một số công cụ phổ biến nhất thường dùng trong quá trình này như: Burp Suite, OWASP ZAP, Nmap, Wireshark, Nessus, Nikto, OpenVAS...

Ngoài ra, theo một cách phân chia khác, có 3 kỹ thuật chính trong vấn đề này, bao gồm:

- **Vulnerability Scanning** (quét lỗ hổng)

Quét hệ thống hoặc ứng dụng để xác định các lỗ hổng bảo mật có thể bị khai thác (ví dụ: phần mềm lỗi, cài đặt không an toàn, cấu hình sai sót...). Kết quả sẽ cung cấp danh sách lỗ hổng để người dùng thực hiện biện pháp bảo mật.

- **Security Scanning** (quét bảo mật)

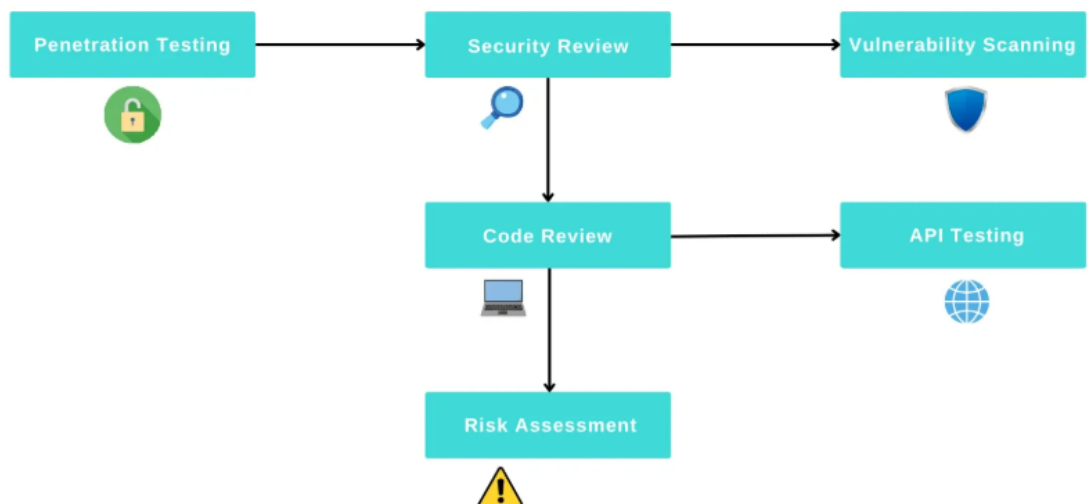
Kiểm tra toàn diện hệ thống hoặc ứng dụng để phát hiện lỗ hổng bảo mật và các thiếu sót trong cấu hình. Quá trình này thường dùng công cụ quét tự động để kiểm tra các cổng mạng, dịch vụ, hệ điều hành, ứng dụng, nhằm phát hiện mọi điểm yếu có thể bị khai thác. Kết quả đem lại thông tin chi tiết về các lỗ hổng bảo mật và khuyến nghị cải thiện.

- **Penetration Testing** (kiểm thử xâm nhập)

Là kiểm thử mạnh hơn: chuyên gia bảo mật giả lập tấn công thực sự vào hệ thống hoặc ứng dụng để tìm lỗ hổng bảo mật. Mục tiêu là khai thác các lỗ hổng để đánh giá khả năng chống lại các cuộc tấn công từ hacker. Và kết quả cung cấp thông tin chi tiết về lỗ hổng đã khai thác và khuyến nghị biện pháp khắc phục.

PenTest cũng giúp kiểm tra xem lỗ hổng có thật sự có thể khai thác được không, hệ thống phản ứng ra sao, và liệu logic bảo mật có đúng không.

Sơ Đồ Quy Trình Kiểm Thử Bảo Mật



2. Phân loại các công cụ kiểm thử Security

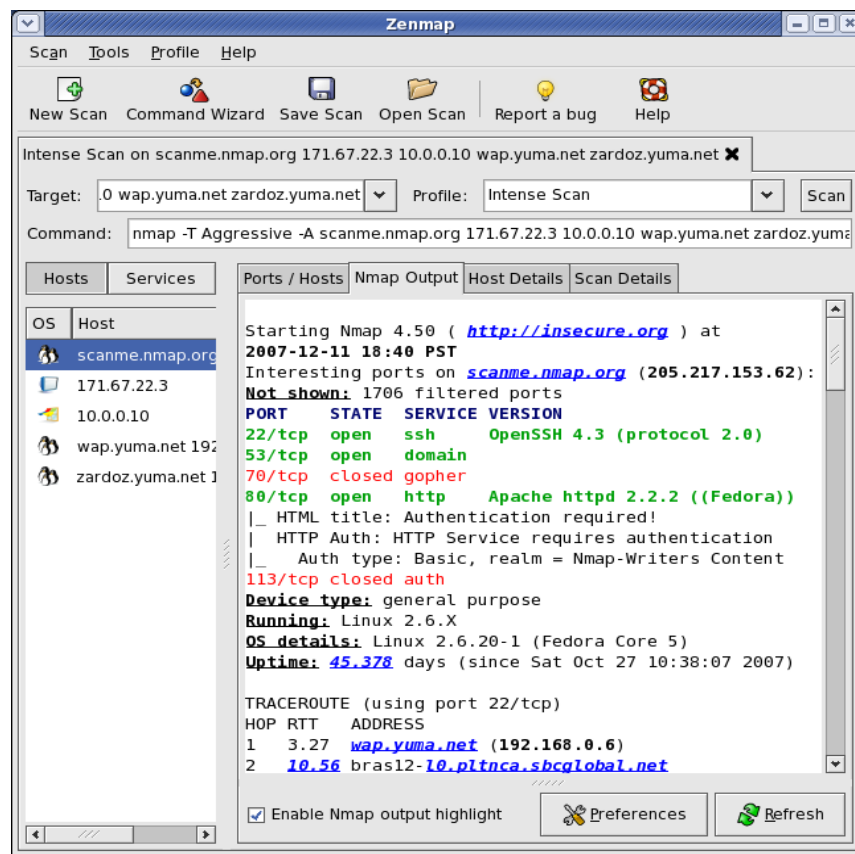
Có thể phân chia các công cụ kiểm thử bảo mật thành các nhóm sau:

2.1 Công cụ quét lỗ hổng (Vulnerability Scanning Tools)

Nhóm này có nhiều công cụ thông dụng như: Nmap, Nessus, OpenVAS, Qualys, Retina, Nexpose...

- Nmap:

Là công cụ quét mạng và phân tích máy chủ mạnh. Có thể quét cổng mạng mở, xác định các dịch vụ đang chạy, máy chủ/thiết bị trong mạng - hữu ích để khám phá bề mặt tấn công. Nmap hỗ trợ tùy chỉnh quét linh hoạt: nhiều lựa chọn quét, xác định mục tiêu chi tiết.



- Nessus

Là công cụ quét lỗ hổng mạnh và phổ biến. Có khả năng quét và phát hiện lỗ hổng bảo mật trong hệ thống, ứng dụng, mạng. Nessus tự động quét, phát hiện lỗ hổng, cung cấp báo cáo chi tiết (mô tả, cấp độ nghiêm trọng, khuyến nghị khắc phục).

- OpenVAS

Là công cụ quét lỗ hổng mã nguồn mở. Hỗ trợ quét mạng & ứng dụng để phát hiện lỗ hổng bảo mật. Nó cho phép quản lý cấu hình quét linh hoạt (quy tắc, tần suất, phạm vi); tạo báo cáo đa dạng về lỗ hổng (với mức độ nghiêm trọng & khuyến nghị).

2.2 Công cụ kiểm tra bảo mật ứng dụng (Application Security Testing Tools)

Tập trung kiểm tra bảo mật các ứng dụng web và di động: kiểm tra mã nguồn, xác thực, ủy quyền, lỗ hổng ứng dụng.

Kiểm tra các vấn đề như:

Broken Object Level Authorization (BOLA)

Rate limit bypass

Token / JWT

API endpoint enumeration

Các công cụ thường dùng ở nhóm này: OWASP ZAP, Burp Suite, Acunetix, Veracode, AppScan, Postman, Insomnia, K6 (stress test API), JWT.io debugger ...

- Burp Suite

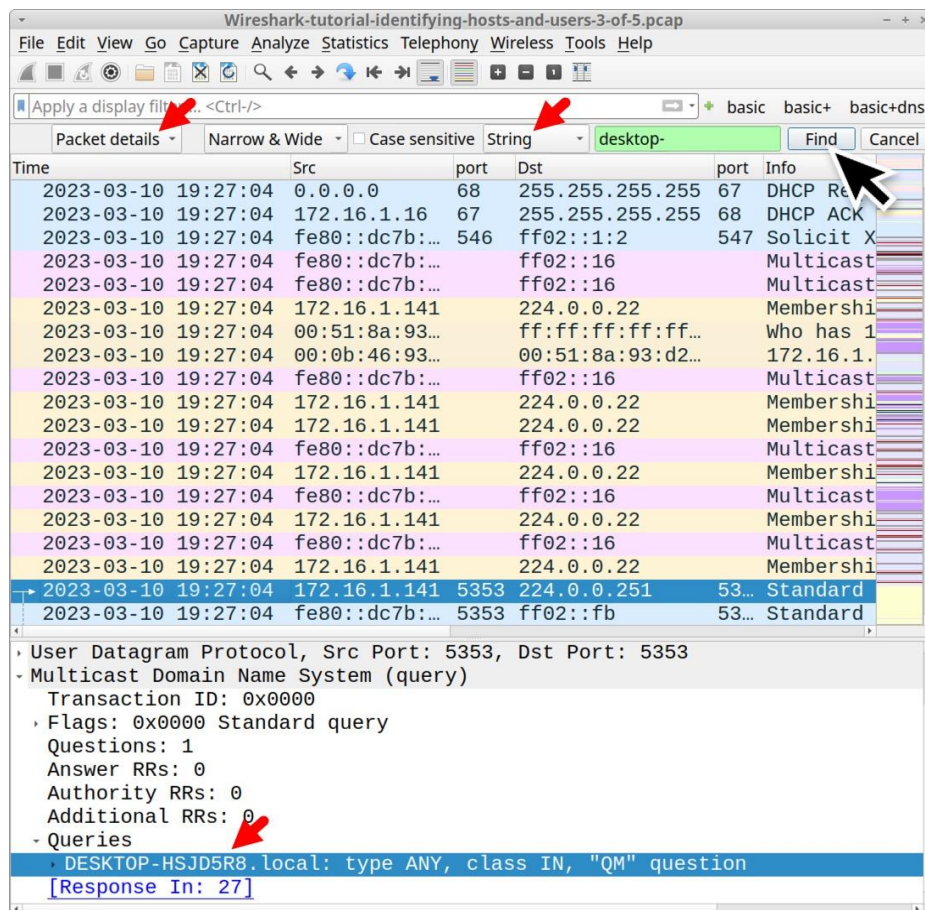
Là bộ công cụ kiểm thử bảo mật ứng dụng web mạnh, bao gồm các thành phần như Proxy, Scanner, Intruder, Repeater, Decoder - hỗ trợ phân tích & khai thác lỗ hổng web. Burp Suite có thể phát hiện lỗ hổng như XSS, SQL injection, tràn buffer, và các tấn công khác; cho phép sửa đổi request/response để thử kịch bản tấn công; hỗ trợ quản lý phiên làm việc.

2.3 Công cụ kiểm thử xâm nhập (Penetration Testing Tools)

Dùng để thực hiện các cuộc tấn công mô phỏng nhằm khai thác lỗ hổng bảo mật. Ví dụ: Metasploit, Nmap, Wireshark, Aircrack-ng, John the Ripper.

- Wireshark

Là công cụ phân tích gói tin mạng mạnh, giúp theo dõi, phân tích lưu lượng mạng, phát hiện hoạt động đáng ngờ, tấn công mạng, lỗ hổng mạng. Wireshark hỗ trợ nhiều giao thức mạng, có khả năng lọc dữ liệu để tìm và hiển thị các gói tin quan trọng.



2.4 Công cụ phân tích mã độc (Malware Analysis Tools)

Dùng để phân tích mã độc, phát hiện hành vi độc hại, nghiên cứu cách thức hoạt động. Chia làm hai loại:

Static analysis: phân tích mã mà không chạy

Dynamic analysis: chạy trong sandbox và theo dõi hành vi

Các công cụ thông dụng: IDA Pro, OllyDbg, Cuckoo Sandbox, VirusTotal.

2.5 Công cụ mã hóa và quản lý khóa (Encryption and Key Management Tools)

Nhóm này cung cấp giải pháp mã hóa dữ liệu và quản lý khóa để bảo vệ dữ liệu khi truyền và lưu trữ. Ví dụ: OpenSSL, VeraCrypt, Keyczar, AWS Key Management Service.

Tóm lại, kiểm thử bảo mật và các công cụ đi kèm đóng vai trò rất quan trọng để đảm bảo an toàn cho hệ thống và ứng dụng hiện đại. Tuy nhiên

ngoài công cụ, cần hiểu rõ phương pháp kiểm thử và có kỹ năng phân tích kết quả - chỉ dùng công cụ thôi là chưa đủ để đảm bảo an toàn toàn diện.

2.6 Web Application Security Testing

Nội dung tuân theo chuẩn **OWASP Web Security Testing Guide (WSTG)**.

Kiểm tra các thành phần sau:

- XSS
- SQLi
- CSRF
- SSRF
- IDOR
- Broken Access Control
- Authentication/Authorization flaws

Các công cụ phổ biến:

- Burp Suite
- OWASP ZAP
- Acunetix
- Netsparker / Invicti

2.7 Mobile Security Testing

Theo chuẩn **OWASP Mobile Testing Guide (MSTG)**.

Kiểm tra các thành phần sau:

- Secure storage
- Traffic encryption
- Reverse engineering
- Jailbreak/root bypass
- API communication

Các công cụ phổ biến thường dùng:

- MobSF
- Frida
- Objection
- APKTool
- Android Studio & Xcode tools

2.8 Network Security Testing

Kiểm tra các thành phần sau:

- Port scanning
- Firewall rules
- VLAN / segmentation
- Detection of sniffing, spoofing
- Protocol security

Các công cụ phổ biến thường dùng:

- Nmap
- Wireshark
- Ettercap
- Aircrack-ng

2.9 Wireless Security Testing

Kiểm tra các thành phần sau:

- WPA/WPA2 cracking
- Rogue AP detection
- Evil Twin attack

Các công cụ phổ biến thường dùng:

- Aircrack-ng
- Kismet
- Wifite

2.10 Cloud Security Testing

Theo chuẩn AWS Well-Architected Security, Azure Security Benchmark, GCP CIS Benchmarks.

Kiểm tra các thành phần sau:

- Misconfigured IAM
- Public S3 bucket
- Key/secret leak
- Misconfigured firewall/security groups

Các công cụ phổ biến:

- ScoutSuite
- Prowler (AWS)
- Aqua Trivy
- Burp + cloud plugins

2.11 Security Audit / Compliance Testing

Kiểm tra theo chuẩn:

- ISO 27001
- PCI-DSS
- HIPAA
- NIST

Các công cụ phổ biến:

- CIS-CAT Pro
- Nessus Compliance
- Qualys Policy Compliance

Bảng các công cụ để thực hiện kiểm thử bảo mật được chia thành nhiều nhóm tùy theo mục đích:

Nhóm công cụ	Mục đích / Phạm vi sử dụng	Ví dụ công cụ
Vulnerability Scanning Tools	Quét hệ thống / mạng / dịch vụ để tìm lỗ hổng tự động	Nessus, OpenVAS, Qualys, Retina, Nexpose
Application Security Testing Tools	Kiểm thử bảo mật ứng dụng web/di động: logic, xác thực, ủy quyền, lỗ hổng ứng dụng	OWASP ZAP, Burp Suite, Acunetix, Veracode, AppScan
Penetration Testing Tools	Dùng để thực hiện tấn công mô phỏng: khai thác lỗ hổng, kiểm tra bảo mật toàn diện	Metasploit, Nmap, Wireshark, Aircrack-ng, John the Ripper
Malware Analysis Tools	Phân tích mã độc, hành vi phần mềm độc hại, đánh giá rủi ro bảo mật từ mã độc	IDA Pro, OllyDbg, Cuckoo Sandbox, VirusTotal
Encryption & Key Management Tools	Mã hóa dữ liệu, quản lý khóa — bảo vệ dữ liệu khi lưu trữ hoặc truyền tải	OpenSSL, VeraCrypt, Keyczar, dịch vụ quản lý khóa như AWS Key Management Service

3. Xây dựng một checklist kiểm thử bảo mật

Dưới đây là checklist kiểm thử bảo mật đã được xây dựng cho một doanh nghiệp có hệ thống mạng thông dụng điển hình, bao gồm các nhóm: **Web , API, Mobile, Network.**

A. WEB APPLICATION SECURITY CHECKLIST

(Theo khuyến nghị **OWASP Web Security Testing Guide – WSTG**)

1. Authentication (Xác thực)

- Kiểm tra Brute-force / Credential stuffing
- Kiểm tra chính sách mật khẩu (độ mạnh, độ dài, ký tự bắt buộc)
- Kiểm tra lock account sau nhiều lần login sai
- Kiểm tra 2FA / MFA
- Kiểm tra reset password (token, hết hạn, rò rỉ thông tin)
- Kiểm tra session fixation

2. Authorization (Phân quyền)

- Kiểm tra truy cập trái phép vào URL (direct access)
- Kiểm tra chức năng không dành cho role hiện tại
- Kiểm tra IDOR (Insecure Direct Object Reference)
- Kiểm tra bypass access (đổi param, đổi ID, đổi token)

3. Session Management (Quản lý phiên)

- Cookie có HttpOnly, Secure, SameSite
- Session hết hạn khi logout
- Session timeout (inactivity)
- Session ID không đoán được
- Kiểm tra chiếm quyền session (session hijacking)

4. Input Validation

- Kiểm tra **SQL Injection**
- Kiểm tra **XSS** (Reflected / Stored / DOM)
- Kiểm tra **HTML injection**
- Kiểm tra **Command Injection**
- Kiểm tra **File Upload** (loại file, bypass filter, upload shell)
- Kiểm tra **Path Traversal**

5. Business Logic

- Kiểm tra bypass step (skip bước thanh toán, skip bước xác nhận)
- Kiểm tra cố ý thay đổi giá
- Kiểm tra race condition
- Kiểm tra abuse chức năng (spam, tạo nhiều order, API flood)

6. Error Handling & Logging

- Không hiển thị lỗi nhạy cảm (stack trace, SQL error)

- Log đầy đủ, không log dữ liệu nhạy cảm
- Kiểm tra log injection

7. Security Headers

- X-Frame-Options
- Content-Security-Policy
- X-XSS-Protection
- Strict-Transport-Security
- Referrer-Policy

8. TLS/SSL

- Kiểm tra chặn HTTP → redirect HTTPS
- Kiểm tra certificate valid
- Kiểm tra SSL version (không dùng SSL v2, v3, TLS 1.0)

B. API SECURITY CHECKLIST

(Chuẩn **OWASP API Security Top 10**)

1. Authentication

- Bắt buộc dùng token (JWT, OAuth2...)
- Token hết hạn (exp claim)
- Kiểm tra refresh token flow
- Không cho login bằng nhiều phương thức để đoán

2. Authorization

- Kiểm tra **BOLA** – Broken Object Level Auth
- Kiểm tra truy cập object của user khác
- Kiểm tra phân quyền theo role

3. Rate Limiting & Throttling

- Giới hạn request / user
- Giới hạn request / IP
- Phát hiện flood, brute-force

4. Input Validation

- SQLi trong API param
- XSS trong JSON
- Command injection
- Kiểm tra upload file qua API

5. Data Exposure

- Không trả về thông tin nhạy cảm (password, token, internal IDs)

- Mask dữ liệu: email, phone, credit card
- Kiểm tra response quá nhiều data (overexposure)

6. Endpoint Security

- Không lộ Swagger / OpenAPI / graphql explorer
- Kiểm tra endpoint ẩn hoặc debug endpoints
- Kiểm tra HTTP method (GET/POST/PUT/DELETE) đúng mục đích

7. Business Logic in APIs

- Bỏ qua bước xác nhận (ví dụ thanh toán, verify OTP)
- Tấn công race condition qua API
- Tạo nhiều request dẫn đến mất tiền, duplicate order

8. JWT Security

- Check alg = none
- Check forgery
- Check weak secret
- Check tampering

C. MOBILE SECURITY CHECKLIST

(Dựa trên **OWASP MSTG**)

1. Storage Security

- Không lưu mật khẩu trong SharedPreferences
- Không lưu token chưa mã hóa
- Không lưu dữ liệu nhạy cảm trong local DB (SQLite)
- Kiểm tra file backup

2. Authentication / Authorization

- Kiểm tra bypass login (patch APK, frida hook)
- Kiểm tra hardcoded credentials
- Kiểm tra root/jailbreak detection

3. Network Security

- Kiểm tra MITM
- SSL Pinning có bật không
- Kiểm tra traffic encryption

4. Reverse Engineering

- Decompile APK/IPA
- Kiểm tra hardcoded API keys
- Kiểm tra obfuscation (ProGuard / DexGuard)

5. Runtime Manipulation

- Kiểm tra bypass logic qua Frida
- Kiểm tra hook được hay không
- Kiểm tra chống debug

6. WebView Security

- Kiểm tra JS Injection
- Kiểm tra file access trong WebView
- Kiểm tra domain whitelist

D. NETWORK SECURITY CHECKLIST

(Dành cho hệ thống, server, hạ tầng)

1. Port & Service Scanning

- Quét tất cả port TCP/UDP
- Xác định service (banner grabbing)
- Kiểm tra service không cần thiết

2. Network Configuration

- Kiểm tra firewall
- Kiểm tra IDS/IPS
- Kiểm tra segmentation (VLAN)

3. Vulnerability Scanning

- Nessus scan
- OpenVAS scan
- Kiểm tra missing patch

4. Protocol Security

- Kiểm tra SMB, FTP, Telnet (tắt nếu không dùng)
- Kiểm tra DNS poisoning
- Kiểm tra ARP spoofing

5. Wireless Security

- Kiểm tra WPA2/WPA3
- Kiểm tra rogue AP
- Kiểm tra password weak

6. Server Hardening

- Tắt dịch vụ không cần
- Kiểm tra quyền file (chmod)
- Kiểm tra SSH security (key, disable root login)
- Kiểm tra cấu hình database

7. Logging & Monitoring

- Kiểm tra log đầy đủ
- Kiểm tra SIEM hoạt động
- Kiểm tra alert bất thường