DANH SÁCH TESTCASE ĐÁNH GIÁ ỨNG DỤNG

1. ĐÁNH GIÁ BẢO MẬT ỨNG DỤNG WEB

1.1. THU THẬP THÔNG TIN

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Information Gathering	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	Sử dụng các công cụ tìm kiếm như Google, Bing, … để tìm kiếm các thông tin như mô hình mạng và cấu hình, tài khoản, thông báo lỗi, …	Không ảnh hưởng đến ứng dụng
	Fingerprint Web Server	Xác định phiên bản và loại máy chủ ứng dụng được sử dụng để xác định các lỗ hổng đã biết và các mã khai thác thích hợp	Không ảnh hưởng đến ứng dụng
	Review Webserver Metafiles for Information Leakage	Phân tích tập tin robots.txt và xác định các nhãn <META> của ứng dụng Tìm kiếm thông tin về các tập tin sao lưu có trên máy chủ	Không ảnh hưởng đến ứng dụng
	Enumerate Applications on Webserver	Tìm kiếm các ứng dụng được host trên máy chủ (bao gồm host ảo, subdomain), các cổng không tiêu chuẩn (các cổng > 1024), chuyển vùng DNS	Không ảnh hưởng đến ứng dụng
	Review Webpage Comments and Metadata for Information Leakage	Tìm kiếm các thông tin nhạy cảm từ các chú thích và metadata có trong mã nguồn (chức năng view-source của trình duyệt)	Không ảnh hưởng đến ứng dụng
	Identify application entry points	Xác định các trường, tham số đầu vào được ẩn đi, các phương thúc gọi HTTP	Không ảnh hưởng đến ứng dụng
	Map execution paths through application	Ánh xạ các chức năng của ứng dụng và hiểu được luồng xử lý chính của ứng dụng	Không ảnh hưởng đến ứng dụng
	Fingerprint Web Application Framework	Xác định framework/CMS ứng dụng sử dụng thông qua các HTTP header, cookie, mã nguồn và các tập tin/thư mục Xác định các thông tin về File Extension được thực thi như php, aspx, jsp, …	Không ảnh hưởng đến ứng dụng
	Fingerprint Web Application	Xác định phiên bản và nền tảng của ứng dụng để xác định các lỗ hổng đã biết và các mã khai thác thích hợp	Không ảnh hưởng đến ứng dụng
	Map Network and Application Architecture	Xác định kiến trúc của ứng dụng bao gồm ngôn ngũ lập trình, WAF, Reverse proxy, máy chủ ứng dụng, CSDL	Không ảnh hưởng đến ứng dụng

1.2. KIỂM TRA QUẢN LÝ CẤU HÌNH & TRIỂN KHAI Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Configuration and Deploy Management Testing	Test Network/Infrastructure Configuration	Tìm hiểu cách thức giao tiếp giữa các thành phần của ứng dụng, cách cấu hình ứng dụng, máy chủ CSDL, WebDAV, FTP để xác định các lỗ hổng đã biết	Không ảnh hưởng đến ứng dụng
	Test Application Platform Configuration	Xác định các tập tin/thư mục cài đặt mặc định, cách thức xử lý lỗi máy chủ (40*, 50*), cách thức phân quyền, ghi log ứng dụng Kiểm tra các lỗ hổng đã biết về cấu hình nền tảng hoặc hệ thống	Không ảnh hưởng đến ứng dụng
	Test File Extensions Handling for Sensitive Information	Kiểm tra thông tin về định dạng, đuôi file (File Extention) thông qua kỹ thuật Fuzzing, sử dụng Wordlist: Tìm các tập tin, thông tin quan trọng (.asa, .inc, .sql, .zip, .tar, .pdf, .txt, …)	Không ảnh hưởng đến ứng dụng
	Backup and Unreferenced Files for Sensitive Information	Kiểm tra mã nguồn Javascript, tập tin cache, tập tin backup (.old, .bak, .inc, .src) và dự đoán tên các tập tin có thể có Kiểm tra các thư mục cài đặt, tập tin sao lưu của framework còn sót lại trong quá trình cài đặt ứng dụng	Không ảnh hưởng đến ứng dụng
	Enumerate Infrastructure and Application Admin Interfaces	Thực hiện liệt kê tập tin và thư mục, tìm kiếm các chú thích và đường dẫn chứa thông tin đến trang quản trị trong mã nguồn (/admin, /administrator, /backoffice, /backend, ...), các cổng dịch vụ khác (Tomcat/8080) Tìm kiếm các thông tin về hạ tầng và ứng dụng như đường dẫn quản trị	Không ảnh hưởng đến ứng dụng
	Test HTTP Methods	Xác định các phương thức được phép gọi đến máy chủ bằng phương thức OPTIONS. Kiểm tra khả năng quản lý truy cập thông qua phương thức HEAD và TRACE	Không ảnh hưởng đến ứng dụng
	Test HTTP Strict Transport Security	"Xác định header HSTS trên máy chủ ứng dụng thông qua header của gói tin HTTP response curl -s -D- https://<url>/ | grep Strict"	Không ảnh hưởng đến ứng dụng
	Test RIA cross domain policy	Phân tích các quyền được phép thông qua các tập tin chính sách (crossdomain.xml/clientaccesspolicy.xml) và header allow-access-from	Không ảnh hưởng đến ứng dụng

1.3. KIỂM TRA QUẢN LÝ ĐỊNH DANH

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Identity Management Testing	Test Role Definitions	Xác thực các vai trò trong hệ thống được định nghĩa bởi ứng dụng thông qua ma trận phân quyền. Tìm kiếm khả năng vượt qua các quy định về vai trò (role) của người dùng trên hệ thống	Không ảnh hưởng đến ứng dụng
	Test User Registration Process	Kiểm tra các yêu cầu định danh cho quá trình đăng ký người dùng phù hợp với yêu cầu nghiệp vụ và bảo mật.	Không ảnh hưởng đến ứng dụng
	Test Account Provisioning Process	Xác định các vai trò được phép tạo người dùng và loại tài khoản được phép tạo.	Không ảnh hưởng đến ứng dụng
	Testing for Account Enumeration and Guessable User Account	Kiểm tra thông báo lỗi đăng nhập, mã kết quả/giá trị tham số, liệt kê mọi giá trị userid có thể có (thông qua chức năng đăng nhập, quên mật khẩu). Xác định các tài khoản mặc định, tài khoản khách (Guest)	Không ảnh hưởng đến ứng dụng
	Testing for Weak or unenforced username policy	Xác định nguyên tác đặt tên tài khoản, liệt kê các tài khoản hợp lệ có thể đoán được Kiểm tra khả năng vượt qua các chính sách yếu trên hệ thống	Không ảnh hưởng đến ứng dụng

1.4. KIỂM TRA CHỨNG THỰC

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Authentication Testing	Testing for Credentials Transported over an Encrypted Channel	Kiểm tra các gói tin chứa tài khoản đăng nhập có thể được thực hiện trên giao thức HTTP thay vì HTTPS	Không ảnh hưởng đến ứng dụng
	Testing for Default Credentials	Kiểm tra các tài khoản mặc định của các ứng dụng/CMS thông dụng, mật khẩu mặc định cho tài khoản mới tạo (nếu có) Xác định các tài khoản mặc định được tạo, khả năng đoán được tên tài khoản hoặc có được tài khoản	Không ảnh hưởng đến ứng dụng
	Testing for Weak Lock Out Mechanism	Đánh giá cơ chế khóa tài khoản để ngăn chặn tấn công vét cạn mật khẩu. Đánh giá cơ chế kiểm soát việc mở khóa tài khoản để ngăn chặn việc mở khóa trái phép	Không ảnh hưởng đến ứng dụng
	Testing for Bypassing Authentication Schema	Kiểm tra khả năng vượt qua cơ chế xác thực của ứng dụng thông qua thay đổi tham số nếu việc xác thực dựa trên tham số, thay đổi giá trị phiên làm việc, lỗ hổng SQL Injection	Không ảnh hưởng đến ứng dụng

	Test Remember Password Functionality	Xác định lỗ hổng có thể có trong chức năng “Gợi nhớ mật khẩu” Kiểm tra thông tin lưu trong cookie, tìm kiếm mật khẩu nếu có. Xác định mật khẩu được lưu dưới dạng cleartext hoặc mã hóa	Không ảnh hưởng đến ứng dụng
	Testing for Browser Cache Weakness	Kiểm tra lỗ hổng trong phương thức đăng xuất, có thể truy cập lại các trang trước mặc dù đã đăng xuất Kiểm tra cơ chế quản lý bộ nhớ đệm của trình duyệt thông qua cơ chế Back sau khi đã đăng xuất. Kiểm tra header Cache-Control trong HTTP response	Không ảnh hưởng đến ứng dụng
	Testing for Weak Password Policy	Xác định cơ chế ngăn chặn tấn công vét cạn mật khẩu của ứng dụng. Kiểm tra chính sách về mật khẩu như độ dài, độ phức tạp, yêu cầu thay đổi mật khẩu, …	Không ảnh hưởng đến ứng dụng
	Testing for Weak Security Question/Answer	Kiểm tra các câu hỏi bảo mật được sử dụng, khả năng tấn công vét cạn câu trả lời	Không ảnh hưởng đến ứng dụng
	Testing for Weak Password Change or Reset Functionalities	"Kiểm tra chức năng reset mật khẩu, xác định kênh gửi thông tin là email hay SMS, đường dẫn reset được tạo ngẫu nhiên hoặc có thể đoán được, thời gian hiểu lực của đường dẫn.	Không ảnh hưởng đến ứng dụng
	Testing for Weaker Authentication in Alternative Channel	Kiểm tra chức năng thay đổi mật khẩu, xác định việc thay đổi có cần mật khẩu cũ, khả năng tạo request để thay đổi mật khẩu người dùng khác trái phép (CSRF)"	Không ảnh hưởng đến ứng dụng

1.5. KIỂM TRA PHÂN QUYỀN

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Authorization Testing	Testing Directory Traversal/File Include	Xác định các chức năng thực hiện tải tập tin dưới hệ thống như lấy hình ảnh, xuất báo cáo, … Kiểm tra lỗ hổng bằng cách thêm các ký tự "../" vào tên tập tin	Không ảnh hưởng đến ứng dụng
	Testing for Bypassing Authorization Schema	Xác định các đường dẫn/chức năng cần tài khoản để truy cập nhưng có thể truy cập mà không cần xác thực, đặc biệt là các trang quản trị Xác định các chức năng cho phép người dùng truy cập các thông tin không thuộc quyền hạn được cấp Kiểm tra khả năng vượt qua cơ chế xác thực bằng các thay đổi tham số định danh, xử dụng phiên làm việc đã biết	Không ảnh hưởng đến ứng dụng

	Testing for Privilege Escalation	Xác định cơ chế định danh quyền/vai trò của tài khoản như thông qua giá trị một biến số lưu trong cookie hoặc đường dẫn (groupid, …). Thực hiện thay đổi giá trị các biến này để leo quyền Kiểm tra khả năng leo quyền/đoạt quyền truy cập đến các tài nguyên/chức năng ứng dụng ngoài quyền hạn được cấp	Không ảnh hưởng đến ứng dụng
	Testing for Insecure Direct Object References	Xác định các đường dẫn chứ tham số có thể là id của một đối tượng như tài khoản, vật phẩm, … Thực hiện thay đổi giá trị này để đọc thông tin của đối tượng khác (?invoice=123 -> ?invoice=456) Kiểm tra khả năng thay đổi quyền hạn người dùng/vai trò người dùng trên ứng dụng từ một tài khoản khác	Không ảnh hưởng đến ứng dụng

1.6. KIỂM TRA QUẢN LÝ PHIÊN

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Session Management Testing	Testing for Bypassing Session Management Schema	Xác định khả năng giải mã cookie, giá trị sessionid hoặc thay đổi giá trị đó để leo quyền	Không ảnh hưởng đến ứng dụng
	Testing for Cookies Attributes	Kiểm tra biến cookie của ứng dụng đã được bật các cờ httponly, secure, thiết lập thời gian hết hạn và không chứa các thông tin nhạy cảm	Không ảnh hưởng đến ứng dụng
	Testing for Session Fixation	Kiểm tra biến cookie của ứng dụng có được hủy sau khi người dùng đăng xuất bằng cách sử dụng lại cookie cũ sau khi đã đăng xuất	Không ảnh hưởng đến ứng dụng
	Testing for Exposed Session Variables	Kiểm tra khả năng giải mã của giá trị phiên làm việc hoặc cùng 1 giá trị được sử dụng nhiều lần, xác định các biến sessionid được gửi theo phương thức GET	Không ảnh hưởng đến ứng dụng
	Testing for Cross Site Request Forgery	Xác định các chức năng có thể bị tấn công Cross Site Request Forgery - CSRF Kiểm tra các chức năng nhạy cảm, cần người dùng xác thực có được kèm theo các token bảo vệ, khả năng giả mạo người dùng để thực hiện các chức năng này	Không ảnh hưởng đến ứng dụng
	Testing for Logout Functionality	Kiểm tra khả năng phiên làm việc vẫn còn được sử dụng sau khi đã đăng xuất	Không ảnh hưởng đến ứng dụng
	Test Session Timeout	Kiểm tra thời gian hết hạn phiên làm việc đã hợp lý, phiên có được hủy sau khi đã hết hạn	Không ảnh hưởng đến ứng dụng

	Testing for Session Puzzling	Xác định các chức năng dẫn đến khởi tạo giá trị phiên làm việc, kiểm tra các giá trị được tạo ra có giống nhau	Không ảnh hưởng đến ứng dụng

1.7. KIỂM TRA SÀNG LỌC DỮ LIỆU ĐẦU VÀO

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Data Validation Testing	Testing for Reflected Cross Site Scripting	Xác định các chức năng chứa trường nhập liệu, kiểm tra lỗ hổng bằng các nhập các đoạn mã Javascript như "<script>alert(1)</script>"	Không ảnh hưởng đến ứng dụng
	Testing for Stored Cross Site Scripting	Xác định các chức năng chứa trường nhập liệu, kiểm tra lỗ hổng bằng các nhập các đoạn mã Javascript như "<script>alert(1)</script>"	Các mã JS được chèn vào nội dung được lưu trong DB. Người dùng bất kỳ khi truy cập các nội dung này sẽ trigger mã JS được chèn. PA hạn chế: chỉ chèn các mã JS thực hiện popup của sổ (alert).
	Testing for HTTP Verb Tampering	Thực hiện thay đổi phương thức của các chức năng, từ GET thành POST và ngược lại Thay đổi các phương thức HTTP thông thường như GET/POST bằng các phương thức PUT/DELETE/TRACE/HEAD	Không ảnh hưởng đến ứng dụng
	Testing for HTTP Parameter pollution	Thực hiện ghi nhận các kết quả trả về khi nhập giá trị đúng cho tham số, thay đổi giá trị tham số và lặp lại tham số nhiều lần để xác định khả năng tồn tại lỗ hổng	Không ảnh hưởng đến ứng dụng
	Testing for SQL Injection	Xác định khả năng tồn tại lỗ hổng thông qua kết quả trả về khi nhập các ký tự đặc biệt nhằm phá vỡ kết cấu câu truy vấn như dấy nhày đơn ('), dấu nháy đôi (")	Không ảnh hưởng đến ứng dụng
	Testing for LDAP Injection	Thực hiện kiểm tra khả năng tồn tại lỗ hổng bằng cách chèn các câu truy vấn LDAP như: /ldapsearch?user=* user=*user=*)(uid=*))(|(uid=* pass=password"	Không ảnh hưởng đến ứng dụng
	Testing for ORM Injection	Xác định khả năng tồn tại lỗ hổng thông qua kết quả trả về khi nhập các ký tự đặc biệt nhằm phá vỡ kết cấu câu truy vấn	Không ảnh hưởng đến ứng dụng

	Testing for XML Injection	Kiểm tra khả năng tồn tại lỗ hổng bằng cách chèn các ký tự Meta của XML vào giá trị tham số như: ', "" , <>, <!--/-->, &, <![CDATA[/]]>, XXE, TAG	Không ảnh hưởng đến ứng dụng
	Testing for SSI Injection	Kiểm tra khả năng tồn tại lỗ hổng bằng cách chèn các ký tự đặc biệt, mã khai thác vào giá trị tham số như: < ! # = / . "" - > and [a-zA-Z0-9]	Không ảnh hưởng đến ứng dụng
	Testing for XPath Injection	"Kiểm tra khả năng tồn tại lỗ hổng bằng cách chèn dấu nháy vào giá trị tham số như: Username: ‘ or ‘1’ = ‘1 Password: ‘ or ‘1’ = ‘1"	Không ảnh hưởng đến ứng dụng
	IMAP/SMTP Injection	Kiểm tra khả năng tồn tại lỗ hổng bằng cách chèn các ký tự đặc biệt vào giá trị tham số như (i.e.: \, ‘, “, @, #, !, |)	Không ảnh hưởng đến ứng dụng
	Testing for Code Injection	Kiểm tra khả năng tồn tại lỗ hổng bằng cách chèn các câu lệnh hệ thống vào giá trị tham số sau dấu chấm phẩy như: ?arg=1; system('id')	Không ảnh hưởng đến ứng dụng
	Testing for Local File Inclusion	Kiểm tra lỗ hổng bằng cách thêm các ký tự "../" vào tên tập tin	Không ảnh hưởng đến ứng dụng
	Testing for Remote File Inclusion	Kiểm tra lỗ hổng bằng cách sử dụng các URL chứa các mã khai thác	Không ảnh hưởng đến ứng dụng
	Testing for Command Injection	Xác định nền tảng của ứng dụng như OS, cấu trúc thư mục, đường dẫn tương đối, … từ đó thực thi các câu lệnh trên máy chủ như: %3Bcat%20/etc/passwd	Không ảnh hưởng đến ứng dụng
	Testing for HTTP Splitting/Smuggling	Kiểm tra khả năng tồn tại lỗ hổng bằng cách chèn thêm vào HTTP header của request nhiều đoạn request khác nhau hoặc break các header bằng ký hiệu xuống dòng CRLF	Không ảnh hưởng đến ứng dụng

1.8. KIỂM TRA CƠ CHẾ XỬ LÝ LỖI

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Error Handling	Analysis of Error Codes	Xác định các mã lỗi được tạo ra từ ứng dụng hoặc máy chủ. Thu thập các thông tin nhạy cảm về máy chủ, ứng dụng, CSDL từ các thông báo lỗi	Không ảnh hưởng đến ứng dụng
	Analysis of Stack Traces	Thực hiện nhập các giá trị có thể gây lỗi vào các trường tham số, từ đó phân tích Stack Trace có thể được trả về:	Không ảnh hưởng đến ứng dụng

		- Giá trị không hợp lệ, không phù hợp với logic của ứng dụng - Giá trị chứa các ký tự đặc biệt không thuộc bảng mã ASCII thông dụng - Truy cập các trang nội bộ mà không xác thực Bypass luồng xác thực của ứng dụng	

1.9. KIỂM TRA THUẬT TOÁN MÃ HÓA

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Cryptography	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection	Xác định ứng dụng SSL đang sử dụng, các thuật toán/giao thức mã hóa yếu được phép sử dụng có thể dẫn đến các lỗ hổng như RC4, BEAST, CRIME, POODLE	Không ảnh hưởng đến ứng dụng
	Testing for Padding Oracle	Kiểm tra khả năng tồn tại lỗ hổng bằng cách thay đổi dữ liệu đã được mã hóa và so sánh kết quả khi đưa các dữ liệu khác nhau vào quá trình giải mã: • Dữ liệu được giải mã và kết quả trả về đúng • Dữ liệu được giải mã và kết quả trả về gây lỗi hoặc ngoại lệ • Dữ liệu không thể giải mã do lỗi padding	Không ảnh hưởng đến ứng dụng
	Testing for Sensitive information sent via unencrypted channels	Kiểm tra các thông tin được truyền không qua mã hóa: • Thông tin dùng để xác thực như tài khoản/mật khẩu, mã PIN, giá trị định danh phiên làm việc, token, cookie…) • Thông tin được bảo vệ bởi pháp luật, quy định hay chính sách của tổ chức cụ thể như thẻ tín dụng, dữ liệu khách hàng, ...	Không ảnh hưởng đến ứng dụng

1.10. KIỂM TRA LOGIC NGHIỆP VỤ

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Business Logic Testing	Test Business Logic Data Validation	Kiểm tra bằng cách nhập các giá trị không phù hợp với logic xử lý của ứng dụng như nhập số tiền âm, …	Không ảnh hưởng đến ứng dụng
	Test Ability to Forge Requests	Kiểm tra các trường/tham số/chức năng ẩn có khả năng truy cập mà không cần tuân theo luồng xử lý của ứng dụng	Không ảnh hưởng đến ứng dụng
	Test Integrity Checks	Kiểm tra khả năng nhập vào các thông tin/dữ liệu trái với logic của ứng dụng, các	Không ảnh hưởng đến ứng dụng

		thao tác dữ liệu có thể được thực hiện trái phép	
	Test for Process Timing	Xác định các chức năng phụ thuộc vào thời gian và thực hiện các trường hợp có thể phá vỡ luồng xử lý của ứng dụng	Không ảnh hưởng đến ứng dụng
	Test Number of Times a Function Can be Used Limits	Kiểm tra các chức năng chỉ nên được thực hiện 1 lần hoặc với số lần nhất định trong 1 khoảng thời gian như OTP bằng khi thực thi liên tục nhiều lần	Không ảnh hưởng đến ứng dụng
	Testing for the Circumvention of Work Flows	Xác định luồng thực thi của các chức năng và kiểm tra khả năng phá vỡ luồng xử lý, có thể bỏ qua các bước	Không ảnh hưởng đến ứng dụng
	Test Defenses Against Application Mis-use	Kiểm tra, đánh giá các cơ chế bảo vệ của ứng dụng như ngăn chặn truy cập, khóa tài khoản, token/captcha	Không ảnh hưởng đến ứng dụng
	Test Upload of Unexpected File Types	Kiểm tra khả năng sàng lọc file upload bằng cách tải lên các tập tin không không phù hợp với ứng dụng như đăng tải tập tin chứa mã nguồn thay vì hình ảnh	Không ảnh hưởng đến ứng dụng
	Test Upload of Malicious Files	Kiểm tra khả năng sàng lọc file upload bằng cách tải lên các tập tin thực thi chứa mã nguồn độc hại như .php, .asp, .jsp, …	Có thể upload Webshell, điều khiển các nội dung của ứng dụng. PA hạn chế: Ngay sau khi xác nhận được lỗ hổng tồn tại sẽ thông báo để xóa webshell đã được upload

1.11. KIỂM TRA XỬ LÝ PHÍA NGƯỜI DÙNG

Bên cạnh các nhóm lỗ hổng liên quan xử lý phía máy chủ, ứng dụng Web thường tồn tại các đoạn mã xử lý ở trình duyệt trên máy người dùng cuối. Khi đó nếu các hàm chức năng tồn tại lỗ hổng có thể dẫn tới người dùng bị tấn công, đánh cắp tài khoản, phiên làm việc hoặc lừa người dùng đánh cắp cả OTP trong một số trường hợp (ứng dụng yêu cầu thanh toán hoặc xác thực nhiều bước). Từ đó cần thực hiện các kiểm tra nhằm đảm bảo an toàn cho người dùng khi sử dụng ứng dụng và cả khi ứng dụng tồn tại lỗ hổng.

Cách thức thực hiện:

- Kiểm tra cách thức trình duyệt nhận về các đối tượng: HTML, Flash, Javascript, DOM, …
- Kiểm tra khả năng xảy ra các tấn công như XSS, Clickjacking, Phishing.

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Client-Side Testing	Testing for DOM based Cross Site Scripting	Xác định các chức năng chứa trường nhập liệu, kiểm tra lỗ hổng bằng các nhập các đoạn mã Javascript như "<script>alert(1)</script>"	Không ảnh hưởng đến ứng dụng

	Testing for JavaScript Execution	Kiểm tra lỗ hổng bằng cách chèn các mã thực thi Javascript vào đường dẫn như:	Không ảnh hưởng đến ứng dụng
		www.victim.com/?javascript:alert(1)	
	Testing for HTML Injection	Kiểm tra lỗ hổng bằng cách chèn các mã HTML vào đường dẫn như: ?user=<img%20src='aaa'%20onerror=alert(1)>	Không ảnh hưởng đến ứng dụng
	Testing for Client-Side URL Redirect	Kiểm tra lỗ hổng bằng cách chèn các đường dẫn độc hại vào đường dẫn như: ?redirect=www.fake-target.site	Không ảnh hưởng đến ứng dụng
	Testing for CSS Injection	Kiểm tra lỗ hổng bằng cách chèn các mã CSS vào đường dẫn như: • www.victim.com/#red;-o-link:'javascript:alert(1)';-o-linksource:current; (Opera [8,12]) • www.victim.com/#red;-:expression(alert(URL=1)); (IE 7/8)	Không ảnh hưởng đến ứng dụng
	Testing for Client-Side Resource Manipulation	Kiểm tra lỗ hổng bằng cách tải tài nguyên chứa mã thực thi Javascript vào đường dẫn như: www.victim.com/#http://evil.com/js.js	Không ảnh hưởng đến ứng dụng
	Test Cross Origin Resource Sharing	Kiểm tra các header quy định khả năng chia sẻ tài nguyên như: • Origin & Access-Control-Allow-Origin • Access-Control-Request-Method & Access-Control-Allow-Method • Access-Control-Request-Headers & Access-Control-Allow-Headers • Access-Control-Allow-Credentials	Không ảnh hưởng đến ứng dụng
	Testing for Cross Site Flashing	Kiểm tra khả năng khai thác ứng dụng Flash thông đánh giá mã nguồn ActionScript của ứng dụng	Không ảnh hưởng đến ứng dụng
	Testing for Clickjacking	Kiểm tra lỗ hổng bằng cách tải ứng dụng vào một iframe trong một ứng dụng khác	Không ảnh hưởng đến ứng dụng
	Testing Web Sockets	Kiểm tra khả năng bảo mật của WebSockets nếu ứng dụng có sử dụng	Không ảnh hưởng đến ứng dụng
	Test Web Messaging	Kiểm tra cách ứng dụng triển khai và xử lý dữ liệu Web Messaing nếu có	Không ảnh hưởng đến ứng dụng
	Test Local Storage	Kiểm tra các thông tin được lưu trữ trong Local Storage của trình duyệt, khả năng chèn mã khai thác như XSS: http://server/StoragePOC.html#<img src=x onerror=alert(1)>	Không ảnh hưởng đến ứng dụng

2. ĐÁNH GIÁ BẢO MẬT ỨNG DỤNG MOBILE – OWASP MOBILE SECURITY TESTING GUIDE

2.1. KIỂM TRA LƯU TRỮ DỮ LIỆU

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Data Storage	Testing Local Storage for Sensitive Data	Ứng dụng lưu trữ các thông tin nhạy cảm ở dạng plain-text, dễ dàng đọc được bởi các chương trình chỉnh sửa văn bản khi tương tác vào các vùng lưu trữ trên thiết bị, từ đó các chuyên gia sẽ thực hiện kiểm tra đầy đủ các tập tin lưu trữ để chắc chắn ứng dụng không lưu chúng dưới dạng bản rõ	Không ảnh hưởng đến ứng dụng
	Testing Logs for Sensitive Data	Nhà thầu thực hiện kiểm tra trong quá trình vận hành/sử dụng từ thiết bị người dùng ứng dụng để lộ các thông tin nhạy cảm trong log của hệ thống, thông qua các hàm Log được dùng trong quá trình Debug/quá trình phát triển ứng dụng.	Không ảnh hưởng đến ứng dụng
	Testing for Sensitive Data Sent to Third Parties	Ứng dụng để lộ các thông tin nhạy cảm do sử dụng thư viện của bên thứ ba và thông tin được gửi qua mạng có thể bị sniff và để lộ thông tin nhạy cảm, các thông tin gửi ra bên ngoài chưa được kiểm tra, nhà phát triển chỉ tích hợp vào theo nhu cầu của ứng dụng.	Không ảnh hưởng đến ứng dụng
	Testing for Sensitive Data in the Keyboard Cache	Khi người dùng nhập vào các trường đầu vào, phần mềm sẽ tự động đề xuất dữ liệu. Tính năng này có thể rất hữu ích cho các ứng dụng nhắn tin. Tuy nhiên, bộ đệm bàn phím có thể tiết lộ thông tin nhạy cảm khi người dùng chọn trường nhập có loại thông tin này. Đối với các vị trí nhập có chứa thông tin nhạy cảm, nhà thầu tiến hành kiểm tra khả năng cache lại các dữ liệu nhạy cảm được nhập từ người dùng.	Không ảnh hưởng đến ứng dụng
	Testing for Sensitive Stored Data Exposed via IPC Mechanisms	IPC là cơ chế giao tiếp, truyền dữ liệu giữa các thành phần trong một ứng dụng, cho phép dữ liệu được lưu trữ của ứng dụng được truy cập và sửa đổi bởi các ứng dụng khác. Nếu không được cấu hình đúng, các cơ chế này có thể rò rỉ dữ liệu nhạy cảm. Tuỳ theo từng nền tảng (Android, iOS) sẽ sử dụng cơ chế IPC khác nhau, tồn tại rủi ro khi các ứng dụng khác có thể gọi vào không mong muốn. Từ đó, dẫn đến việc thất thoát dữ liệu.	Không ảnh hưởng đến ứng dụng

	Testing for Sensitive Data Disclosure Through the User Interface	Nhiều ứng dụng yêu cầu người dùng nhập một số loại dữ liệu, ví dụ, đăng ký tài khoản hoặc thanh toán. Dữ liệu nhạy cảm có thể bị lộ nếu ứng dụng không che dấu đúng cách, khi hiển thị dữ liệu ở dạng văn bản rõ ràng.	Không ảnh hưởng đến ứng dụng
		Việc che dấu dữ liệu nhạy cảm, bằng cách hiển thị dấu hoa thị hoặc dấu chấm thay vì văn bản rõ ràng nên được thi hành trong hoạt động của ứng dụng để ngăn tiết lộ và giảm thiểu rủi ro như nhìn trộm hoặc ghi màn hình (các ứng dụng có thể đọc và ghi nhận lại những thông tin người dùng nhập vào trên thiết bị.	
	Testing Backups for Sensitive Data	Hầu hết các thiết bị, hệ điều hành trên Mobile hỗ trợ phương pháp Backup dữ liệu. Tuy nhiên, các bản sao lưu thường bao gồm các bản sao dữ liệu đang lưu trữ và có thể giải nén/trích xuất ra bản rõ dữ liệu. Các dữ liệu người dùng nhạy cảm được lưu trữ bởi ứng dụng có thể rò rỉ khi đưa vào các bản sao lưu này và là nơi có rủi ro thất thoát, rò rỉ dữ liệu người dùng.	Không ảnh hưởng đến ứng dụng
	Testing Auto-Generated Screenshots for Sensitive Information	Các nhà sản xuất cung cấp cho người dùng trải nghiệm mượt khi khởi động và thoát ứng dụng để khôi phục trạng thái hoạt động, vì vậy họ đã giới thiệu tính năng lưu ảnh chụp màn hình để sử dụng khi ứng dụng được chạy nền. Tính năng này có thể gây ra rủi ro bảo mật. Dữ liệu nhạy cảm có thể bị lộ nếu người dùng cố tình chụp màn hình ứng dụng trong khi dữ liệu nhạy cảm được hiển thị. Một ứng dụng độc hại đang chạy trên thiết bị và có thể liên tục chụp màn hình cũng có thể làm lộ dữ liệu. Ảnh chụp màn hình được ghi vào bộ nhớ cục bộ, từ đó chúng có thể được phục hồi bởi một ứng dụng giả mạo (nếu thiết bị đã được root) hoặc ai đó đã đánh cắp thiết bị. Ví dụ: chụp ảnh chụp màn hình của ứng dụng ngân hàng có thể tiết lộ thông tin về tài khoản, tín dụng, giao dịch của người dùng, v.v.	Không ảnh hưởng đến ứng dụng
	Testing Memory for Sensitive Data	Kỹ thuật phân tích bộ nhớ có thể giúp các nhà phát triển xác định nguyên nhân gốc rễ của một số vấn đề, chẳng hạn như sự cố ứng dụng (crash). Đồng thời, kỹ thuật này cũng có thể được sử dụng để kiểm tra dữ liệu nhạy cảm được lưu trữ trên bộ nhớ trong quá trình hoạt động của ứng dụng (ví dụ tải về private key hoặc các key quan trọng lưu trữ trên máy chủ).	Không ảnh hưởng đến ứng dụng

2.2. KIỂM TRA THUẬT TOÁN MÃ HÓA

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Cryptographic APIs	Test Configuration of Cryptographic Standard Algorithms	Kiểm tra ứng dụng tuân thủ các hàm mã hoá mạnh.	Không ảnh hưởng đến ứng dụng
		Kiểm tra sử dụng các hàm Custom mã khoá có thể phá vỡ hoặc tồn tại lỗ hổng có thể tấn công Brute Force.	
	Testing Random Number Generation	Kiểm tra ứng dụng sử dụng các hàm Random không tồn tại các lỗ hổng đã được công bố (theo lý thuyết).	Không ảnh hưởng đến ứng dụng
	Testing Key Management	Kiểm tra cơ chế quản lý khoá mã hoá của ứng dụng, kiểm tra hardcode các khoá mã hoá.	Không ảnh hưởng đến ứng dụng

2.3. KIỂM TRA AN TOÀN CƠ CHẾ CHỨNG THỰC

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Insecure Authentication	Weak Password Policy	Ứng dụng cho phép sử dụng các tài khoản với mật khẩu yếu, có thể dễ dàng cho kẻ tấn dò, đoán ra mật khẩu, truy xuất tài nguyên hoặc chiếm đoạt tài khoản người dùng.	Không ảnh hưởng đến ứng dụng
	Bypass Authentication Schema	Ứng dụng cung cấp chức năng chứng thực offline để có thể tương tác với các hàm chức năng bên trong sau khi chứng thực thành công, nhưng người dùng anonymous có thể gọi được các chức năng của ứng dụng mà không cần phải đăng nhập.	Không ảnh hưởng đến ứng dụng
	Testing Fingerprint Authentication using an Asymmetric Key Pair	Thực hiện kiểm tra cách thức tạo khóa ký bằng class KeyPairGenerator và đăng ký khóa chung với máy chủ để triển khai xác thực dấu vân tay. Sau đó xác thực các mẫu dữ liệu bằng cách ký chúng trên thiết bị và xác minh chữ ký trên máy chủ.	Không ảnh hưởng đến ứng dụng

	Test Configuration of Local Authentication Framework	Framework xác thực cục bộ cung cấp các phương tiện để yêu cầu mật khẩu hoặc xác thực Touch ID từ người dùng. Bằng cách sử dụng hàm AssessmentPolicy của lớp LAContext có thể hiển thị và sử dụng một dấu nhắc xác thực. Hai Policies có sẵn xác định các hình thức xác thực được chấp nhận: + Nếu Touch ID không được kích hoạt, mật mã thiết bị được yêu cầu thay thế. Nếu mật mã thiết bị không được bật, đánh giá chính sách thất bại. + Xác thực được giới hạn trong sinh trắc học nơi người dùng được nhắc nhập Touch ID. Hàm AssessmentPolicy trả về giá trị boolean cho biết người dùng đã xác thực.	Không ảnh hưởng đến ứng dụng
	Test Configuration of Keychain Services	API Keychain được sử dụng để lưu trữ token xác thực bí mật hoặc một phần dữ liệu bí mật dùng để xác định người dùng.	Không ảnh hưởng đến ứng dụng
Nhóm	**Kịch bản**	**Mô tả chi tiết**	**Phạm vi ảnh hưởng**
		Để xác thực với dịch vụ từ xa, người dùng phải mở khóa Keychain bằng cụm mật khẩu hoặc dấu vân tay của họ để lấy dữ liệu bí mật. Keychain cho phép lưu các mục với thuộc tính SecAccessControl đặc biệt, sẽ chỉ cho phép truy cập vào mục từ Keychain sau khi người dùng đã thông qua xác thực Touch ID (hoặc mật mã, nếu dự phòng thuộc tính đó được cho phép bởi dự phòng thuộc tính).	

2.4. KIỂM TRA AN TOÀN GIAO TIẾP MẠNG

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng

Insecure Communication	Verifying Data Encryption on the Network	Một trong những chức năng cốt lõi của ứng dụng di động là gửi/nhận dữ liệu qua các hệ thống mạng không tin cậy như là Internet. Đảm bảo trong quá trình trao đổi dữ liệu, giao thức truyền nhận dữ liệu là giao thức có cơ chế mã hóa dữ liệu an toàn. Vì nếu như dữ liệu không được bảo vệ đúng cách thì kẻ tấn công nếu có thể truy cập vào bất kỳ phần nào của cơ sở hạ tầng mạng thì hoàn toàn có khả năng chặn, bắt và sửa đổi dữ liệu. Đây là lý do tại sao các giao thức mạng không được mã hóa hiếm khi được khuyến khích sử dụng. Nhà thầu kiểm tra sự tồn tại các gói giao tiếp với máy chủ Web/API thông qua giao thức HTTP. Kiểm tra các dữ liệu gửi từ các thư viện bên thứ ba có sử dụng kênh truyền không an toàn (HTTP).	Không ảnh hưởng đến ứng dụng
	Making Sure that Critical Operations Use Secure Communication Channels	Đối với các ứng dụng nhạy cảm như ứng dụng ngân hàng, các hoạt động quan trọng (ví dụ: đăng ký người dùng và khôi phục tài khoản) của là một số mục tiêu hấp dẫn đối với kẻ tấn công. Điều này yêu cầu thực hiện các kiểm soát bảo mật nâng cao, chẳng hạn như các kênh bổ sung để xác nhận hành động của người dùng mà không cần dựa vào SMS hoặc email. Ví dụ: hardware token.	Không ảnh hưởng đến ứng dụng
Nền tảng Android	Testing Endpoint Identify Verification	Sử dụng TLS để truyền nhận thông tin nhạy cảm qua mạng để đảm bảo dữ liệu an toàn. Tuy nhiên mã hóa dữ liệu giữa một ứng dụng di động và API bổ trợ của nó không phải là một việc dễ dàng. Do đó các nhà phát triển thường quyết định những giải pháp đơn giản, thuận lợi cho quá trình	Không ảnh hưởng đến ứng dụng

	Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng

		phát triển. Điều đó dẫn đến khi đưa sản phẩm vào sử dụng sẽ phát sinh những vấn đề có khả năng khiến người dùng bị tấn công nghe lén. Có hai vấn đề chính cần được giải quyết: + Xác minh chứng chỉ có phải được cung cấp bởi một nguồn đáng tin cậy (CA). + Xác định rõ chứng chỉ ở máy chủ đầu cuối có hợp lệ hay không. Đảm bảo tên máy chủ và chứng chỉ của nó được xác minh chính xác. Kiểm tra cơ chế hiện thực các hàm liên quan đến kiểm tra chữ ký số an toàn (ví dụ về việc sử dụng TrustManager và Hostname Verifier). Kiểm tra việc sử dụng các thư viện giao thức không an toàn hoặc không còn sử dụng ở phiên bản Android 8.0 trở đi (SSLv3 và HttpsURLConection)	
	Testing Custom Certificate Stores and Certificate Pinning	Certificate pinning là quá trình liên kết ứng dụng di động với chứng chỉ X.509 của máy chủ, thay vì chấp nhận bất kỳ chứng chỉ nào được ký bởi cơ quan chứng nhận tin cậy. Khi thực hiện cơ chế Pinning, ứng dụng phải tự kiểm tra chính xác chứng chỉ máy chủ hoặc định danh chứng chỉ của máy chủ mong muốn. Chứng chỉ có thể được Pinning và mã hóa cứng vào ứng dụng hoặc truy xuất tại thời điểm thiết lập kết nối SSL/TLS với Web Server hoặc API.	Không ảnh hưởng đến ứng dụng
	Testing the Network Security Configuration Settings	Nhà thầu kiểm tra hỗ trợ phiên bản Android và an toàn dữ liệu truyền thông qua cấu hình bảo mật mạng được hỗ trợ đối với phiên bản Android 7 trở lên (nếu ứng dụng có hỗ trợ.	Không ảnh hưởng đến ứng dụng
	Testing the Security Provider	Android dựa vào nhà cung cấp bảo mật để cung cấp các kết nối mã hoá dựa theo giao thức SSL / TLS. Tuy nhiên phần lớn các thiết bị chưa được cập nhật để vá lỗ hổng liên quan OpenSSL. Để tránh các lỗ hổng đã biết, các nhà phát triển cần đảm bảo rằng ứng dụng sẽ được cài đặt một nhà cung cấp bảo mật thích hợp. Nhà thầu kiểm tra ứng dụng có cơ chế kiểm tra hoặc xử lý lỗi khi chạy trên các thiết bị chưa có bản vá liên quan tới lỗ hổng trên thư viện OpenSSL bằng cách kiểm tra mảng trả về trong Class java.security.Security tồn tại giá trị “GmsCore_OpenSSL”	Không ảnh hưởng đến ứng dụng
Nhóm	**Kịch bản**	**Mô tả chi tiết**	**Phạm vi ảnh hưởng**

Nền tảng iOS	Test App Transport Security Configuration	App Transport Security (ATS) là một thiết lập kiểm tra bảo mật mà hệ điều hành thực thi khi thực hiện kết nối NSURLConnection, NSURLSession và CFURL với tên máy chủ công cộng. ATS được kích hoạt theo mặc định đối với các ứng dụng được xây dựng dựa trên iOS SDK 9 trở lên. Kết nối được thực hiện với địa chỉ IP, tên miền không đủ điều kiện hoặc TLD của .local đều không được bảo vệ bằng ATS. Danh sách tóm tắt các yêu cầu bảo mật khi thực hiện trao đổi dữ liệu trên ứng dụng: + Không cho phép kết nối HTTP + Chứng chỉ X.509 phải có SHA-256 fingerprint và tối thiểu nhất là phải được ký bằng khóa RSA 2048 bit hoặc khóa mã hóa Elliptic-Curven (ECC) 256 bit. + Phiên bản TLS của Transport Layer Security phải từ 1.2 trở lên và phải hỗ trợ Bảo mật Chuyển tiếp Hoàn hảo (PFS) thông qua Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) và trao đổi khóa AES-128 hoặc AES-256. + Nhà thầu kiểm tra cấu hình cho phép chấp nhận hoặc bỏ qua kiểm tra chữ ký số trong cấu hình ATS.	Không ảnh hưởng đến ứng dụng
	Testing Custom Certificate Stores and Certificate Pinning	Certificate pinning là quá trình liên kết ứng dụng di động với chứng chỉ X.509 của máy chủ, thay vì chấp nhận bất kỳ chứng chỉ nào được ký bởi cơ quan chứng nhận tin cậy. Khi thực hiện cơ chế Pinning, ứng dụng phải tự kiểm tra chính xác chứng chỉ máy chủ hoặc định danh chứng chỉ của máy chủ mong muốn. Chứng chỉ có thể được Pinning và mã hóa cứng vào ứng dụng hoặc truy xuất tại thời điểm thiết lập kết nối SSL/TLS với Web Server hoặc API.	Không ảnh hưởng đến ứng dụng

2.5. KIỂM TRA TƯƠNG TÁC NỀN TẢNG ỨNG DỤNG

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Client Side Code	Testing App Permissions	Kiểm tra, đánh giá các quyền cần cấp cho ứng dụng. Đảm bảo ứng dụng chỉ cần các quyền cần thiết và phù hợp với các tác vụ của ứng dụng	Không ảnh hưởng đến ứng dụng
	Testing Custom URL Schemes	Kiểm tra khi ứng dụng đăng ký với hệ thống các URL Schema dùng để trao đổi	Không ảnh hưởng đến ứng dụng

		thông tin hoặc gọi từ các ứng dụng khác trong hệ thống, các URL này dựa theo các tham số đầu vào để thực hiện nhiều xử lý ngầm bên trong ứng dụng. Kiểm tra khả năng lợi dụng tham số để thực thi các hàm không cần chứng thực. Kiểm tra khả năng phá vỡ các nghiệp vụ quan trọng khi tương tác các URL Schema.	
	Testing for Sensitive Functionality Exposure Through IPC	Liệt kê cơ chế IPC được định nghĩa trong ứng dụng bao gồm Activity, Service, Content Provider, Broadcast Receiver. Kiểm tra các dữ liệu được xử lý, xác định các thông tin nhạy cảm có thể bị leak	Không ảnh hưởng đến ứng dụng
	Testing JavaScript Execution in Web Views	Kiểm tra khả năng thực thi mã nguồn Javascript trong WebView, nên tắt tính năng này để đảm bảo an toàn. Đối với trường hợp cần thực thi Javascript, cần đảm bảo kênh truyền là HTTPS để bảo vệ mã nguồn HTML và Javascript và các mã nguồn này chỉ nên được tải từ nội bộ hoặc từ các nguồn an toàn	Không ảnh hưởng đến ứng dụng
	Testing WebView Protocol Handlers	Kiểm tra các thiết lập quyền truy cập của WebView, đảm bảo chỉ cho phép các quyền cần thiết và phù hợp với các tác vụ của ứng dụng	Không ảnh hưởng đến ứng dụng
	Testing for Java Objects Exposed Through Web Views	Kiểm tra khả năng thực thi các hàm hệ thống thông qua Javascript trên WebView. Đảm bảo chỉ cho phép các mã nguồn được phát triển kèm ứng dụng được thực hiện chức năng này.	Không ảnh hưởng đến ứng dụng
	Testing Object Persistence	Kiểm tra các đối tượng được serialize/deserialize, đối với các đối tượng có chứa thông tin nhạy cảm cần đảm bảo mã hóa hoặc ký sau khi đã serialize và khóa mã hóa cần được quản lý truy cập chặt chẽ. Ngoài ra kiểm tra việc sàng lọc dữ liệu của đối tượng sau khi đã deserialize	Không ảnh hưởng đến ứng dụng

2.6. KIỂM TRA CHẤT LƯỢNG MÃ NGUỒN VÀ CẤU HÌNH

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Code Quality	Testing App Signature	Kiểm tra chữ ký của tập tin APK, khả năng	Không ảnh hưởng đến ứng dụng
	Testing Ability to Debug App	Kiểm tra cấu hình cho phép sử dụng Debug trong AndroidManifest.	Không ảnh hưởng đến ứng dụng
	Testing for Debugging Code and Verbose Error Logging	Kiểm tra cờ Debug và các cơ chế ghi nhật ký các lỗi trong hệ thống, trong quá trình vận hành.	Không ảnh hưởng đến ứng dụng

	Testing for Injection Flaws	Kiểm tra tồn tại các lỗ hổng thông qua các Schema được dùng trong ứng dụng. Sử dụng các ứng dụng Custom, gọi và truyền các tham số kèm theo mã khai thác. Ví dụ: SQLlite Injection (chèn thêm các câu lệnh thực thi ở CSDL sqlite trên thiết bị hoặc chèn thêm các tham số vào Schema	Không ảnh hưởng đến ứng dụng
	Testing Exception Handling	Kiểm tra cơ chế bẫy lỗi trong ứng dụng khi nhận các kiểu/loại dữ liệu đầu vào không hợp lệ.	Không ảnh hưởng đến ứng dụng
	Testing for Enabled Security Features	Kiểm tra các tính năng bảo mật theo từng nền tảng được thiết lập.	Không ảnh hưởng đến ứng dụng
	Testing Weaknesses in Third Party Libraries	Kiểm tra ứng dụng sử dụng các thư viện bên ngoài tồn tại các lỗ hổng được công bố.	Không ảnh hưởng đến ứng dụng

2.7. KIỂM TRA KHẢ NĂNG CHỐNG DỊCH NGƯỢC

Danh sách các bài đánh giá:

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
Android Anti-Reversing Defenses	Testing Root Detection	Nhà thầu thực hiện kiểm tra khả năng phát hiện và khả năng vượt qua các cơ chế kiểm tra Root (đã hiện thực bởi ứng dụng).	Không ảnh hưởng đến ứng dụng
	Testing Anti-Debugging	Thực hiện kiểm tra cơ chế hạn chế ứng dụng trong quá trình chạy có thể bị attach, hook bởi các trình gỡ lỗi (debugger, ví dụ gdb, ida).	Không ảnh hưởng đến ứng dụng
	Testing File Integrity Checks	Kiểm tra cơ chế có thể tự nhận ra khả năng bị Repack bởi các công cụ decompiler như apktool. Kiểm tra khả năng có thể rebuild lại APK sau khi sử dụng các công cụ decompiler.	Không ảnh hưởng đến ứng dụng
	Testing the Detection of Reverse Engineering Tools	Nhà thầu kiểm tra khả năng phát hiện sự hiện diện của các công cụ dịch ngược trên thiết bị nhằm phân tích và điều chỉnh các luồng thực thi hoặc kẻ tấn công đang muốn dịch ngược hoặc hiểu được các luồng xử lý nghiệp vụ quan trọng trong ứng dụng.	Không ảnh hưởng đến ứng dụng
	Testing Emulator Detection	Kiểm tra khả năng phát hiện và hạn chế thực thi trong môi trường giả lập (Genymotion, Nox…).	Không ảnh hưởng đến ứng dụng
	Testing Runtime Integrity Checks	Kiểm tra khả năng phát hiện thay đổi trên bộ nhớ không mong muốn, bởi các ứng dụng bên ngoài, khả năng phát hiện các Framework như Saurik, Frida, Xposed…	Không ảnh hưởng đến ứng dụng
	Testing Device Binding	Kiểm tra khả năng sao chép, clone ứng dụng từ thiết bị A sang thiết bị B, kiểm tra khả năng ứng dụng vẫn thực thi đầy đủ	Không ảnh hưởng đến ứng dụng

Nhóm	Kịch bản	Mô tả chi tiết	Phạm vi ảnh hưởng
		các tính năng sau khi người dùng đã đăng nhập. Kiểm tra cơ chế Binding dữ liệu người dùng theo thiết bị, tránh việc tái sử dụng trên thiết bị khác.	
	Testing Obfuscation	Khi release sản phẩm, nhà phát triển không thêm vào các kỹ thuật Code Obfuscate, khiến cho kẻ tấn công có thể dễ dàng dịch ngược mã nguồn, thấy rõ các tên hàm (function) và dễ dàng đoán được chính xác các chức năng bên trong, vẽ lại luồng thực thi ứng dụng.	Không ảnh hưởng đến ứng dụng
iOS AntiReversing Defenses	Testing Jailbreak Detection	Kiểm tra khả năng ứng dụng phát hiện chạy trên thiết bị iOS đã jailbreak. Kiểm tra khả năng vượt cơ chế phát hiện thiết bị Jailbreak đã hiện thực của ứng dụng.	Không ảnh hưởng đến ứng dụng
	Testing Anti-Debugging	Thực hiện kiểm tra cơ chế hạn chế ứng dụng trong quá trình chạy có thể bị attach, hook bởi các trình gỡ lỗi (debugger, ví dụ gdb, ida, hopper). Kiểm tra khả năng vượt cơ chế Anti Debug.	Không ảnh hưởng đến ứng dụng
	Testing File Integrity Checks	Kiểm tra toàn vẹn tập tin thực thi và các tập tin quan trọng bên trong ứng dụng, sau khi biên dịch và đóng gói và thực hiện ký với chữ ký của nhà phát triển	Không ảnh hưởng đến ứng dụng
	Testing Device Binding	Kiểm tra khả năng sao chép dữ liệu từ thiết bị iOS A sang thiết bị iOS B thông qua các công cụ sao lưu như iFunBox, Backup … Kiểm tra cơ chế đảm bảo dữ liệu trên thiết bị chỉ có thể sử dụng trên thiết bị đã đăng nhập thành công	Không ảnh hưởng đến ứng dụng

3. CÔNG CỤ THỰC HIỆN

No	Nhóm công cụ	Công cụ
I	Công cụ mã nguồn mở	Nmap, Firefox addons, Grabber, Zed, Sqlmap, WebScarab, Wireshark, Mestasploit community và các công cụ khác trên HĐH Kali Linux (nền tảng kiểm thử xâm nhập nâng cao),
		Công cụ dò quét Framework: Drupal, Joomla, WordPress, …

		Dex2Jar, Android SDK, Mobile Security Framework (MobSF), Genymotion, APKInspector, IDB, apktool, Frida
II	Công cụ thương mại	Burpsuite – Công cụ kiểm thử xâm nhập ứng dụng
		Nessus – Đánh giá lỗ hổng bảo mật Ứng dụng & Hệ thống
		Hopper disassembler – Công cụ dịch ngược và debug ứng dụng di động
		Sn1per Pro – Công cụ dò quét lỗ hổng ứng dụng Web
III	Công cụ tự phát triển	Scanner & Tool - Thu thập dữ liệu cấu trúc ứng dụng web - Liệt kê các điểm nhập: URL, tham số, thông tin người dùng nhập, … - Bộ mã khai thác XSS, SQL - Xác định các thành phần thông thường dễ bị khai thác (GHDB, Module, keyword, email, comment, backup data, …) - Các mã khai thác cho các lỗ hổng nghiêm trọng: SQL Injection, Blind SQLi, XSS, Heartbleed, XPath, XXE, File Upload, File Inclusion, OS Command Injection, … và các lỗ hổng khác trong OWASP Top 10