

# BCA Finance

## ME MA Cluster KKB

### Penetration Test Mobile (Android) Report

#### Private & Confidentiality Notice

The information transmitted in this document is intended only for the addressee and may contain confidential and/or privileged material. Any interception, review, retransmission, dissemination, or other use of, or taking of any action upon this information by persons or entities other than the intended recipient is prohibited by law and may subject them to criminal or civil liability

**December 31, 2024**

Version 1.0

#### Address

Sopo Del Tower Lt.8,  
Jalan Mega Kuningan Barat III Lot 10.1-6, RT.3/RW.3,  
Kuningan Tim., Kecamatan Setiabudi, Daerah Khusus  
Ibukota Jakarta 12950

## Table of Content


<b>Table of Content</b>	<b>2</b>
<b>Document Information</b>	<b>3</b>
<b>Document Control</b>	<b>4</b>
<b>Scope of Test</b>	<b>5</b>
<b>Executive Summary</b>	<b>6</b>
<b>Findings Table</b>	<b>7</b>
<b>Findings Detail</b>	<b>8</b>
<b>Additional Information</b>	<b>9</b>
1. Segmentasi - HNWI	9
2. Segmentasi - Affluent	11
3. Segmentasi - Uppermass	13
4. Segmentasi - Mass	15
5. Segmentasi - Tidak Tersegmentasi	17
<b>Manday Information</b>	<b>19</b>
<b>Glossary</b>	<b>20</b>
<b>Mobile Application Security Testing Checklist - Android</b>	<b>24</b>
1. Storage	24
2. Crypto	25
3. Auth	26
4. Network	27
5. Platform	28
6. Code	29
7. Resilience	30
8. API	31

## Document Information

Assessment Information		
Assessors		Client
Jakson Simamora  security@glair.ai		BCA Finance  Wisma BCA Pondok Indah Lt. 2 Jalan Metro Pondok Indah Nomor 10 Jakarta Selatan 12310
Project Manager		Client Contact
Azza Amalia Rafly Dwizaputra Nikmah Salsabila  security@glair.ai		Pak Sandhy  sandhy_nasution@bcafinance.id
Assessment Type	Penetration Test Method	Assessment Period
Mobile Application Penetration Test	Whitebox	December 31, 2024
Project Number		Report Date
1224 - BCAAF - ME MA Cluster KKB - 1.0		December 31, 2024

## Document Control

Changelog				
No	Author	Date	Report Version	Notes
1	Jakson Simamora	December 31, 2024	1.0	Initial Report

Approvals			
No	Name	Title	Approved
1	Tok Sukiadi Hartono	Deputy Director IT & Business Process	
2	Nikmah Salsabila	Product Manager	

## Scope of Test

### 1. BCAAF - ME MA Cluster KKB

#### Development

1. **MA9095.apk (bca.fin)**
2. **ME16443.apk (com.emobile.mobileentry)**
  - a. `channel.trxCode.checkSegmentationDataMeLogic=CHECK_SEGMENTATI  
ON_DATA_ME`

## Executive Summary

GLAIR was contacted to perform a penetration test for **BCAF - ME MA Cluster KKB**. This report discusses the results from the assessment. Overall, there are no finding and security threats on this endpoint.

## Findings Table

---

*There are no finding and security threats on this endpoint.*

## Findings Detail

---

*There are no finding and security threats on this endpoint.*



## Additional Information

### 1. Segmentasi - HNWI

#### Description

There are no finding and security threats on this endpoint.

Tested URL(s):

1. [https://mapps.idofocus.co.id:16443/?d=\[ENCRYPTED\]&trx\\_code=CHECK\\_SEGMENTATION\\_DATA\\_ME](https://mapps.idofocus.co.id:16443/?d=[ENCRYPTED]&trx_code=CHECK_SEGMENTATION_DATA_ME)

#### PoC table

Request (Decrypted)	Response
<pre>{   "confirmPassword": null,   "desc": null,   "mSelectedItems": null,   "menu": "com.emobile.mobileentry.newapp.InitiationActivity",   "mobileId": null,   "oldPassword": null,   "password": null,   "sessionId": "eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIiX0TE2MiIsImhhdCI6MTczNTYxMDU1Mywic3ViIjoIcXNDQjZzQUEyNzk2OTYwRUUzQjcxNEExMjM0RDZBQTNFOEVEMDI4NDAA4MjJCMzRDQjRBODdDN0VBQjYxQzA3QjIiImIzcyI6ImhbmRyeV9tb3R5ImV4cCI6MTczNTYxNDU1M30.c1jVgpEcG_RSd4-C_t-S5BDA98HFuP3uZ-RlhoAcTuY",   "terms": {     "jenis_debitur": "Komersial",     "membership": "Reguler",     "segmentasi": "HNWI"   },   "trxCode": "CHECK_SEGMENTATION_DATA_ME",   "userData": {     "allRegion": 0,     "authorizedBy": 0,     "authorizeOn": null,     "branchCode": "9498",     "branchName": "KKB BANDUNG",     "branchSelected": [238],     "canExpired": 1,     "canExpiredSelect": false,     "changedPassOn": 1665138035110,     "createdBy": 11862,     "createdByDisplay": null,     "createdOn": 1665137585807,     "email": "hendry_mo@gmail.com",     "groupDesc": "Group Menu Marketing Officer",     "groupName": "N.MO",     "id": 19162,     "idGroupData": [41],     "idLevel": 30,     "idLevel2": 16,     "imei": "",     "invalidCount": 0,     "isChangedPass": 1,     "lastLoginDate": 1735610364994,     "limit": false,     "l</pre>	<pre>HTTP/1.1 200 OK Server: nginx Date: Tue, 31 Dec 2024 02:05:04 GMT Content-Type: text/plain; charset=ISO-8859-1 Content-Length: 119 Connection: keep-alive Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Referrer-Policy: same-origin Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate Content-Security-Policy: default-src * data: blob: filesystem: about: ws: wss: 'unsafe-inline' 'unsafe-eval' 'unsafe-dynamic'; script-src * data: blob: 'unsafe-inline' 'unsafe-eval'; connect-src * data: blob: 'unsafe-inline'; img-src * data: blob: 'unsafe-inline'; frame-src * data: blob: ;style-src * data: blob: 'unsafe-inline'; font-src * data: blob: 'unsafe-inline';  {"sessionId": null, "id": 12, "segmentasi":</pre>

<pre>imitCs":false,"limitKkbClusterA":false ,"limitKkbClusterB":false,"limitKkbClusterC":false,"limitKkbClusterSemiB":false,"limitValue":-1.0,"limitValueCs":0 ,"limitValueKkbClusterA":0,"limitValueKkbClusterB":0,"limitValueKkbClusterC":0,"limitValueKkbClusterSemiB":0,"positionCode":"MO","positionName":"MARKETING OFFICER","productId":2,"regionSelected":[10],"sessionId":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxOTE2MiIsImIhdCI6MTczNTYxMDM2NCwic3ViIjoqkNDQjQzQUEyNzk2OTYwRUUzQjcxNEExMjM0RDZBQTNFOEVEMDI4NDA4MjJCmZRDQjRB0DdDN0VBQjYxQzA3QiIsImIzcyI6Imh1bmRyeV9tb3R1eSImV4cCI6MTczNTYxMzk2NH0.pql69UkzSHtS7wjv4ASD-oMQI2eGK_aTzLlVS26j6PI","statusDisplay":null,"updatedBy":11862,"updatedByDisplay":null,"updatedOn":1735609881177,"userCode":"hendry_mo","userConfirmPassword":null,"userName":"hendry_mo","userPassword":"BCCB43AA2796960EE3B714A1234D6AA3E8ED02840822B34CB4A87C7EAB61C07B","userStatus":1},"userId":"hendry_mo"}</pre>	<pre>: "HNWI", "membership": "REGULER", "jenisD ebitur": "KOMERSIAL", "jenisCluster": "UP PER"} }</pre>
--	---

## 2. Segmentasi - Affluent

### Description

There are no finding and security threats on this endpoint.

Tested URL(s):

1. [https://mapps.idofocus.co.id:16443/?d=\[ENCRYPTED\]&trx\\_code=CHECK\\_SEGMENTATION\\_DATA\\_ME](https://mapps.idofocus.co.id:16443/?d=[ENCRYPTED]&trx_code=CHECK_SEGMENTATION_DATA_ME)

### PoC table

Request (Decrypted)	Response
<pre>{   "confirmPassword": null,   "desc": null,   "mSelectedItems": null,   "menu": "com.emobile.mobileentry.newapp.InitiationActivity",   "mobileId": null,   "oldPassword": null,   "password": null,   "sessionId": "eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxOTE2MiIsImhhdCI6MTczNTYxMDU1Mywic3ViIjoicQkNDQjZzQUEyNzk2OTYwRUUzQjcxNEExMjM0RDZBQTNFOEVEMDI4NDAA4MjJCMzRDQjRBODdDN0VBQjYxQzA3QiIsImZlcyI6ImhbmRyeV9tb3R5ImV4cCI6MTczNTYxNDU1M30.c1jVgpEcG_RSd4-C_t-S5BDA98HFuP3uZ-RlhoAcTuY",   "terms": {     "jenis_debitur": "Komersial",     "membership": "Reguler",     "segmentasi": "Affluent"   },   "trxCode": "CHECK_SEGMENTATION_DATA_ME",   "userData": {     "allRegion": 0,     "authorizedBy": 0,     "authorizedOn": null,     "branchCode": "9498",     "branchName": "KKB BANDUNG",     "branchSelected": [238],     "canExpired": 1,     "canExpiredSelect": false,     "changedPassOn": 1665138035110,     "createdBy": 11862,     "createdByDisplay": null,     "createdOn": 1665137585807,     "email": "hendry_mo@gmail.com",     "groupDesc": "Group Menu Marketing Officer",     "groupName": "N.MO",     "id": 19162,     "idGroupData": [41],     "idLevel": 30,     "idLevel2": 16,     "imei": "",     "invalidCount": 0,     "isChangedPass": 1,     "lastLoginDate": 1735610364994,     "limit": false,     "l</pre>	<pre>HTTP/1.1 200 OK Server: nginx Date: Tue, 31 Dec 2024 02:05:27 GMT Content-Type: text/plain; charset=ISO-8859-1 Content-Length: 123 Connection: keep-alive Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Referrer-Policy: same-origin Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate Content-Security-Policy: default-src * data: blob: filesystem: about: ws: wss: 'unsafe-inline' 'unsafe-eval' 'unsafe-dynamic'; script-src * data: blob: 'unsafe-inline' 'unsafe-eval'; connect-src * data: blob: 'unsafe-inline'; img-src * data: blob: 'unsafe-inline'; frame-src * data: blob: ; style-src * data: blob: 'unsafe-inline'; font-src * data: blob: 'unsafe-inline'; {"sessionId": null, "id": 27, "segmentasi": "Affluent", "membership": "REGULER", "jenisDebitur": "KOMERSIAL", "jenisCluster": "UPPER"}</pre>

```
limitCs":false,"limitKkbClusterA":false
,"limitKkbClusterB":false,"limitKkbClusterC":false,"limitKkbClusterSemiB":false,"limitValue":-1.0,"limitValueCs":0
,"limitValueKkbClusterA":0,"limitValueKkbClusterB":0,"limitValueKkbClusterC":0,"limitValueKkbClusterSemiB":0,"positionCode":"MO","positionName":"MARKETING
OFFICER","productId":2,"regionSelected":
":[10],"sessionId":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxOTE2MiIsImIhdCI6MTczNTYxMDM2NCwic3ViIjoiaQkNDQjQzQUEyNzk2OTYwRUUzQjcxNEEzMjM0RDZBQTNFOEVEMDI4NDA4MjJCmZRDQjRBODdDN0VBQjYxQzA3QiIsImIzcyI6Imh1bmRyeV9tb3R1eSImV4cCI6MTczNTYxMzk2NH0.pql69UkzSHtS7wjv4ASD-oMQI2eGK_aTzLlVS26j6PI","statusDisplay":null,"updatedBy":11862,"updatedByDisplay":null,"updatedOn":1735609881177,"userCode":"hendry_mo","userConfirmPassword":null,"userName":"hendry_mo","userPassword":"BCCB43AA2796960EE3B714A1234D6AA3E8ED02840822B34CB4A87C7EAB61C07B","userStatus":1
},"userId":"hendry_mo"}
```

## Description

Tested URL(s):

1. [https://mapps.idofocus.co.id:16443/?d=\[ENCRYPTED\]&trx\\_code=CHECK](https://mapps.idofocus.co.id:16443/?d=[ENCRYPTED]&trx_code=CHECK)  
SEGMENTATION DATA ME

Request (Decrypted)	Response
<pre>{"confirmPassword":null,"desc":null,"mSelectedItems":null,"menu":"com.emobile.mobileentry.newapp.InitiationActivity","mobileId":null,"oldPassword":null,"password":null,"sessionId":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxOTE2MiIsImhhdCI6MTczNTYxMDU1Mywic3ViIjoiaQNDQjZzQUEyNzk2OTYwRUUzZjcxeEEtMjM0RDZBQTNEOEVEVEMDI4NDAMjJCMzRDQjRBOddDN0VBQjYxQzA3QiIsImVudCI6Imh1bmRyeV9tbSIsImV4cCI6MTczNTYxNDE1M30.c1jVgpEcG_RSd4-C_t-S5BDA98HFuP3uZ-RlhoAcTuY"},"terms":{"jenis_debitur":"Komersial","membership":"Reguler","segmentasi":"Uppermass"},"trxCode":"CHECK_SEGMENTATION_DATA_ME","userData":{"allRegion":0,"authorizedBy":0,"authorizedOn":null,"branchCode":"9498","branchName":"KKKBANDUNG","branchSelected":[238],"canExpired":1,"canExpiredSelect":false,"changedPassOn":1665138035110,"createdBy":11862,"createdByDisplay":null,"createdOn":1665137585807,"email":"hendry_mo@gmail.com","groupDesc":"Group Menu Marketing Officer","groupName":"","NO.MO"},"id":19162,"idGroupData":[41],"idLevel":30,"idLevel2":16,"imei":"","invalidCount":0,"isChangedPass":1,"lastLoginDate":1735610364994,"limit":false,"limitCs":false,"limitKkbClusterA":false,"limitKkbClusterB":false,"limitKkbClusterC":false,"limitKkbClusterSemiB":false,"limitValue":-1.0,"limitValueCs":0}</pre>	<pre>HTTP/1.1 200 OK Server: nginx Date: Tue, 31 Dec 2024 02:32:41 GMT Content-Type: text/plain; charset=ISO-8859-1 Content-Length: 124 Connection: keep-alive Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Referrer-Policy: same-origin Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate Content-Security-Policy: default-src * data: blob: filesystem: about: ws: wss: 'unsafe-inline' 'unsafe-eval' 'unsafe-dynamic'; script-src * data: blob: 'unsafe-inline' 'unsafe-eval'; connect-src * data: blob: 'unsafe-inline'; img-src * data: blob: 'unsafe-inline'; frame-src * data: blob; ;style-src * data: blob: 'unsafe-inline'; font-src * data: blob: 'unsafe-inline'; {"sessionId":null,"id":57,"segmentasi":"Uppermass","membership":"REGULER","jenisDebitur":"KOMERSIAL","jenisCluster":"UPPER"}</pre>





<pre>KkbClusterB":0,"limitValueKkbClusterC":0,"limitValueKkbClusterSemiB":0,"positionCode":"MO","positionName":"MARKETING OFFICER","productId":2,"regionSelected":[10],"sessionId":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiIxOTE2MiIsImIhdCI6MTczNTYxMDM2NCwic3ViIjoicQkNDQjQzQUEyNzk2OTYwRUUzQjcxNEExMjM0RDZBQTNFOEVEMDI4NDA4MjJCMzRDQjRBODdDN0VBQjYxQzA3QiIsImIzcyI6Imh1bmRyeV9tb3R5ImV4cCI6MTczNTYxMzk2NH0.pql69UkzSHtS7wjv4ASD-oMQI2eGK_aTzLLVS26j6PI","statusDisplay":null,"updatedAt":11862,"updatedByDisplay":null,"updatedAtOn":1735609881177,"userCode":"hendry_mo","userConfirmPassword":null,"userName":"hendry_mo","userPassword":"BCCB43AA2796960EE3B714A1234D6AA3E8ED02840822B34CB4A87C7EAB61C07B","userStatus":1},"userId":"hendry_mo"}</pre>	
--	--







## Manday Information

No	Activity	Total Member	Duration (day)	Report Date	Total Mandays
1.	Penetration Test + Report	1	1	Dec 31, 2024	1
Total					1

## Glossary

1. **Penetration Test:** used to evaluate the security of a computer system and network by doing a simulation cyberattack.
2. **Penetration Test Method:**
  - a. **Blackbox Testing:** a method where the tester is not given any information, either infrastructure or source code for the system to be tested.
  - b. **Gray Box Testing:** a method where the tester is given some information about the system to be tested.
  - c. **Whitebox Testing:** a method where a tester has been given all the information or full access needed to perform a penetration test.
3. **Scope of Test:** a collection of systems/endpoints that are included in the scope to perform penetration testing.
4. **Classification:** a systematic arrangement in groups established to help understand.
5. **CVSS Score:** a measurement value used by various individuals/agencies to assess vulnerability to the system. CVSS will judge from a score of 0-10 which will be divided into 4 aspects, namely Low (0.0 - 3.9), Medium (4.0 - 6.9), High (7.0-8.9), and Critical (9.0 - 10.0).
6. **Severity:** an assessment of test results based on the CVSS score. The severity level is divided into 5 levels, the addition of "Informational" as a result of the findings is only informational and does not have a dangerous risk.

Severity	Definition	Color Code
Critical	The issues marked as Critical Severity can allow attackers to execute code on the web	#ff725e

	application or application server, or access sensitive data.	
High	<p>The issues marked as High Severity can allow malicious attackers to access application resources and data. This can allow an attacker to steal session information or sensitive data from the application or server.</p> <p>The difference between a Critical and High Severity is that with a High Severity vulnerability, a malicious attacker cannot execute code or a command on the application or server.</p>	#f4b965
Medium	<p>The issues marked as Medium Severity usually arise because of errors and deficiencies in the application configuration. By exploiting these security issues, malicious attackers can access sensitive information on the application or server.</p>	#efe47d
Low	<p>The issues marked as Low Severity include information leakage, configuration errors and a lack of some security measures. They can be combined with other issues of a higher severity level, and can be used in conjunction</p>	#d4d4d4

	with social engineering (manipulating people into following certain actions or revealing crucial information), to cause a more severe impact on the target.	
Informational	The findings reported are mostly for informing you about the target's ingredients and infrastructure. They help you to understand the application's technology stack and dependencies well.	#ececec

7. **Status:** a marker for previously obtained findings.

Status	Definition	Color
Present	This indicates that the Issue has been present	#ff0000
Partial Fixed	This indicates that the Issue has been fixed partially	#ff9900
Fixed	This indicates that the Issue has been fixed and confirmed by pentester, and so requires no further action	#5faf27
Accepted Risk	This indicates that the Issue has been considered and is marked as a low risk vulnerability.	#999999

Mitigated	This indicates that the Organization has taken temporary measures to reduce the risk of exploitation until a permanent fix can be implemented.	#161e44
Ignored	It is said to be "Ignored" if the findings previously obtained are not related/not part of the scope of the test. This indicates that the Issue was ignored by the user	#990000
Revived	This indicates that the issue had been fixed in previous scans but revived again	#ffff00

8. **OWASP** : a non-profit organization focused on web app security which is the world's standard for web app security.

# Mobile Application Security Testing Checklist - Android

## 1. Storage

No	Test Name	Checklist	Vulnerable	Notes
1	Testing Local Storage for Sensitive Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Testing Logs for Sensitive Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Determining Whether Sensitive Data Is Shared with Third Parties via Embedded Services	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Determining Whether Sensitive Data Is Shared with Third Parties via Notifications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Determining Whether the Keyboard Cache Is Disabled for Text Input Fields	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Testing Backups for Sensitive Data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Testing Memory for Sensitive Data	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope
8	Testing the Device-Access-Security Policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



## 2. Crypto

No	Test Name	Checklist	Vulnerable	Notes
1	Testing Symmetric Cryptography	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Bypassed for testing purposes
2	Testing the Configuration of Cryptographic Standard Algorithms	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Testing the Purposes of Keys	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Testing Random Number Generation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

### 3. Auth

No	Test Name	Checklist	Vulnerable	Notes
1	Testing Confirm Credentials	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope
2	Testing Biometric Authentication	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope

#### 4. Network

No	Test Name	Checklist	Vulnerable	Notes
1	Testing Data Encryption on the Network	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Testing the TLS Settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Testing Endpoint Identify Verification	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Testing Custom Certificate Stores and Certificate Pinning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Bypassed for testing purposes
5	Testing the Security Provider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

## 5. Platform

No	Test Name	Checklist	Vulnerable	Notes
1	Determining Whether Sensitive Stored Data Has Been Exposed via IPC Mechanisms	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Checking for Sensitive Data Disclosure Through the User Interface	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Finding Sensitive Information in Auto-Generated Screenshots	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Testing for App Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Testing Deep Links	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope
6	Testing for Sensitive Functionality Exposure Through IPC	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Testing for Vulnerable Implementation of PendingIntent	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope
8	Testing JavaScript Execution in WebViews	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope
9	Testing WebView Protocol Handlers	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope
10	Testing for Java Objects Exposed Through WebViews	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope
11	Testing for Overlay Attacks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Testing WebViews Cleanup	<input type="checkbox"/>	<input type="checkbox"/>	Out of scope

## 6. Code

No	Test Name	Checklist	Vulnerable	Notes
1	Testing Local Storage for Input Validation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Testing for Injection Flaws	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Testing Implicit Intents	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Testing for URL Loading in WebViews	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Out of scope
5	Testing Object Persistence	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Testing Enforced Updating	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Out of scope
7	Checking for Weaknesses in Third Party Libraries	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Memory Corruption Bugs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Out of scope
9	Make Sure That Free Security Features Are Activated	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Out of scope

## 7. Resilience

No	Test Name	Checklist	Vulnerable	Notes
1	Making Sure that the App is Properly Signed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Out of scope
2	Testing whether the App is Debuggable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Out of scope
3	Testing for Debugging Symbols	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Testing for Debugging Code and Verbose Error Logging	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Testing Root Detection	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Bypassed for testing purposes
6	Testing Anti-Debugging Detection	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Bypassed for testing purposes
7	Testing File Integrity Checks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Testing Reverse Engineering Tools Detection	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Testing Emulator Detection	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Bypassed for testing purposes
10	Testing Runtime Integrity Checks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Testing Obfuscation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Out of scope

## 8. API

No	Test Name	Checklist	Vulnerable	Notes
1	Broken Object Level Authorization	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Broken Authentication	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Broken Object Property Level Authorization	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Unrestricted Resource Consumption	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Broken Function Level Authorization	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Unrestricted Access to Sensitive Business Flows	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Server Side Request Forgery	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Security Misconfiguration	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Improper Inventory Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Unsafe Consumption of APIs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	