Mobile Application Security Testing

2/4/24

Android OS

Authored by: Subhajit Mondal

Contents

Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of INFOPERCEPT. Nothing contained in this document shall be construed as conferring by implication, estoppels, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of INFOPERCEPT or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of INFOPERCEPT. Any use you make of the information provided, is at your own risk and liability. Document Authorities

INFOPERCEPT makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and INFOPERCEPT shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and INFOPERCEPT agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

This report is being supplied by us on the basis that it is for your benefit and information only and that, save as may be required by law or by a competent regulatory authority (in which case you shall inform us in advance), it shall not be copied, referred to or disclosed, in whole (save for your own internal purpose) or in part, without our prior written consent. The report is submitted on the basis that you shall not quote our name or reproduce our logo in any form or medium without prior writtenconsent. You may disclose in whole this report to your legal and other professional advisers for the purpose of your seeking advice in relation to the report, provided that when doing so you inform them that:

- Disclosure by them (save for their own internal purposes) is not permitted without our prior written consent, and
- To the fullest extent permitted by law we accept no responsibility or liability to them in connection with this report.

Any advice, opinion, statement of expectation, forecast or recommendation supplied or expressed by us in this report is based on the information provided to us and we believe such advice, opinion, statement of expectation, forecast or recommendation to be true. However, such advice, opinion, statement of expectation, forecast or recommendation shall not amount to any form of guarantee that we have determined or predicted future events or circumstances but shall ensure accuracy, competency, correctness or completeness of the report based on the information provided to us.

Company	ABC Corporation Ltd.
Document Title	Mobile Application Penetration Testing
Date	03/04/2024
Reference	Security Assessment
Scope	As defined in the document
Classification	☐ Public ☐ Internal ☐ Confidential ☐ Secret
Document	☐ Proposal ☐ Deliverable ☐ General

Recipients

Name	Title	Company
Mr. XYZ	Chief Information Security Officer	ABC Corporation Ltd.

Document History

Date	Version	Prepared by	Status
02/04/2024	1.0	ABC	Draft Report
03/04/2024	1.1	ABC	Final Report

1. Executive Summary

1.1 Introduction

INFOPERCEPT Conducted Vulnerability Assessment and Penetration Testing Assessment for Mobile Application of ABC. The assignment was carried out by INFOPERCEPT technical team between 5th JULY 2018 to 8th JULY 2018 with the following goals:

- Identifying security vulnerabilities
- Providing risk mitigation recommendations for the discovered vulnerabilities.

This audit report contains:

- The description of the scope and its business case
- The security vulnerabilities discovered as a result of the technical assessment
- The risk mitigation strategies that need to be implemented to ensure that the ABC meets information security compliance.

1.2 Scope of the Audit

The Security audit has been conducted to provide a holistic picture of Security of ABC's Mobile Application.

Bearing this in mind the audit was conducted with below approach:

TECHNICAL AUDIT

The objective of this phase is to identify and provide remedies for all technical vulnerabilities in the scope defined. The idea behind this audit is to discover whether an attacker can leverage flaw and compromise the confidentiality, integrity or availability of ABC.

As the client side of the application will be operated by semi-trusted third parties. Specific attention has been given to the security mechanisms of the client application and the potential damage a malicious third party could cause, by exploiting flaws in the client-server architecture.

The technical audit was conducted as a 'black-box' exercise, implying that the auditors were not given access to the source-code of the application, nor were they given any special privileges to connect to the application. This was done to simulate, as closely as possible, the access level granted to a normal user of the application.

The security of the application was audited to ensure that confidentiality, integrity and availability ABC. Critical information is maintained, and sufficient audit-trails are created during the normal use of the application.

1.3 Summary of the Findings

ABC.'s Mobile Application has been found with multiple security issues in its design, platforms and deployments. These issues could seriously compromise the confidentiality, integrity and availability of the systems and the data residing on these systems.

Making use of vulnerabilities in the application, network and OS, an attacker could compromise and take full control of the application. This implies that the attacker could, among other things,

- Steal and/or modify confidential information
- Poison legitimate transactions
- Caused denial-of-service conditions and prevent legitimate use of the application

It must be emphasized that, these attacks could be carried out not just by a malicious user of the application but also by any external attacker as well an insider, operating remotely over the Internet or a similar communications channel inside the local network.

A few of the targets have not been scanned despite of several attempts due to infrastructure limitations at the hosting provider.

1.4 Recommendations Summary

INFOPERCEPT's consultants have addressed each of the identified security concerns and provided recommendations to mitigate the risk involved.

2. ABC Company

2.1 Introduction of ABC

ABC is an independent, international insurance and reinsurance broker headquartered within the XXX Insurance Market. ABC is an accredited XXX.

Employing more than 20 nationalities within the ABC group, we benefit from an exceptionally culture sensitive team. With our staff fluent in over 16 languages, we are able to communicate freely with our global clientele.

ABC offers extensive expertise in all the major insurance disciplines:

- Aviation & Space
- Construction
- Corporate & Commercial
- Energy
- Marine
- Non-Marine
- Treaty Reinsurance

The trained and highly motivated staff at ABC provides comprehensive, cost effective and specially crafted insurance programmers that meet the insurance and risk management requirements of our clients.

As an international broking firm, ABC has strategic owned and partner offices located around the globe enabling ABC to meet its clients' needs no matter what time zone they are in.

Detailed Vulnerability Information

Following are the technical details of vulnerabilities discovered in the Scope of Assessment

Vulnerability Information:

Below is the vulnerability table

Compliance of IP Address:	
Risk	
Abstract	
IPMG Control Violation	
Reference	
Ease of Exploitation	
Impact	
Recommendations	
Remark	
References	

Vulnerability Title – A short title that describes the vulnerability.

For each vulnerability, the title bar is color coded for a quick identification of the risk level. Title bar color codes are as follows:

Risk Level & Color Code

- **Abstract –** Describes the flaw or bugs that cause the vulnerability.
- **Reference -** Describes the reference for the respective vulnerability found.
- **Ease of Exploitation –** Provides a metric for the skill level required to exploit the vulnerability.

The categories are:

Metric Skill-level	Metric Skill-level
Easy	Casual user
Medium	Computer-savvy individual
Hard	Determined hacker

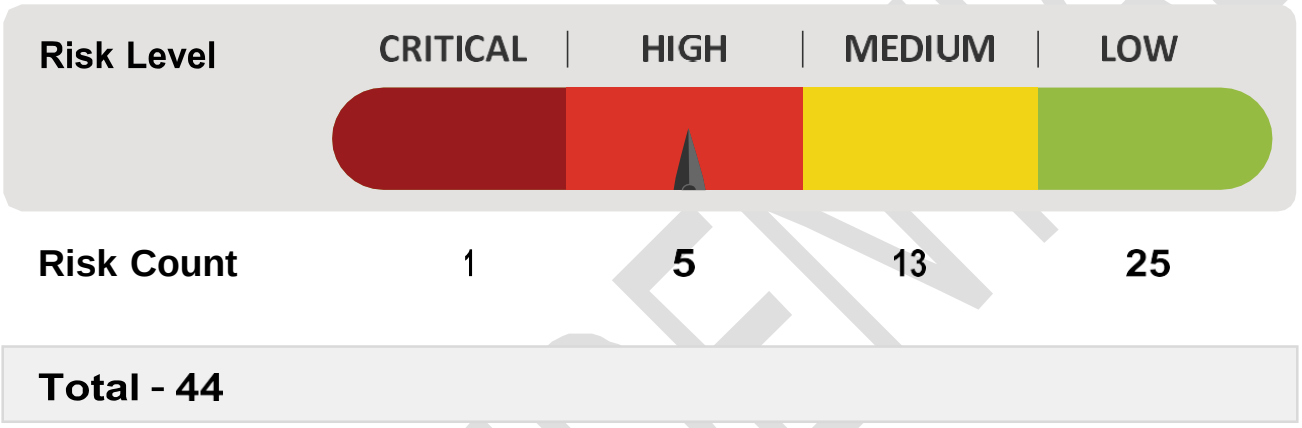
- **Impact -** Describes the possible business impact to ABC if this vulnerability is successfully exploited by an attacker.
- **Recommendation -** Provides solutions or workarounds to mitigate the risk arising from this vulnerability.
- **Proof of Concept -** Screenshots / supporting evidence showing the vulnerability being exploited.

2.2 List of Mobile Applications (.APK & IPA) in the scope of Assessment of ABC

The following list defines the systems to scan for vulnerabilities:

Sr. No	IP Addresses Range
01	/data/data/com.xyz/
02	Possible Filter-Bypass via unsafe URL check

Vulnerability overview (Management Summary Dashboard)



3. Vulnerabilities Discovered / Compliance Ip Of Each Ip Address Under Scope

3.1 Possible Remote Code Execution via MitM in WebView

Compliance of IP Address: /data/data/com.xyz /	
Risk	Possible Remote Code Execution via MitM in WebView
Severity	Critical
Vulnerability Description	After downloading the APK and decompiling the DEX file, a simple fulltext search unveiled the first critical security issue. This vulnerability allows an attacker to get control over a phone running the xyz app by abusing insecure usage of Android's JavaScript Interfaces for WebViews
System Details	/data/data/com.xyz /
Ease of Exploitation	Hard
Recommendations	Given that all network traffic between the app and the MOIB API servers is locked to use HTTP, a MitM attack5 can be trivially executed by any attacker who manages to lure a victim into a malicious WiFi network.
Remark	Object objl = "http://xyz.moib.org/pushAlarm"; _L6: WebView webview = (WebView)findViewByld(0x7f070000); webview.setWebViewClient(new l(this)); webview.getSettings().setJavaScriptEnabled(true); webview.getSettings().setSavePassword(false); webview.getSettings().setSaveFormData(false); webview.addJavascriptInterface(new JavaScriptInterface(), "xyz"); webview.setWebChromeClient(new org.co.wigsys.xyz.ui.f(this)); webview.postUrl(((String) (objl)), ((String) (obj)).getBytes());
References	N/A

3.2 Possible Filter-Bypass via unsafe URL check:

Compliance of IP Address: /data/data/com.xyz /	
Risk	Possible Filter-Bypass via unsafe URL check
Severity	High
Vulnerability Description	The app uses a WebView method called shouldOverrideUrlLoading()7 to determine whether a URL should be loaded or blocked. This method is implemented in a vulnerable way because it checks the URL string for certain values and makes use of the string- method contains().8 This means that any URL, even if blacklisted, can be requested, as long as the string xyz.moib.org is simply attached. Then, the contains() method call will return a true and the URL will be considered whitelisted.
System Details	/data/data/com.xyz /
Ease of Exploitation	Hard
Recommendations	The way this test is being constructed shows that the blacklisting feature was not built with security in mind. Trivial bypasses like this imply a lack of understanding regarding how URLs and filters work
Remark	function shouldOverrideUrlLoading: s.s tartsWith("market://") || s.startsWith("tel:") || s.startsWith("http") && ! s.contains("xyz.mobi.org")

3.3 Test-Page leaks Application-Internals

Compliance of IP Address: Test-Page leaks Application-Internals	
Risk	Test-Page leaks Application-Internals
Severity	Medium
Vulnerability Description	The websites and web services the app communicates with are riddled with pointers and URLs exposing debug pages, test- pages and similar clutter that should never be published on a production system.
System Details	Test-Page leaks Application-Internals
Ease of Exploitation	Hard
Impact	Medium
Recommendations	Among the highlighted parts the URL http://xyz.moib.org./html/filelist.html is considered most interesting. This is due to the fact that it is available without any authentication and reveals a large amount of information.
Remark	‹li›‹a href='/index'›abc‹/a›‹/li› ‹li›‹a href='/subMain'›xyz‹/a›‹/li› ‹li›‹a href='/harm/app/list'›abc‹/a› ‹li›‹a href="/harm/app/appList"›xyz‹/a›‹/li› ‹li›‹a href="/harm/site/list"›abc‹/a›‹/li› ‹li›‹a href="/harm/accept/acceptList_app"›xyz‹/a›‹/li› ‹li›‹a href='/member/admin/memberAdm'›abc‹/a› ‹li›‹a href='/minwon/minwonList'›xyz‹/a› ‹li›‹a href='/home/report/list'›xyz‹/a›‹/li› ‹p› ‹a href='/html/filelist.html'›xyz‹/a›‹br/›‹br/› ‹a href='/minwon/minwonPushTest'›Push TEST‹/a›‹br/›‹br/› ‹a href='/minwon/livePushTest'›Live Push TEST‹/a›‹br/› ‹a href="minwon/logPushTest"›log Push Test‹/a›‹/br› </p> </body> </html>
References	'http://xyz.moib.org/'sample 'http://xyz.moib.org/' sample

4. AUDITOR'S END NOTES

During course of the audit, the auditors identified certain points that could be potential security concerns. This activity is done considering the scope, boundary and defined timeline, as this is a business-critical application it is highly recommended to conduct the assessment at regular interval based recommended every quarter. This section gives a brief description of each of the vulnerability reported and column to submit the retest report once the patching is done by the development team:

ACTION ITEMS AND RETEST COMPLIANCE CHECK

No.	Vulnerability Details	Responsibility to close	Time-line	Rating Comply (Y / N)
01				
02				
03				
04				
05				
06				
07				
08				
09				
10				

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accrditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for yourspecific business needs exactly the way you want it to be.