**web vapt**

**Synopsis:**

As part of the service requested by the Infrastructure Owner or their representative, this report outlines the vulnerabilities that were identified for wifi--web vapt engagement.

The gj hired the gj to undertake a black Box activity with the provided scope.

The goal of this evaluation was to detect web app security concerns that could have a detrimental impact on gj company or reputation if they resulted in system penetration or abuse.

GJ and GJ conducted the testing from October 27 to October 28 under the supervision of Steve Wozniak.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Authors** | **Status** |
| 0.1 | 27-Oct-2024 | GJ | First partial report |
| 0.1 | 27-Oct-2024 | GJ | First release of the final report |
| 0.2 | 19-11-1976 | Steve Jobs | Peer Review |
| 1.0 | 19-11-2019 | Ada Lovelace | Final release |

**Table of Contents**

[1. Executive Summary 4](#_Toc80292021)

[1.1 Table of Findings Summary 5](#_Toc80292022)

[2. Detailed Findings 6](#_Toc80292026)

# Executive Summary

During an ongoing web vapt security assessment, gj assessed the security of the gj’s web app. The security assessment was done using none VPN provided by gj.

The following **0 critical risk, 1 high risk, 1 medium risk and 0 low risk** issues were found. The activity was performed from **October 27** to **October 28**.

**HIGH Risk(s)**

The following vulnerabilities account for the HIGH-risk findings:

|  |
| --- |
| Insecure deeplink leads to sensitive information disclosure ::: A deeplink feature was found missing validation that led to sensitive information disclosure. Once triggered, the deeplink would direct users to load any attacker-controlled URL within a webview. |

**MEDIUM Risk(s)**

The following vulnerabilities account for the MEDIUM--risk findings:

|  |
| --- |
| Activity is vulnerable to Local file Stealing ::: Activity is set to exported so external app can communicate with it. As this activity doesn't validate data pass through intent critical uri like javascript and file so malicious app can steal users files as well as inject javascript. It can leads to many issue like UXSS, Token steal, etc. |

## Table of Findings Summary

|  |  |  |
| --- | --- | --- |
| Serial No | Finding | Risk |
| 1.0 | Insecure deeplink leads to sensitive information disclosure | HIGH |
| 1.1 | Activity is vulnerable to Local file Stealing | MEDIUM |



# Findings



The complete descriptions of security issues discovered throughout the assessment are listed below.

## Insecure deeplink leads to sensitive information disclosure

|  |  |  |  |
| --- | --- | --- | --- |
| **SEVERITY** | HIGH | **IMPACT** | HIGH |
| **LIKELIHOOD** | MEDIUM |

### Description of Finding

A deeplink feature was found missing validation that led to sensitive information disclosure. Once triggered, the deeplink would direct users to load any attacker-controlled URL within a webview.

### POC

The screenshot(s) below show the Insecure deeplink leads to sensitive information disclosure. Open any arbitray attacker controlled URLs .



codeblock\_1



codeblock\_2

### Remediation

set the android:autoVerify="true" in any of the web URL intent filters of your app and allows http, https schemes.

### References and additional information

* https://hackerone.com/reports/401793

## Activity is vulnerable to Local file Stealing

|  |  |  |  |
| --- | --- | --- | --- |
| **SEVERITY** | MEDIUM | **IMPACT** | HIGH |
| **LIKELIHOOD** | MEDIUM |

### Description of Finding

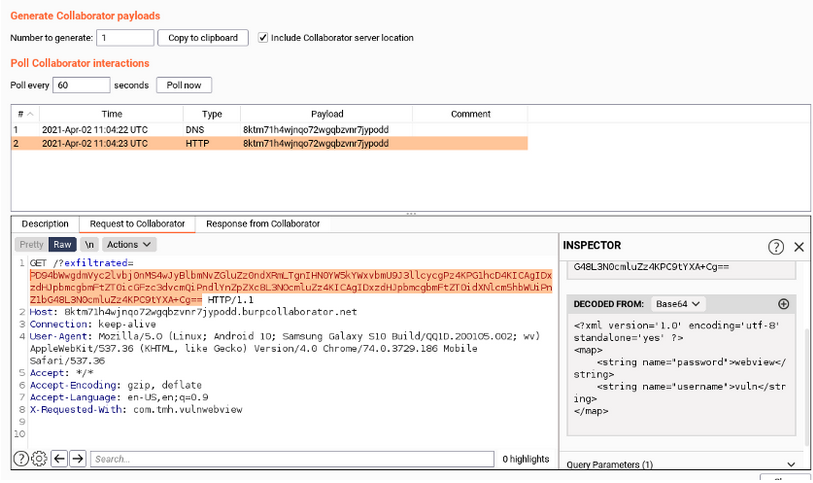
Activity is set to exported so external app can communicate with it.  
As this activity doesn't validate data pass through intent critical uri like javascript and file so malicious app can steal users files as well as inject javascript.  
It can leads to many issue like UXSS, Token steal, etc.

### POC

The screenshot(s) below show the Activity is vulnerable to Local file Stealing. As critical uri like javascript & file is not being validate malicious app can steal users session token, users files etc.



LFI\_cap\_1



LFI\_cap\_2

### Remediation

we recommend to validate the input passed to the activity.

### References and additional information

* https://hackerone.com/reports/499348