Bugsmirror Research Pvt. Ltd.

9th Floor, Unit No 905 and 906, Skye Corporate Park
Plot No 25, Scheme No 78-II, Old No 385/2, A.B. Road
Niranjanpur, Indore, Indore, Madhya Pradesh, 452010

Website : https://bugsmirror.com

RUNTIME SECURITY

TESTING REPORT

(Basic version)

Table of Contents

1. Executive Summary

1.1. Scope of Testing

Security assessment included runtime testing for security loopholes in the scope defined below.

The following was the scope covered under the runtime security testing:

Parameter	Values
Application name	**Funey Money**
Package name	**com.funeymoney.app**

1.2. Security Recommendations

The application exhibits vulnerabilities across a spectrum of High, Medium, and Low severity threats. To ensure comprehensive security and protect against potential exploitation, the following measures are strongly recommended:

- **Comprehensive Security Audit:**

  ○ Immediate Action: Conduct a thorough security audit to assess the impact of the identified threats on the application. This audit should include a detailed analysis of each vulnerability, focusing on the potential risks and the application's exposure.

  ○ Target Areas: Pay special attention to areas related to device integrity, OS integrity, secure communication, mobile privacy, mobile fraud, social engineering, and app tampering. Each of these categories contains critical threats that could significantly compromise the security of the application.

- **Implement Runtime Application Self-Protection (RASP):**

  ○ Integration: Incorporate a RASP solution like Bugsmirror Defender into the application to provide real-time threat detection and response capabilities. RASP solutions are effective in mitigating a wide range of security threats by monitoring the application's behaviour and preventing exploitation attempts in real-time.

  ○ Threat Coverage: RASP can help neutralise threats related to Root Detection, Frida Detection, Debugger Detection, and other critical 45+ such issues including few listed in the table below.

2. Key Findings

2.1 Exploitable Runtime Security Threats

Sr. No.	Threat	Attack Type	Severity	Status
1	Device Integrity	Root Detection	High	Absent
2		Emulator Detection	High	Absent
3		Frida Detection	High	Absent
4		Debugger Detection	High	Absent
5		Hooking Framework Detection	High	Absent
6		Runtime Code Injection	High	Absent
7		Unlocked Bootloader Detection	High	Absent
8		Malicious Root App Detection	Medium	Absent
9	App Tampering	App Repackaging Prevention	High	Absent
10		App Spoofing Prevention	High	Absent
11		Static App Patching Prevention	Medium	Absent
12	OS Integrity	OEM Unlock	Medium	Absent
13		ADB Wireless/USB Debugging	Low	Absent
14		Developer Mode Enable Check	Low	Absent
15		Accessibility Permission Detection	Low	Absent
16	Secure Communication	Unsecured Wifi Detection	Medium	Absent
17		Packet Sniffing Detection	Medium	Present
18		VPN Detection	Low	Absent
19	Mobile Privacy	Screen Capturing Prevention	Medium	Absent
20		Copy Paste Prevention	Medium	Absent
21		Screen Overlay Prevention	Medium	Absent
22		Screen Share Prevention	Medium	Absent
23		Device Screen Lock Enablement Check	Low	Absent
24	Mobile Fraud	App Cloning/Second Space Prevention	Medium	Absent
25		Keylogger Prevention	Medium	Absent
26		Time Manipulation	Low	Present
27	Social Engineering	Marketplace Enforcement Check	Medium	Absent

Our Clients

Google

Meta

NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

onemoney

TECNO

SAMSUNG

भारत सरकार
GOVERNMENT OF INDIA
सत्यमेव जयते

गृह मंत्रालय
MINISTRY OF **HOME AFFAIRS**
सत्यमेव जयते

Contact Bugsmirror

Get in touch

✈ sales@bugsmirror.com

🌐 www.bugsmirror.com

in www.linkedin.com/company/bugsmirror

📍 905, Skye Corporate Park, Plot no. 25,
Scheme no. 78-II (old no. 385/2), Niranjanpur
A.B. Road, Indore, Madhya Pradesh - 452010