Bugsmirror

Mobile Application Runtime Security Report

Runtime Security

What is Runtime Security?

Runtime Security refers to real-time monitoring and protection mechanisms that safeguard mobile applications during their operation. It actively detects, analyses, and mitigates threats as they arise, providing continuous protection against emerging attack vectors. To assess the presence of these attack vectors effectively, you need to perform Runtime Security Testing.

Runtime Security Testing

In today's dynamic cyber threat landscape, Runtime Security Testing is crucial for identifying vulnerabilities that emerge while an app is actively running. This testing approach helps you assess the security posture of your application and ensures you're aware of scenarios that could be exploited by attackers. It is important because:

- **Feasibility for Attackers to Bypass:** Attackers can bypass traditional static testing approaches, making it essential to test for vulnerabilities during real-time app operation i.e. real attacker scenarios .
- **Often Overlooked by Penetration Testing:** Runtime vulnerabilities might not be fully addressed by standard pentesting teams, leaving critical security gaps that could be exploited.

Bugsmirror Defender - Our Runtime Security Solution

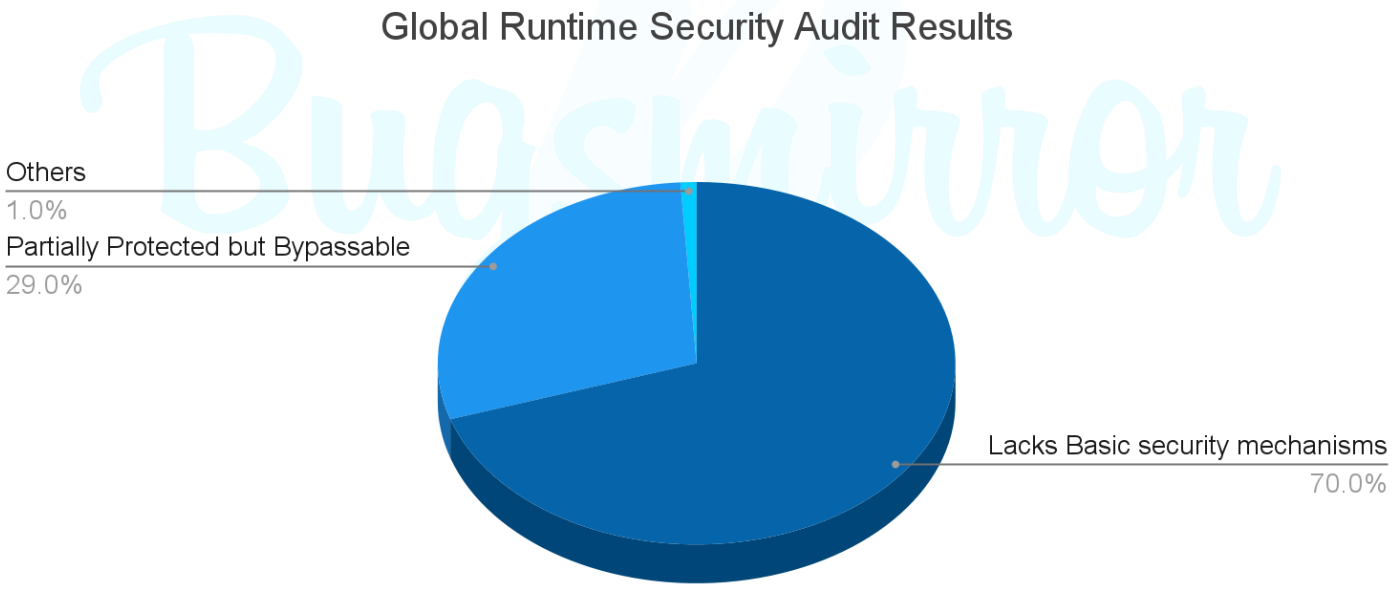
With **Bugsmirror Defender,** you not only benefit from real-time detection but also proactive mitigation of these threats, ensuring comprehensive protection for your mobile applications that provide:

Why Choose Our Runtime Security Solution?

Our Practical Analysis:

In our extensive **Runtime Security audits** of more than 300 mobile applications across the globe, we uncovered alarming trends that underscore the urgent need for stronger mobile app protection.

- **70% of the applications we tested lacked even basic security mechanisms,** leaving them wide open to various attack vectors.
- Even more concerning, the remaining **29% of companies, despite having some protection mechanisms in place, were still easily bypassable**. This means attackers can successfully compromise these apps, despite the presence of certain security measures.



These findings highlight the critical need for a robust solution like **Bugsmirror Defender**, which offers not only **real-time threat detection** but also **proactive mitigation**, ensuring that your app is not just protected but fortified against evolving threats.

1. Executive Summary

1.1. Scope of Work

The security assessment includes Runtime Security Testing to identify potential security loopholes. The following Mobile Application is considered for the Runtime Security Testing:

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

1.2. Severity Description

The following are the deciding factors for the severity rating of any vulnerability:

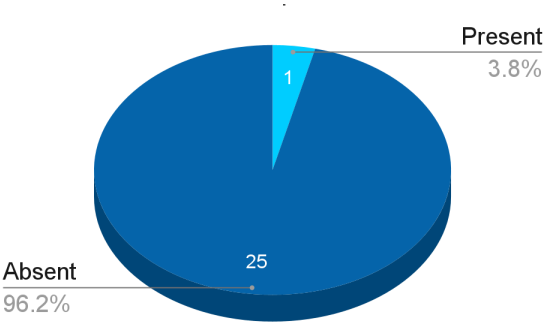
- Impact: How will the business be affected if a particular vulnerability is exploited?
- Amount of User Interaction: How much interaction of the user is required in order to exploit the vulnerability?
- OWASP MASVS: Vulnerabilities are classified based on references from **OWASP MASVS** standards.

Severity	Description
High	These are attack scenarios that compromise the overall security of the device or app, exposing sensitive data or enabling unauthorised access. These require immediate attention and mitigation.
Medium	These threats pose privacy risks or allow some level of tampering but do not immediately compromise the entire system or application.
Low	These are minor threats that pose a low risk to the app's security but could still lead to issues under certain conditions, requiring monitoring.

1.3. Current App Security Landscape

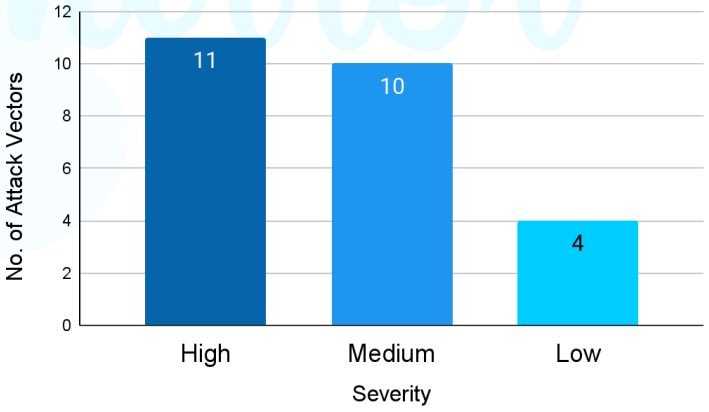
Runtime Security Parameter Status

Runtime Parameter status	Number of parameters
Present	1
Absent	25



Number of attack vectors present as per their severity

Severity	No. of Attack Vectors
High	11
Medium	10
Low	4



1.4. Ensuring Mobile App Security through RASP/App Shielding

There is no one-size-fits-all solution to mobile app security. An effective approach combines secure coding, regular penetration testing, updated APIs, encryption, robust authentication, and compliance with relevant standards. Security checklists should be customised to meet each organisation's unique requirements.

Conducting a thorough security audit is essential for identifying vulnerabilities, with a focus on risks such as device integrity, secure communication, and app tampering. By incorporating a RASP solution like Bugsmirror Defender, organisations can achieve real-time threat detection and response, effectively addressing issues like root detection, debugging, and over 45 other critical threats, as detailed in the table in the **Key findings** section of this report.

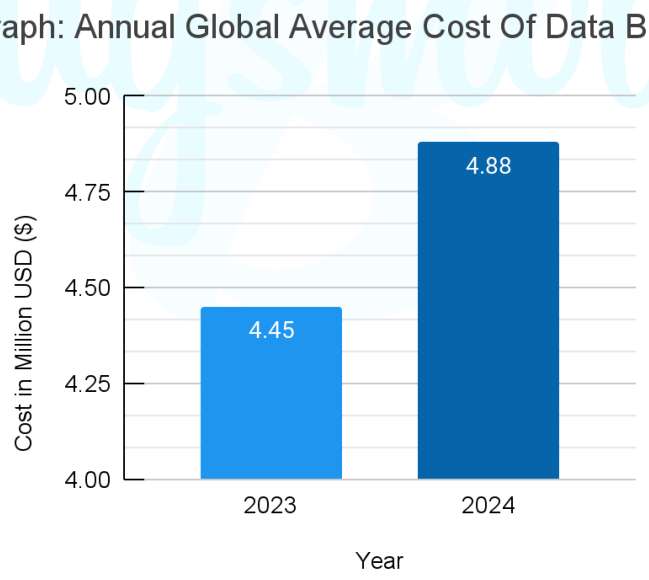
1.5. Attack Vectors and Protection Through Runtime Security

Mobile applications are susceptible to a range of vulnerabilities that span high, medium, and low severity threats. To ensure robust protection against potential exploitation, our product safeguards you from over 45 attack scenarios. While attackers may attempt to exploit these vulnerabilities, our solution significantly increases the time and effort required to discover additional attack vectors. Implementing these measures is crucial for comprehensive security and maintaining the integrity of your mobile applications.

2. SECURITY BEYOND COMPLIANCE

2.1. Organisations Should Prioritise Mobile App Security

With the rise in cyber-attacks, businesses must prioritise protecting customer data to prevent financial loss and reputational damage. While implementing mobile app security measures is essential for ensuring regulatory compliance and avoiding legal issues, it's crucial to understand that attackers will still attempt to exploit vulnerabilities regardless of compliance.



Therefore, organisations should focus on mobile app security not just as a means to mitigate legal risks but as a fundamental strategy for safeguarding their infrastructure and preserving their customers' trust.

2.2. Mobile Apps Should Comply with Guidelines and Regulatory Standards

In today's regulated environment, compliance with standards like **PCI-DSS, OWASP, MASVS, GDPR, NIST** and **RBI CSF** is essential. These frameworks demand robust **Mobile App Security Testing,** focusing on **user privacy, data security**, and protection against **app tampering:**

- OWASP Mobile Top 10's impact on mobile app development and security.
- MASVS (Mobile Application Security Verification Standard)
- GDPR (General Data Protection Regulation) is a regulation on information privacy.
- The NIST (National Institute of Science and Technology) Cybersecurity Framework helps understand, manage, and reduce cybersecurity risk.
- RBI CSF (Reserve Bank of India Cyber Security Framework)

Regulatory compliance is essential for securing your mobile applications and building user trust. Governments and regulatory bodies globally, including the as well as international standards like GDPR mandate rigorous data protection and security measures for mobile apps.

Failure to comply with these regulations can lead to:

By adhering to these standards, you ensure that your mobile app operates within legal frameworks while protecting user data, preventing breaches, and avoiding legal complications. **Our security solution enables you to meet these compliance requirements through real-time threat detection, robust data privacy measures, and zero performance impact, providing peace of mind and safeguarding your business against non-compliance and runtime threats.**

Key Findings:

Protection Against 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	High	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 Wi-Fi Detection	Medium	Absent
17		Packet Sniffing Detection	High	Absent
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	Mobile Fraud	App Cloning/Second Space Prevention	Medium	Absent
24		Keylogger Prevention	Medium	Absent
25		Time Manipulation	Low	Present
26	Social Engineering	Marketplace Enforcement Check	Medium	Absent

Suggested Next Course of Action:

1. NDA before getting an acceptance for Runtime Security Testing.
2. Engage Bugsmirror Team in Identifying Vulnerabilities from the various Apps.
3. Implement Bugsmirror Defender to protect the App and Build a Strategy on how to address the challenges with Remediations.
4. Quarterly/Half Yearly Application Test Services.

Who are we

Bugsmirror, the **#1 Bug Hunter of Google**, has rapidly emerged as a leader in OS-level security solutions. We specialise in identifying and securing vulnerabilities across Android, iOS, and hybrid apps using our advanced in-house tools like BugsTracker and BugsUtility. Our approach goes beyond compliance, focusing on real-world attack simulations through Red Teaming and penetration testing, ensuring robust protection against evolving threats. This makes us a trusted partner for businesses that prioritise comprehensive mobile security.

This proactive approach guarantees not only compliance but robust protection against evolving threats, ensuring your business is always one step ahead of potential risks. Bugsmirror is your one-stop destination for keeping your business apps safe and secure. Focus on what you do best – building and running your business – and let Bugsmirror handle your mobile application security.