Bugsmirror

Mobile Application Runtime Security Report

(CISO Version)

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 pen-testing teams, leaving critical security gaps that could be exploited.

Bugsmirror Defender - Our Runtime Security Solution

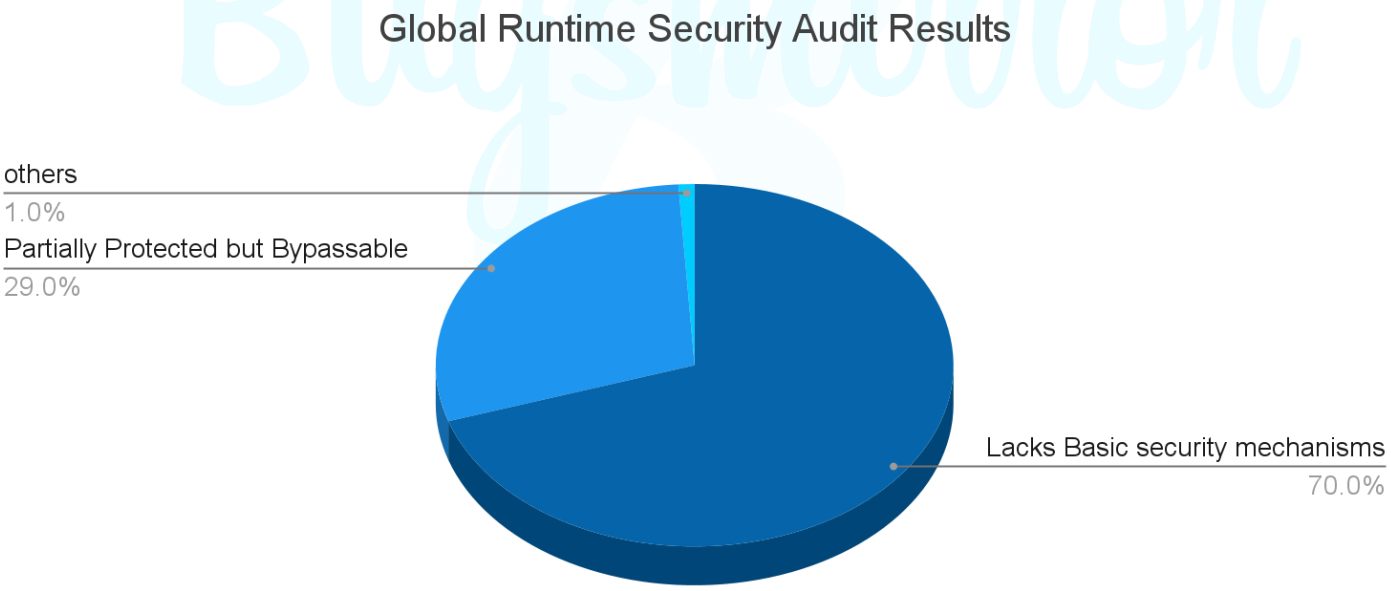
With **Bugsmirror Defender**, you not only benefit from real-time detection but also proactive mitigation of these threats, ensuring comprehensive protection for your mobile applications that provide:

Why Choose Our Runtime Security Solution?

Our Practical Analysis:

In our extensive **Runtime Security Audits** of more than 400 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.

The vulnerabilities detected/confirmed during the tests have been given a Risk Score calculated based on the **Common Vulnerability Scoring System** (CVSS) as below:

Rating	Info	Low	Medium	High	Critical
CVSS Score	0.0	0.1-3.9	4.0-6.9	7.0-8.9	9.0-10.0

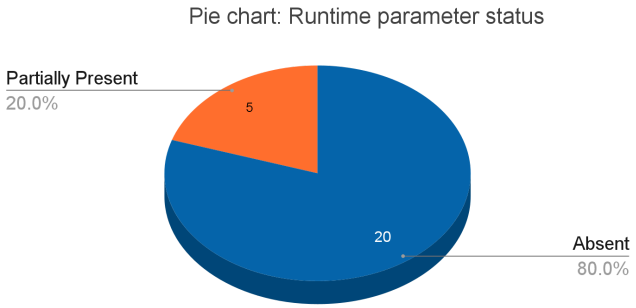
CVSS Score Metrics is as below:

Base Score											
Attack Vector (AV)				Attack Complexity (AC)		Privileges Required (PR)			User Interaction (UI)		
Network (N)	Adjacent (A)	Local (L)	Physical (P)	Low (L)	High (H)	None (N)	Low (L)	High (H)	None (N)	Required (R)	
Scope (S)				Confidentiality (C)			Integrity (I)			Availability (A)	
Unchanged (U)		Changed (C)		None (N)	Low (L)	High (H)	None (N)	Low (L)	High (H)	None (N)	Low (L)	High (H)

1.3. Current App security landscape

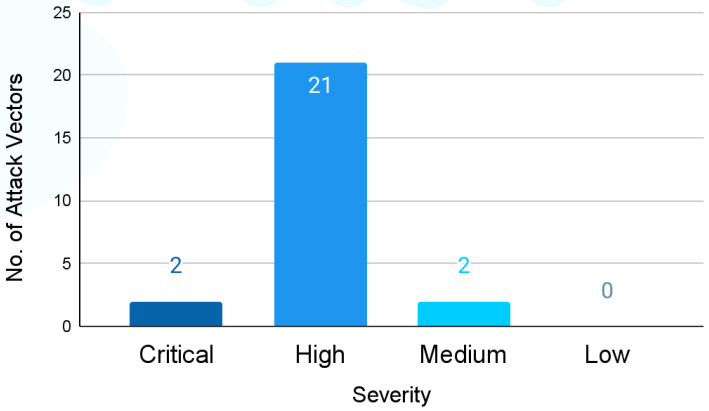
Runtime Security Parameter Status

Runtime Parameter status	Number of parameters
Present	0
Partially Present	05
Absent	20



Number of attack vectors present as per their severity

Severity	No. of Attack Vector
Critical	02
High	21
Medium	02
Low	0



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, organizations 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

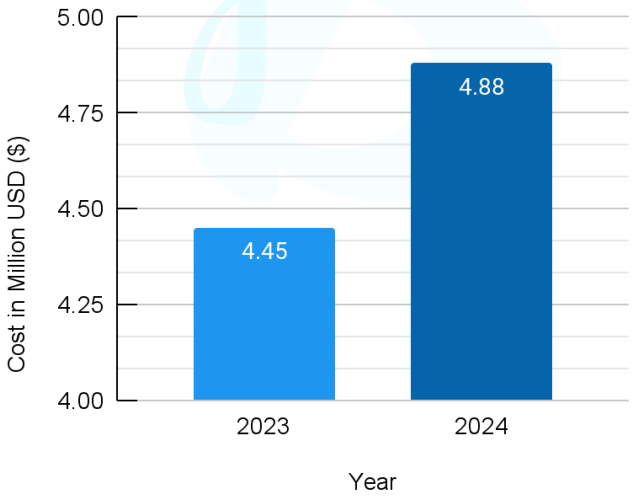
Mobile applications are susceptible to a range of vulnerabilities that span high, medium, and low-severity threats. To ensure robust protection against potential exploitation, our product safeguards you from over 45 attack scenarios. While attackers may attempt to exploit these vulnerabilities, our solution 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 prioritize 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.

Graph: Annual Global Average Cost Of Data Breach



Therefore, organizations 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: Your security posture against Exploitable Runtime Security Threats

Threat: Device Integrity

1	Root Detection	Severity	High	OWASP Category	RESILIENCE-1	Status	Partially Present
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
2	Emulator Detection	Severity	High	OWASP Category	RESILIENCE-1	Status	Partially Present
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
3	Frida Detection	Severity	High	OWASP Category	RESILIENCE-4	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
4	Debugger Detection	Severity	High	OWASP Category	RESILIENCE-4	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
5	Hooking Framework Detection	Severity	High	OWASP Category	RESILIENCE-4	Status	Absent
		CVSS Score	7.0	CVSS Vector	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
6	Runtime Code Injection	Severity	High	OWASP Category	RESILIENCE-4	Status	Absent
		CVSS Score	7.0	CVSS Vector	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
7	Unlocked Bootloader Detection	Severity	High	OWASP Category	-	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
8	Malicious Root App Detection	Severity	High	OWASP Category	-	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

Threat: App Tampering

1	App Repackaging Prevention	Severity	High	OWASP Category	RESILIENCE-2	Status	Absent
		CVSS Score	7.0	CVSS Vector	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
2	App Spoofing Prevention	Severity	Medium	OWASP Category	RESILIENCE-2	Status	Absent
		CVSS Score	6.7	CVSS Vector	AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H		
3	Static App Patching Prevention	Severity	High	OWASP Category	RESILIENCE-3	Status	Absent
		CVSS Score	7.5	CVSS Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Threat: OS Integrity

1	OEM Unlock	Severity	High	OWASP Category	RESILIENCE-1	Status	Absent
		CVSS Score	7.0	CVSS Vector	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
2	ADB Wireless/USB Debugging	Severity	High	OWASP Category	-	Status	Partially Present
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
3	Developer Mode Enable Check	Severity	High	OWASP Category	-	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
4	Accessibility Permission Detection	Severity	High	OWASP Category	-	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

Threat: Secure Communication

1	Unsecured Wifi Detection	Severity	Critical	OWASP Category	-	Status	Absent
		CVSS Score	9.8	CVSS Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
2	Packet Sniffing Detection	Severity	Critical	OWASP Category	NETWORK	Status	Absent
		CVSS Score	9.8	CVSS Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
3	VPN Detection	Severity	Medium	OWASP Category	-	Status	Absent
		CVSS Score	5.9	CVSS Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		

Threat: Mobile Privacy

1	Screen Capturing Prevention	Severity	High	OWASP Category	PLATFORM-3	Status	Partially Present
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
2	Copy Paste Prevention	Severity	High	OWASP Category	PLATFORM-3	Status	Absent
		CVSS Score	7.0	CVSS Vector	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
3	Screen Overlay Prevention	Severity	High	OWASP Category	PLATFORM-3	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
4	Screen Share Prevention	Severity	High	OWASP Category	PLATFORM-3	Status	Partially Present
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

Threat: Mobile Fraud

1	App Cloning/ Second Space Prevention	Severity	High	OWASP Category	RESILIENCE-1	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
2	Keylogger Prevention	Severity	High	OWASP Category	-	Status	Absent
		CVSS Score	7.8	CVSS Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

Threat: Social Engineering

1	Marketplace Enforcement Check	Severity	High	OWASP Category	-	Status	Absent
		CVSS Score	8.4	CVSS Vector	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Note: The CVSS vectors and scores mentioned in this report are calculated based on the guidelines and metrics provided by the official Common Vulnerability Scoring System (CVSS) documentation, available at https://www.first.org/cvss/calculator/3.1.

Suggested Next Course of Action:

1. Sign the NDA to start with the engagement.
2. Our approach: **a)** Detection > **b)** Assessment > **c)** Mitigation
3. Engage the Bugsmirror Team in Identifying Vulnerabilities for your mobile app through our Red-teaming comprehensive assessment.
4. Implement Bugsmirror Defender, our flagship app shielding product to protect your Apps from Runtime threats.
5. Successfully and **securely** release your app on trusted marketplaces.

Who are we:

Bugsmirror, the #1 bug hunter for 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.

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

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 - 45201