# Vulnerability Scan Report: A Summary

| | | |
|---|---|---|
| **Application Name** | **Package Version** | **Package Name** |
| Roblox | 2.624.525 | com.roblox.client |
| **Total Scanned Vulnerabilities** | **Total Vulnerabilities Detected** | **Generated On** |
| 50 | 12 | 28 May 2024 12:03 AM GMT |
| **High Severity Threats** | **Medium Severity Threats** | **Low Severity Threats** |
| 6 | 2 | 3 |

## CERTIFICATE INFORMATION ⌄

| # | OWASP Security Requirements | Total Vulnerabilities scanned | Vulnerabilities found |
|---|---|---|---|
| **V2** | Data Storage and Privacy | 9 | 2 |
| **V3** | Cryptography | 8 | 2 |
| **V5** | Network Communication | 6 | 1 |
| **V6** | Platform Interactions | 11 | 4 |
| **V7** | Code Quality and Build Settings | 6 | 3 |
| **V8** | Resilience Requirements | 4 | 0 |

| MASVS | Issue | Severity | Assessment Status | CWE | Exploits | Can be fixed by Quixxi Shield | View Details |
|---|---|---|---|---|---|---|---|
| V2 Data Storage and Privacy | Read/Write access to External Storage | High | Fail | CWE-276 | CVE-2018-6599 | | View Details |
| | Unsafe files deletion | High | Fail | CWE-200 | CVE-2018-3987 | | View Details |
| V3 Cryptography | Weak Java Hash Code implementation | Warning | Fail | CWE-327 | | | View Details |
| | Weak Random Number Generator | Medium | Fail | CWE-1241 | Multiple vulnerabilities | | View Details |
| V5 Network Communication | Application uses HTTPURLConnection | Low | Fail | | | | View Details |
| | Improper Export of your Android Activities | High | Fail | CWE-926 | CVE-2017-12816 | | View Details |
| V6 Platform Interactions | Improper Export of your Android Services | High | Fail | CWE-926 | CAPEC-501 | | View Details |
| | Improper Export of your Android Broadcast Receiver | High | Fail | CWE-927 , CWE-925 | CAPEC-499 , CAPEC-501 | | View Details |
| | Raw SQL queries used for SQLLite database | High | Fail | CWE-89 | CVE-2019-5454 , CVE-2020-0060 | | View Details |
| | Debugging Information Provision | Medium | Fail | CWE-215 | CAPEC-133 , CVE-2018-6599 | FIXABLE BY QUIXXI | View Details |
| V7 Code Quality and Build Settings | Native binaries contains debugging symbols | Low | Fail | | | | View Details |
| | Missing check for the download source | Low | Fail | CWE-610 | CVE-2018-9582 | FIXABLE BY QUIXXI | View Details |

---

**Abbreviations**

| | |
|---|---|
| CWE (https://cwe.mitre.org/data/definitions/311.html) – Common Weakness Enumeration | CVE (https://cve.mitre.org/) – Common Vulnerabilities and Exposures |
| MASVS (https://github.com/OWASP/owasp-masvs) – Mobile Application Security Verification Standard | OWASP (https://owasp.org/) – Open Web Application Security Project |

---

**Our full report includes threats, risk and fix information for remediation**

Buy Full Report
~~$49~~ **$29**

Upload a Different App