Penetration Testing Report

Date: 2024-06-10

Version: 1.0

Table of Contents

Executive Summary

This report presents the results of penetration testing activity conducted on the Company Names mobile applications. The assessment was performed by VaporVM United Arab Emirates and it took 5 days to complete. Testing was mainly based on enumeration misconfigurations assessment and manual identification of vulnerabilities. The results of the assessment were used to develop recommendations and action plans to address identified security gaps.

Scoping and Time Limitations

The scope limitations for this current engagement involved not to perform social engineering DDOS on the scoped application. Scoping during the engagement did not permit social engineering across all testing components.

Testing Summary

Company Names mobile applications were tested under the current assignment. The purpose of the engagement was to perform a comprehensive review of the security posture of the mobile application without any prior knowledge of its internal workings. The objective of the testing was to identify vulnerabilities that could be exploited by attackers and to assess the application's ability to withstand various attacks. The testing included a range of techniques such as manual testing, automated scanning, and vulnerability analysis. This was done to evaluate the security posture of Company Name against the industrys best practices, validate its security mechanisms, and identify vulnerabilities at the application level and within the source code.

Mobile App Penetration Testing

VaporVM conducted a comprehensive security assessment of Company Name's mobile applications. The mobile application was analyzed from an external attackers perspective. The applications were tested for vulnerabilities and security flaws using various techniques such as static and dynamic analysis and reverse engineering.

Conclusion

It was concluded that the tested mobile applications were well-configured with moderate security controls. The team has performed all the test cases to bypass implemented security controls. Moreover, it was observed that the tested applications have certain security controls to protect the application to run on rooted phones and prevent reverse engineering. The methodology used during the activity was the OWASP Mobile Application Security Verification Standard (MASVS) testing guide.

High-Level Recommendations

The following actionable recommendations along with priority have been listed below: Although the main defense of jailbreak detection bypass is well implemented and not bypassed with the available tools and techniques, no actionable recommendations are required for Target Name.

Assessment Overview

From 9th June 2023 to 15th June 2023, Company Name engaged VaporVM to conduct a Mobile Application Security Assessment. The assessment aimed to identify, validate, and prioritize vulnerabilities within the mobile application based on their impact and exploitability. The assessment was performed using industry-standard testing methodologies such as the OWASP Mobile Application Security Verification Standard (MASVS) testing guide and customized testing frameworks.

Finding Severity Ratings

Severity	Definition
Critical	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	Vulnerabilities are non-exploitable but would reduce an organizations attack surface. It is advised to form a plan of action and patch during the next maintenance window.

Scope

Penetration Testing

The scope as defined in the RFP for assets to be tested and their count is mentioned below:

No	Scope	Assets	Count
1	Mobile Application	ASSET NAME	1
Total Counts			1

Scope Exclusions

For the scope of the activity, the following activities were not part of the scope:

- Conduct Phishing Campaign against Company Name employees.
- Vulnerability exploitation on Critical production servers.
- The exploitation of vulnerabilities resulting in DoS.
- The exploitation of vulnerabilities requiring initial access/client-side testing.
- Using Brute Force attempts to gain access.
- Other exploits impacting services and business continuity.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Critical	High	Medium	Low
0	0	1	0

Vulnerability Details

VULNERABILITY TITLE

Risk Rating	**Critical**
Tools/Tech. Used	**Automated Testing and Manual Validation**
Observation	**Critical**
Implications	**Critical**
Recommendation	**Critical**
Affected Assets	**Critical**
Evidence	**Critical**

Document Management

Document Control

Document Type	**Mobile Application Penetration Testing Report**
Client Name	Company Name
Assets	Asset Name
Testing Performed By	VaporVM
Duration	Business Days
Start Date	Date June 2023
Completion Date	Date June 2023
Classification	Confidential
Version	1.0

Disclaimer

The report contains confidential information about the security vulnerabilities and misconfigurations observed in the tested assets. Access to this report by unauthorized personnel may allow them to compromise the organization's assets, data, or network.

Appendix

Mobile Application Assessment

Mobile application assessment is the process of evaluating the security, privacy, and functionality of a mobile application. The main goal of this process is to identify any vulnerabilities, weaknesses, or other security risks that could be exploited by attackers. The assessment is typically performed by security experts who use various testing methodologies and tools to examine the application and its code.

The stages of mobile application assessment can vary depending on the methodology used but generally involve the following:

- **Reconnaissance:** In this stage, the assessment team gathers information about the application, including its purpose, features, and functionality. This can involve examining the application's code, analyzing network traffic, and reviewing documentation.
- **Static Analysis:** This stage involves analyzing the application's code without executing it to identify any vulnerabilities or weaknesses.
- **Dynamic Analysis:** This stage involves testing the application in a live environment to evaluate its behavior under different conditions and identify any vulnerabilities or weaknesses.
- **Reporting:** In this stage, the assessment team prepares a detailed report of their findings, including recommendations for remediation or mitigation of any identified vulnerabilities or weaknesses.