Mobile Application Security Assessment Report

Customer: Cirus

Date: 13/05/2024

We express our gratitude to the Cirus team for the collaborative engagement that enabled the execution of this Security Assessment.

Platform: iOS

Timeline: 16/04/2024 - 23/04/2024

Methodology: https://hackenio.cc/dApp_methodology

Audit Summary

9.5/10	-	-	-
Security Score	Code quality score	Test coverage	Documentation quality score

Total 9.5/10

The system users should acknowledge all the risks summed up in the risks section of the report

6	5	1	0
Total Findings	Resolved	Accepted	Mitigated

Findings by severity

Critical	0
High	0
Medium	2
Low	4

Vulnerability	Status
F-2024-1487 - No Jailbreak Detection for iOS Application	Accepted
F-2024-1491 - The App Allows Screenshots with Sensitive Data	Fixed
F-2024-1493 - Unrestricted Clipboard Access to Sensitive Fields	Fixed
F-2024-1494 - Sensitive Data Exposure via iOS Pasteboard	Fixed
F-2024-1495 - Accessible Swagger API Endpoint	Fixed
F-2024-1498 - Lack of Anti-Debugging Protection	Fixed

This report may contain confidential information about IT systems and the intellectual property of the Customer, as well as information about potential vulnerabilities and methods of their exploitation.

The report can be disclosed publicly after prior consent by another Party. Any subsequent publication of this report shall be without mandatory consent.

Document

Name	Decentralized Application (dApp) Code Review and Security Analysis Report for Cirus
Audited By	Ece Orsel
Approved By	Stephen Ajayi
Website	https://hacken.io
Changelog	23/04/2024 - Preliminary Report

System Overview

The following table provides a synopsis of target systems that were within the scope of this Security Assessment.

Cirus Mobile Application: iOS

Security score

Upon auditing, the code was found to contain **0** critical, **0** high, **2** medium, and **4** low severity issues, leading to a security score of **9.5** out of **10**.

All identified issues are detailed in the “Findings” section of this report.

Summary

The comprehensive audit of the customer's dapp yields an overall score of **9**. This score reflects the combined evaluation of documentation, code quality, test coverage, and security aspects of the project.

Disclaimers

Hacken Disclaimer

The application given for audit has been analyzed based on best industry practices at the time of the writing of this report, with cybersecurity vulnerabilities and issues in the application's source code, its deployment, and functionality (performing the intended functions) being the focus of our analysis.

The report contains no statements or warranties regarding the identification of all vulnerabilities or the absolute security of the code. The report covers only the code that was submitted and reviewed, and therefore may not remain relevant after any modifications have been made. This report should not be considered a definitive or exhaustive assessment of the utility, safety, or bug-free status of the application, nor should it be taken as a guarantee of the absence of other potential issues.

While we have exerted our best efforts in conducting the analysis and producing this report, it is crucial to understand that this report should not be the sole source of reliance for ensuring the security of the application. We strongly recommend undertaking multiple independent audits and establishing a public bug bounty program to enhance the security posture of the application.

English is the original language of this report. The Consultant is not liable for any errors or omissions in any translations of this report.

Technical Disclaimer

Applications, whether decentralized apps (DApps) or other types of applications, are deployed and run within specific environments that may include various platforms, programming languages, and other related software components. These environments and components can have inherent vulnerabilities that might lead to security breaches. Consequently, the Consultant cannot guarantee the absolute security of the audited application.

Appendix 1. Severity Definitions

Severity	Description
Critical	These issues present a major security vulnerability that poses a severe risk to the system. They require immediate attention and must be resolved to prevent a potential security breach or other significant harm.
High	These issues present a significant risk to the system, but may not require immediate attention. They should be addressed in a timely manner to reduce the risk of the potential security breach.
Medium	These issues present a moderate risk to the system and cannot have a great impact on its function. They should be addressed in a reasonable time frame, but may not require immediate attention.
Low	These issues present no risk to the system and typically relate to the code quality problems or general recommendations. They do not require immediate attention and should be viewed as a minor recommendation.

Appendix 2. Scope

The scope of the project includes the following;

Scope Details	
Mobile Application	iOS
API	Not Required
Whitepaper	Not Required
Requirements	Not Required
Technical Requirements	Not Required