HACKEN

Orange Crypto Wallet Code Review And Security Analysis Report

Customer: Orange Crypto

Date: 08/04/2024

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

Orange Wallet is a browser extension software wallet that simplifies managing Bitcoin, BRC20 tokens, Stacks, and Ordinals NFTs. It features integration with Orange Assistant and AI for instant access to crypto industry insights. Orange Wallet stands out for its user-friendly, decentralized, non-custodial, and anonymous nature, offering direct Bitcoin blockchain access without third-party involvement. Your private key remains exclusively yours, ensuring your Bitcoin is securely stored on the blockchain without collecting any personal data. Supporting a variety of protocols like BRC20, Ordinals, Stacks, and Bitcoin itself, Orange Wallet is your all-in-one solution for diverse crypto assets management.

Platform: Crypto Wallet

Language: TypeScript

Timeline: 16/02/2024 - 22/03/2024

Methodology: https://hackenio.cc/dApp_methodology

Review

Scope

Repository	https://github.com/orangecryptohq/orangewallet/tree/release/v1.0.4, https://github.com/orangecryptohq/orangeseed/tree/develop
Commit	n/a

Audit Summary

10/10

Security Score

Total 10/10

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

15	13	2	0
Total Findings	Resolved	Accepted	Mitigated

Findings by severity

Critical	0
High	4
Medium	5
Low	5

Vulnerability	Status
F-2024-0958 - Insecure Password Update Policy	Accepted
F-2024-1033 - Sensitive Data Exposure through Clipboard	Accepted
F-2024-0822 - Open Redirect Vulnerability in Wallet Redirection Logic	Fixed
F-2024-0823 - Exposure of Sensitive Information in Test Suites	Fixed
F-2024-0824 - Vulnerability Wallet Dependencies	Fixed
F-2024-0847 - Insecure Deserialization	Fixed
F-2024-0848 - Cache Poisoning/Outdated Information	Fixed
F-2024-0862 - Use of Password Hash Directly as Key	Fixed
F-2024-0871 - Insecure Random Number Generation	Fixed
F-2024-0874 - Overly Broad Host Permissions	Fixed
F-2024-0875 - Insecure Content Security Policy	Fixed
F-2024-0876 - Insecure Default Configuration (CORS)	Fixed
F-2024-0951 - Potential Mismanagement of Sensitive Information	Fixed
F-2024-1035 - Plaintext Secret Keyphrase Exposure in Memory	Fixed
F-2024-1036 - Plaintext User Password Exposure in Memory	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 Orange Crypto
Audited By	Stephen Ajayi
Approved By	Stephen Ajayi
Website	https://hacken.io
Changelog	25/02/2024 - Preliminary Report

System Overview

Orange Wallet is a browser extension software wallet that simplifies managing Bitcoin, BRC20 tokens, Stacks, and Ordinals NFTs. It features integration with Orange Assistant and AI for instant access to crypto industry insights. Orange Wallet stands out for its user-friendly, decentralized, non-custodial, and anonymous nature, offering direct Bitcoin blockchain access without third-party involvement. Your private key remains exclusively yours, ensuring your Bitcoin is securely stored on the blockchain without collecting any personal data. Supporting a variety of protocols like BRC20, Ordinals, Stacks, and Bitcoin itself, Orange Wallet is your all-in-one solution for diverse crypto assets management.

Asset:

- Browser Wallet Extension
- Source Code

Executive Summary

This report presents an in-depth analysis and scoring of the customer's dapp project. Detailed scoring criteria can be referenced in the scoring methodology.

Documentation quality

The total Documentation Quality score is 10 out of **10**.

- Comprehensive functional requirements were outlined.
- Detailed technical specifications were provided.
- Complete documentation for setting up, building the wallet, and integrating it with a browser was made available.

Code quality

The total Code Quality score is **10** out of **10**.

- The code has been structured with clarity and coherence.
- The coding style maintained throughout is uniform.
- The development environment has been properly configured.

Security score

Upon auditing, the code was found to contain **0** critical, **4** high, **5** medium, and **5** low severity issues, leading to a security score of **10** 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 **10**. This score reflects the combined evaluation of documentation, code quality, test coverage, and security aspects of the project.

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 endpoints from the provided repository:

Scope Details	
Repository	https://github.com/orangecryptohq/orangewallet/tree/release/v1.0.4, https://github.com/orangecryptohq/orangeseed/tree/develop
Commit	n/a
Whitepaper	https://docs.orangecrypto.com
Requirements	https://docs.orangecrypto.com
Technical Requirements	https://docs.orangecrypto.com