SALUS SECURITY

March 2024



PENETRATION TESTING REPORT

TRUST WALLET

Overview

Project Name	Trust Wallet
File Name	Penetration Testing Report for Trust Wallet
Creator	Salus Security
Create Date	4 March 2024
Total days	8 Days
Receive Date	13 March 2024

Modify History

Version	Modify Date	Modifier	Modify Type	Modified Chapter	Modified Content

*Modified Type are categorized by **A** - ADDED **M** - MODIFIED **D** – DELETED

Copyright Statement

All content appearing in this document, unless otherwise specified, is copyrighted by Salus. No individual or institution may copy, decipher or quote any fragment of the document in any way without the written authorisation of Salus Security.

SALUS

Table of Contents

Introduction **4**

1 About Salus Security 4

2 Assessment Scope 4

3 Risk Summary Description 5

4 Disclaimer 5

5 Findings 6

Security Summary **7**

Security Recommendations 7

Introduction

1 About Salus Security

At Salus Security, we are in the business of trust. We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve. In addition to smart contract audits and red teaming, our Rapid Detection Service for smart contracts aims to make security accessible to all. This high calibre, yet cost-efficient, security tool has been designed to support a wide range of business needs including investment due diligence, security and code quality assessments, and code optimisation.

2 Assessment Scope

Penetration test coverage is assessed based on the range of assets that need to be tested. This penetration test only covers assets under the names Trust Wallet. So we have a high level of important assets under Trust Wallet. trustwallet.com stand out in the asset list and become the main evaluation penetration object. As such, the report reflects detailed security summary reports related to business security.

SALUS

3 Risk Summary Description

Overall Risk Level: **Medium**

Description: Through the security penetration test in real environment, it is found that Trust Wallet has such dangerous vulnerabilities as The mailbox service is not well configured, Cross-site scripting, Strict transport security not enforced and AWS bucket with Object listing. Based on these vulnerabilities, it can be judged that they may be used by hackers or criminals, which will bear certain security risks.

4 Disclaimer

This report is considered by Salus Security to be private information; it is licensed to Trust Wallet under the terms of the project statement of work. Material within this report may not be reproduced or distributed in part or in whole without the express written permission of Salus Security.

Test Coverage Disclaimer
All activities undertaken by Salus Security in association with this project were performed in accordance with a statement of work and mutually agreed upon project plan. Security Penetration Testing projects are time-boxed and often reliant on the information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Salus Security uses automated testing techniques to test the controls and security properties of software rapidly. These techniques augment our penetration testing work, but each has its limitations. Their use is also limited by the time and resource constraints of a project.

Salus Security makes all effort but holds no responsibility for the findings of this penetration testing. Salus Security makes no judgments on the underlying business model or the individuals involved in the project.

SALUS

5 Findings

The Findings section briefly describes the severity level of the discovered problem, the content of the problem, and the disposition status of the vulnerability.

The following table provides an overview of the findings.

#	Severity	Description	Status
1	High	The mailbox service is not well configured	Resolved
2	High	Cross-site scripting (reflected)	Resolved
3	Low	Strict transport security not enforced	Resolved
4	Low	AWS bucket with Object listing	Resolved
5	Low	Incorrect configuration HTML Injection	Acknowledged

SALUS

Security Summary

Security Recommendations

1) Fuzzify relevant sensitive information, do it on the server side, and strictly check the data returned by the server side. the query data and page display data has to be consistent and never return redundant data.
2) Delete pages that are not related to the business. If it is a middleware management page that must be used, it is recommended to control the access rights of the page.

SALUS