Safeheron Security Audit Report

Project Overview

This security audit project aims at a fast and comprehensive security audit for Safeheron to detect potential threats and further improve the security of Safeheron. The utmost efforts are made along with the Safeheron Team to safeguard the security of users and their funds in particular.

Foreword

We extend our gratitude for Safeheron recognition of SlowMist and hard work and support of relevant staff.

Audit Information

Audit Period: 30 working days

Audit Team: SlowMist Security Team

Audit Duration: June 2, 2021 - July 2, 2021

Web information

https://www.safeheron.vip/login

iOS Information

Download link: App Store

Version number:1.0.2

Project Profile

Safeheron is a leading provider of safe custody solutions for digital assets. Use MPC and a trusted framework to ensure that the entire link of digital assets from generation to storage to use is safe and trustworthy; through a free and flexible policy engine, customize the secure digital asset use approval flow; adopt a zero-trust security architecture design and Practice has ensured that our system is always in a very safe state. The mission of Safeheron is to solve the problem of safe custody and safe flow of digital assets, and to provide safe and efficient custody services for digital asset institutions.

Audit Results

(Other unknown security vulnerabilities are not included in the scope of this audit)

Serial Number	Audit Class	Audit Subclass	Audit Reesult
1	Open Source Intelligence Gathering	Whois information collection	Passed
		Real IP discovery	Passed
		Subdomain detection	Passed
		Mail service detection	Passed
		Certificate information collection	Passed
		Web services component fingerprint collection	Passed
		Port service component fingerprint collection	Passed
		Segment C service acquisition	Passed
		Personnel structure collection	Passed
		GitHub source code leak locating	Passed
		Google Hack detection	Passed
		Discovery of the privacy leaked	Passed
2	Server Security Configuration Audit	CDN service detection	Passed
		Network infrastructure configuration test	Passed
		Application platform configuration management test	Passed

		File extension resolution test	Passed
		Backup, unlinked file test	Passed
		Enumerate management interface test	Passed
		HTTP method test	Passed
		HTTP strict transmission test	Passed
		Web front-end cross-domain policy test	Passed
		Web security response head test	Passed
		Weak password and default password detection	Passed
		Management background discovery	Passed
3	Identity Management Audit	Role definition test	Passed
		User registration process test	Passed
		Account rights change test	Passed
		Account enumeration test	Passed
		Weak username strategy testing	Passed
4	Certification and Authorization Audit	Password information encrypted transmission test	Passed
		Default password test	Passed

		Account lockout mechanism test	Passed
		Certification bypass test	Passed
		Password memory function test	Passed
		Browser cache test	Passed
		Password strategy test	Passed
		Security quiz test	Passed
		Password reset test	Passed
		OAuth authentication model test	Passed
		Privilege escalation test	Passed
		Authorization bypass test	Passed
		Two-factor authentication bypass test	Passed
		Hash robustness test	Passed
5	Session Management Audit	Session management bypass test	Passed
		Cookies property test	Passed
		Session fixation test	Passed
		Session token leak test	Passed
		Cross Site Request Forgery (CSRF) test	Passed
		Logout function test	Passed
		Session timeout test	Passed

		Session token overload test	Passed
6	Input Security Audit	Cross Site Scripting (XSS) test	Passed
		Template injection test	Passed
		Third-party component vulnerability test	Passed
		HTTP parameter pollution test	Passed
		SQL injection test	Passed
		XXE entity injection test	Passed
		Deserialization vulnerability test	Passed
		SSRF vulnerability test	Passed
		Code injection test	Passed
		Local file contains test	Passed
		Remote file contains test	Passed
		Command execution injection test	Passed
		Buffer overflow test	Passed
		Formatted string test	Passed
7	Business Logic Audit	Interface security test	Passed
		Request forgery test	Passed
		Integrity test	Passed
		Overtime detection	Passed
		Interface frequency limit test	Passed
		Workflow bypass test	Passed

		Application misuse protection test	Passed
		Unexpected file type upload test	Passed
		Malicious file upload test	Passed
8	Cryptographic Security Audit	Weak SSL/TLS encryption, insecure transport layer protection test	Passed
		SSL pinning security deployment test	Passed
		Non-encrypted channel transmission of sensitive data test	Passed
9	App Security Audit	App environment testing audit	Passed
		Code decompilation detection	Passed
		File storage security detection	Passed
		Communication encryption detection	Passed
		Permissions detection	Passed
		Interface security test	Passed
		Business security test	Passed
		WebKit security test	Passed
		App cache security detection	Passed
		App Webview DOM security test	Passed
		SQLite storage security audit	Passed
10	Web Security Audit	Registration security Audit	Passed
		Password recovery security policy	Passed

		Login security policy	Passed
		Data transmission security	Passed
		2FA security policy	Passed
		Session security policy	Passed
		API security policy	Passed
		Deposit security policy	Passed
		Withdraw security policy	Passed
		Cryptocurrency recharge security policy	Passed
		Cryptocurrency withdrawal security policy	Passed
		Exchange security policy	Passed
		Security Education	Passed
		Anti-phishing policy	Passed
		Listing application security policy	Passed
		KYC security policy	Passed
		AML security policy	Passed
		DNSSEC check	Passed
		SSL/TLS security check	Passed
		HTTP header security check	Passed

		Business logic security check	Passed
Audit Summary			Passed

Final rating : Remarkably good

Disclaimer

SlowMist only issues this report based on the fact that has occurred or existed before the report is issued, and bears the corresponding responsibility in this regard. For the facts that occur or exist later after the report, SlowMist cannot judge the security status of theits smart contract. SlowMist, and is not responsible for it.

The security audit analysis and other contents of this report are based on the documents and materials provided by the information provider to SlowMist as of the date of this report (referred to as "the provided information"). SlowMist assumes that: there has been no information missing, tampered with, deleted, or concealed. If the information provided has been missinged, modified, deleted, concealed or reflected andor is inconsistent with the actual situation, SlowMist will not bear any responsibility for the resulting loss and adverse effects. SlowMist will not bear any responsibility for the background or other circumstances of the project.

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist