SCORPIONES

WEB APPLICATION SECURITY ASSESSMENT

FOR:

KIROBO

IN THE CUSTODY OF BLOCKCHAIN

June 30, 2020
Version 2.0

To the management of Kirobo:

We have completed our engagement to assess the security of your application. This assessment was conducted by performance of attack and penetration services, in accordance with our engagement letter dated June 7, 2020.

Our procedures were limited to those outlined in the letter and described in this report. The findings and recommendations resulting from our assessment are provided in the "Detailed Findings and Recommendations" sections.

The procedures summarized in this report do not constitute an audit, a review or other form of assurance as defined by generally accepted audit, review or other assurance standards and accordingly we do not express any form of assurance. This assessment relates to actions that were performed at a specific point in time. As a result, it does not reflect events or circumstances that may arise after this service has concluded.

This report is intended solely for the information and use of the audit committee and management of Kirobo and is not intended to be, and should not be used, by anyone other than these specified parties.

The ratings in the detailed findings and recommendations section of this report do not represent a conclusive determination on the adequacy or effectiveness of internal controls. Rating definitions are as defined in Appendix.

We appreciate your cooperation and assistance during the course of our work.

Sincerely,

Scorpiones.

Executive Summary

Intro

Scorpiones team performed the web application penetration testing assessment during the period from June 14, 2020 to June 22, 2020.
The findings in this report result from our attempts to discover, validate and exploit vulnerabilities that were considered to be within the project's scope and duration. The outcomes of the exploitation activities performed during this review demonstrate the threats associated with both unauthorized and authorized malicious access, and illustrate the risk of potential compromise. The recommendations provided in this report are structured to facilitate remediation of the identified security risks.

Scope

The web application assessment was a time-boxed security review of Kirobo safer web application (https://safer.kirobo.me/welcome) via hardware wallet integration (Ledger Nano S) using a gray-box methodology, which identifies potential security exposures, including the OWASP Top 10 vulnerabilities, through automated and manual testing.

Current Risk Level

Kirobo's application security status currently resides in a **Low** risk level.
This means the application was discovered to contain low-level vulnerabilities and security flaws.
It is recommended to perform the offered mitigations in order to minimize security risks and avoid future attacks against the application.
For additional information regarding the risk ratings and definitions, please refer to Appendix.

Limitations

There were no limitations for the testing.

Summary of Findings

The following table summarizes the number of identified security issues categorized by risk level:

Assessment	Risk			Total
	High	Medium	Low	6
Kirobo Safer Web Application	0	2	4	

Appendix – Risk Rating Definitions

- **High** - Finding reveals a serious vulnerability that could result in a loss of control (to system or application) and/or exposure of sensitive data. A finding rated as 'HIGH' could indicate a risk to confidentiality or integrity, resulting, for example, in compromised user accounts, or unauthorized access to restricted system functions.
- **Medium** – This vulnerability does not directly lead to a compromised administrative or user account, but could be used in conjunction with other techniques to compromise accounts or perform unauthorized activity on the site or application.
- **Low** - This vulnerability has a limited potential of exposing or compromising user-accounts, or of unauthorized access to data due to configuration issues, outdated patches and/or policy.

Retest

The following table summarizes the status of the finding after re-testing by fixed or not fixed:

Finding	Technical Risk	Status
M#1 – IDOR Vulnerability Leads to Confidential Data Leaking	Medium	FIXED
M#2 – Weak and Permanent Password Policy	Medium	FIXED
L#1 – Passcode Field with Autocomplete Enabled	Low	FIXED
L#2 – Local Storage Stored Sensitive Information	Low	FIXED
L#3 – Json Web Token Implemented with Weak Algorithm	Low	FIXED
L#4 – Improper Error Handeling	Low	FIXED