SCORPIONES

MOBILE APPLICATION SECURITY ASSESSMENT

iOS & Android

FOR:

ZenGo

October 03, 2022
Version 2.0

Executive Summary

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 May 9, 2022.

Our procedures were limited to those outlined in the letter and described in this report.

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 ZenGo 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.

ZenGo Penetration Testing

Intro

Scorpiones team performed the mobile application penetration testing assessment during the period from June 6, 2022 to June 14, 2022.
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 mobile application assessment was a time-boxed security review of ZenGo mobile application (iOS & Android) using a grey-box methodology, which identifies potential security exposures, including the OWASP Top 10 vulnerabilities, through automated and manual testing.

Current Risk Level

It is evident the ZenGo development team invested a lot of efforts in securing their product.

It is recommended to perform the offered mitigations in order to minimize security risks and avoid future attacks against the application.

Scorpiones confirms that there are no open high-risk or medium-risk vulnerabilities identified at the time of report submission.

Limitations

The testing team did not encounter any limitations during the testing phase.

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.