SCORPIONES

MOBILE APPLICATION SECURITY ASSESSMENT

FOR:

February 9, 2020
Version 2.0

Executive Summary

Intro

Scorpiones team performed the mobile application penetration testing assessment during the period from November 17, 2019 to November 25, 2019.
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.

Scope

The mobile application assessment was a time-boxed security review of ZenGo mobile application (Android) and server using a grey-box methodology, which identifies potential security exposures, including the OWASP Top 10 vulnerabilities, through automated and manual testing. The testing consisted of the software components developed by ZenGo (first party) and not Third parties.

Current Risk Level

The system has been found to meet Scorpiones security criteria as recommended by the OWASP methodologies. Based on the results of testing and verification process completed on November 2019, and in accordance with the testing scope, details and limitations as stated in this document, **Scorpiones confirms that there are no open high-risk or medium-risk vulnerabilities** identified at the time of report submission.

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

Appendix A – 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potential of exposing or compromising user-accounts, or of unauthorized access to data due to configuration issues, outdated patches and/or policy.

Appendix B: Additional disclosures to the management of ZenGo:

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 October 2, 2019.

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.

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

Sincerely,

Scorpiones.

Appendix C: About Scorpiones

Scorpiones is a provider of professional and creative solutions to information security problems in applications, databases, blockchain and corporate infrastructure. Among its clients are major financial institutes and leading companies around the world. We offer unique point of view in the technology and methodology of application security, as well as out-of-the-box ingenuity and thorough grasp of the operational patterns of hackers.

Our group is led by a team of elite software testing professionals, who are among the world's pioneers in application and network security. Each of them has vast experience in the field of application security and the highest level of expertise in development and security.

Our testers have extensive experience working with different types of enterprises in varied industries and with a variety of infrastructures and systems. This experience ensures that the customers will be provided with the most professional services focused at creating tailor-made solutions for your organization.

In addition to penetration testing, network and application security consulting services, we provide wide range of application level security trainings, in order to increase awareness and skill in secure application coding.

All our training programs are based on home-grown, unique platform, which simulates a real online enterprise environment, which include both applications and networking products, vulnerable to various application level vulnerabilities. In addition to demonstrations, our technical training programs also include hands-on practice using the environment, which include vulnerable webs, network devices, management interfaces and more that simulates an enterprise environment that allows the trainees to participate in real-time penetration testing.