SECURE CODE REVIEW

For: CoinsPaid
By: Hacken
Dated: 08.02.22

This document contains confidential information about IT systems and the network infrastructure of the customer, as well as information about potential vulnerabilities and methods of their exploitation.
This confidential information is for internal use by the customer only and shall not be disclosed to third parties.

Document

Name:	SECURE CODE REVIEW FOR CoinsPaid
Type:	Detailed Code Review Report with Second Remediation
Revision:	Version 3
Date:	08 February 2022

Contractor Contacts

Role	Name	Email
Project Lead	Evgenia Broshevan	e.broshevan@hacken.io

Contents

Introduction

We thank CoinsPaid for allowing us to conduct a Secure Code Review. This document outlines our methodology, limitations, and results of the security assessment.

Executive Summary

Hacken OÜ (Consultant) was contracted by CoinsPaid (Customer) to conduct the Security Assessment of their application.

This report presents the findings of the security assessment of the application & API security assessment that was conducted between October 05, 2021 - November 05, 2021.

The purpose of the engagement was to utilize active exploitation techniques to evaluate the security of the application against best practices and to validate its security mechanisms.

Next vulnerabilities and mistakes were identified during the assessment:

	High	Medium	Low	Informational
Web	2	2	6	2

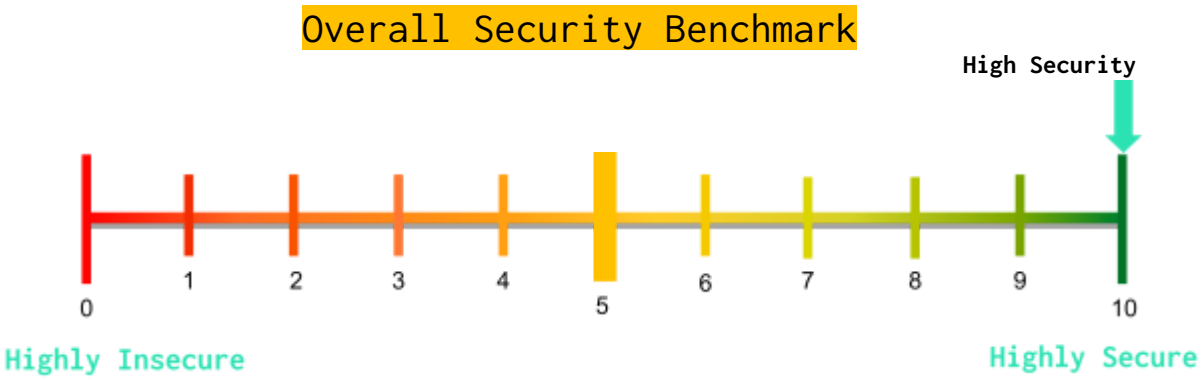
Next vulnerabilities and mistakes were identified after remediation check:

	High	Medium	Low	Informational
Web	1	0	1	0

Next vulnerabilities and mistakes were identified after second remediation check:

	High	Medium	Low	Informational
Web	0	0	0	0

According to our research after performing the security assessment, Web Infrastructure was identified as a High-Security level.



The overall rating of CoinsPaid Applications, after the security assessment by the Consultant's Security Team, stands out to be 10 out of 10. The security assessment was carried out following the in-house test cases, manual methods, exploitation, and automated tools.

Security Assessment Overview

Scope

The following list of the information systems was the scope of the Security Assessment.

#	Name	Type
1	https://wallet.sandbox.coinspaid.com - wallet	Demo Site
2	https://wb.sandbox.coinspaid.com - admin panel	Demo Site

Security Assessment start and end dates were coordinated by email according to the following table:

Testing start date:	October 5, 2021
Preliminary Report:	October 20, 2021
Testing end date:	November 5, 2021
Reporting:	November 5, 2021
Remediation check:	December 15, 2021
Second remediation check	February 8, 2022

Team Composition

The project team consisted of 3 security experts with the following roles, certifications, and responsibilities:

Role	Responsibility
Project Manager	Customer communication Project delivery and quality control
Senior Security Engineer #1 (Lead Penetration tester, OSCP, Node.js, React, PHP, Websockets)	Code review Identify security and business risks for applications
Middle Security Engineer #2 (Penetration tester, Certified Ethical Hacker, Java, PHP, Node.js, Databases)	Code review Identify security and business risks for applications

Main Vectors

Secure Code Review is a specialized task with the goal of identifying types of weaknesses that exist within a given code base. The task involves both manual and automated review of the underlying source code and identifies specific issues that may be representative of broader classes of the weakness inherent in the code.

A code review includes reviewing all of the code for the Application Security Risks:

- Injection flaws – such as SQL, OS and LDAP
- Cross-Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References – exposing a file, directory or database key
- Cross-Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

During this process, members of the review team review the application code for security problems and categorize the findings based on the weakness categories. Each finding is assigned a risk rating of High, Medium, Low, or Info. These findings and the broader weakness classes that they represent are presented in this final report that the development team can use as the foundation for improving the overall quality of the codebase.

Objectives

Secure Code Review has the following objectives:

- Identify technical and functional vulnerabilities.
- Estimate their severity level.
- Modeling the “most likely” attack vector against the Customer’s Information System.
- Proof of concept and exploitation of vulnerabilities.
- Draw up a prioritized list of recommendations to address identified weaknesses.

Methodology

Our methodology for Security Assessment is based on our own experience, best practices in the area of information security, international methodologies, and guides such as PTES and OWASP.
Within the scope of this project, we have investigated the following functional domains:

- Intelligence gathering activities against a target;
- Service detection and identification;
- Vulnerabilities detection, verification, and analysis;
- The exploitation of vulnerabilities;
- Providing recommendations aimed to address a security weakness.

Limitations and Assumptions

This project limited by the scope of this document
During this project, the Consultant will follow the following limitations:

- The operational impact to the networks will be maintained to the minimum and coordinated with the client;
- No denial of service attacks will be used;
- No active backdoor or Trojans will be installed;
- No client data will be copied, modified, or destroyed.

The following security tests shall be considered Out of Scope for this assessment:

- Internal networks assessment;
- Denial of Service testing;
- Physical Social Engineering testing.

Disclaimer

This security assessment was conducted for the CoinsPaid application and is valid on the date of the report submission hereto. The description of findings, recommendations, and risks was valid on the date of submission of the report hereto. Any projection to the future of the report’s information is subject to risk due to changes in the Infrastructure architecture, and it may no longer reflect its logic and controls.