Netsecurity

Firi

Penetration test

Feb/2022

CONFIDENTIAL

Netsecurity AS

Oslo / Kristiansand / Grimstad / Bergen / Stavanger

2 Executive summary

This report documents the result of the penetration test against Firi's cryptocurrency platform, specifically the components listed in section 5 – Scope. The overall goal of the penetration test was to ascertain whether there were any security vulnerabilities that could threaten Firi or its customers.

During the test, Netsecurity made several positive observations about the environment.

- Access control – Netsecurity found no ways to access data from other users than the ones that we created ourselves
- Injection resistance – Netsecurity attempted several various injection attacks (ex SQL injection, Server- and Client-Side Template Injection, etc) but found no way to exploit the application in this way
- Strong authentication to access the platform either via Vipps or username/password combinations

Netsecurity did however find some vulnerabilities that should be corrected. It is believed that if the recommendations listed in this report is followed, the security posture of Firi's platform will be strengthened significantly.

Vulnerability overview:

Reference	Description	Risk	Status
6.1	Blind Server-Side Request Forgery	High	Open
6.2	Firebase API Key Exposed	Medium	Open
6.3	Cross-Origin Resource Sharing: Arbitrary Origin Trusted	Medium	Open
6.4	Username Enumeration	Medium	Open
6.5	Lack of Brute Force Protection	Medium	Open
6.6	Stack Trace Enabled	Medium	Open
6.7	Session Tokens not Reset on Password Change	Medium	Open
6.8	Vulnerable Third-Party Library	Low	Open

Vulnerability highlight:

- Functions in the GraphQL interface allowed for an attacker to send forged messages from the server to an arbitrary destination. It was possible to send both GET and DELETE requests. As testing was performed in the production environment, Firi was notified and no further exploration into the risk of this finding was performed (as this could have severe, unintended consequences)