RIVER
SECURITY

Penetration Test report

CONFIDENTIAL

02.2022

Summary and Key Findings

This report covers the penetration testing activities conducted against Firi, specifically the assets listed in the Scope section. The penetration testing took place in February 2022, following a Digital Footprint assessment. In total, 5 different penetration testers have been involved in the testing activities.

There were mainly three systems in scope for testing, where all are in good shape for their online accessibility without any huge risks to infrastructure or disclosure of sensitive data. However, there are few parts of the applications where weaknesses or abnormalize were discovered. These are highlighted below:

- **Outdated 3rd party JavaScript (jQuery) with known vulnerabilities.**
  Vulnerable component of jQuery (htmlPrefilter) has not been found in use within the application.
- **Unexploitable Reflected Cross-Site-Scripting.**
  Multiple GraphQL endpoint reflects user input and could lead to cross-site-scripting issues. Modern browser, and the application correctly identifies content-type, make this an information only finding.
- **Invalidating of gift cards when redeemed with account without bank details completed.**
  A business logic flaw was found when redeeming gift cards resulting in gift cards used on an account that was not completed with bank details would fail, and the gift card would be marked as used.
- **Deleting Bank Accounts - Misleading responding from API.**
  When sending a delete request for bank account details, the API response with a success message, even if the bank account id does not exist, or the user do not have access.
- **Missing authorization check on a few public calls to api.firi.com**
  Requesting marking information from the API, can be done without an access token. As this could be consider public information, this is rated as information only. Albeit when the same request is done with an invalid access token, the API rejects the request.
- **Web Security headers**
  By implementing security headers, the overall security posture of the service could be lifted. Mainly Strict Security Headers should be implemented. Content Security Policy should be consider for the main application (platform.firi.com)
- **Log/Debug information that contains sensitive information is sent to 3rd party.**
  Request are sent to sentry.io that contains authorization token. Such information is normally not needed for log/debug scenario and should be restricted.

The application is considered to be in a very good security state; scripts are hardened, and input is sanitized in a way that makes cyber attacks very challenging. Furthermore, business logic and flaws were attempted uncovered, but the application proved to be resilient. River Security believes that if these findings are addressed, the applications and systems within target scope would be in very good shape. With continuous surveillance and the necessary governance over these systems, the state of elements in-scope should be considered of adequate level regarding information security.