Xref Web and API Penetration Test Report

Prepared for Xref on the 9th of March 2022

Red Cursor

Table of Contents

1 Document Control

1.1 Revision History

Version	Author	Date
Initial Draft v0.9	Gordon Maddern	28th February 2022
QA and Final Release v1.0	Michael Bielenberg	9th of March 2022

1.2 Document Distribution

Version	Date	Details of Distribution
Final Release v1.0	9th of March 2022	Released to Xref as password protected file. Password sent via SMS

This document is Copyright Red Cursor Pty Ltd 2022.

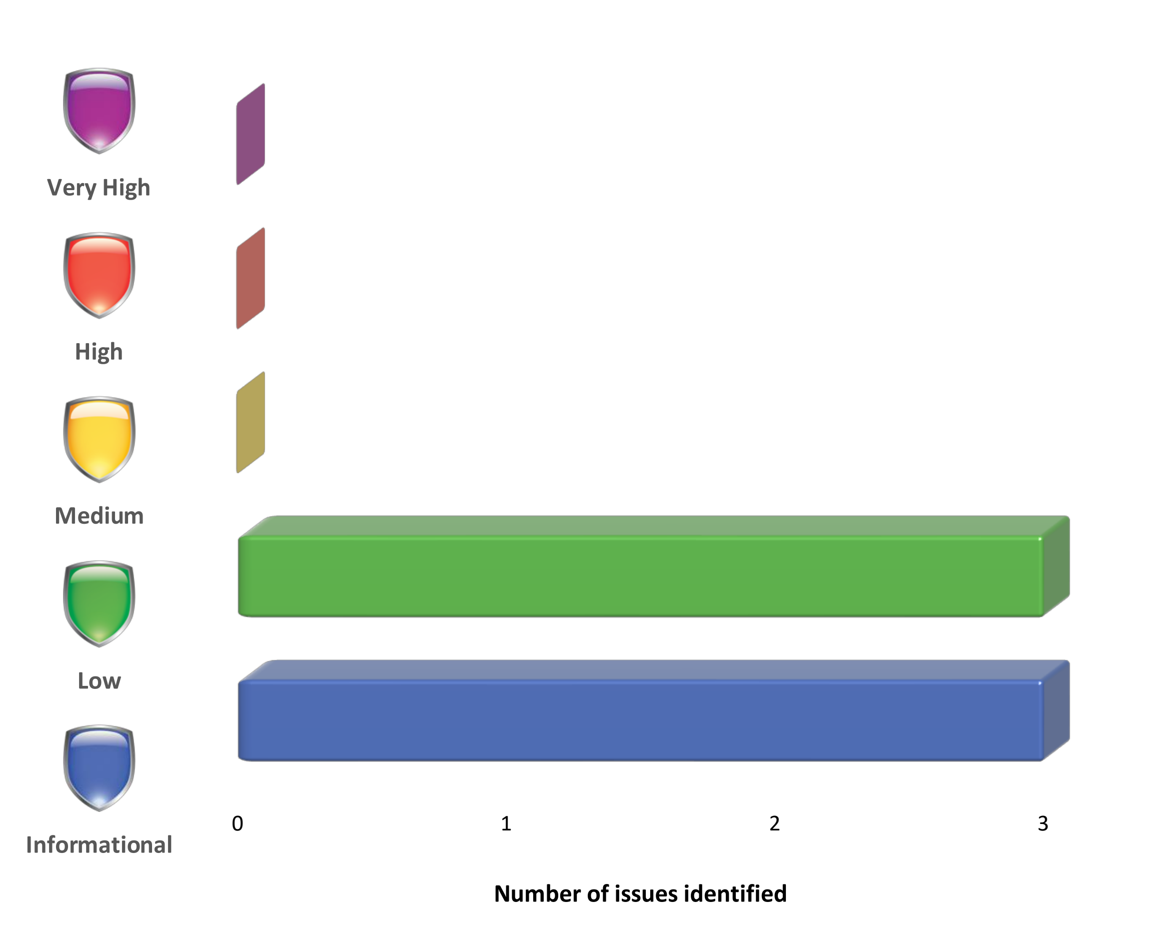
2 Executive Summary

Red Cursor was engaged by Xref on the 28th of February 2022 to perform web application penetration testing of their Xref application and its backend APIs and microservices. This application is used to manage workflows between employers, candidates, and referees.

This testing was designed to simulate a malicious user on the Internet as well as a malicious or compromised authenticated user.

During the testing six security issues were identified. The graph below shows the number and security rating of the risks identified during the engagement:

Risk Summary Chart



Out of the six findings, none of these pose any significant risk to Xref or their customers.

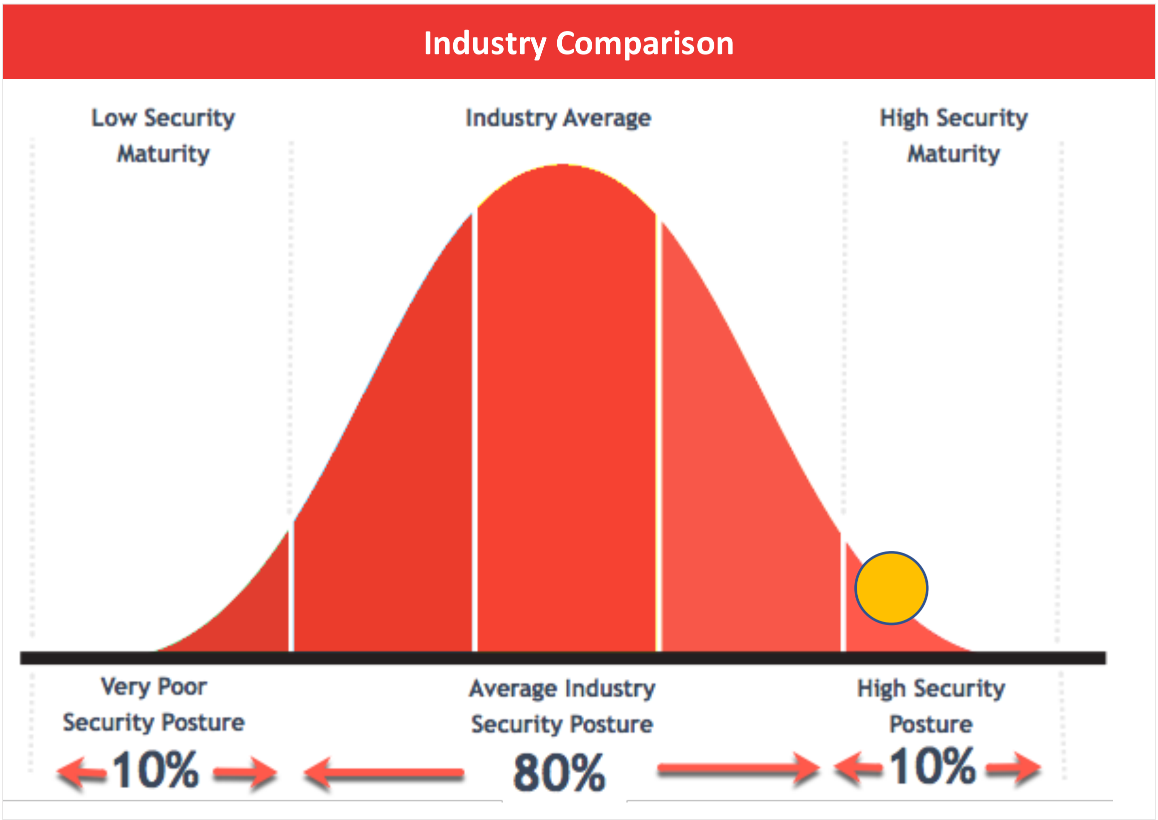


Figure 1. Security posture relative to peers

The yellow ball on the above bell curve shows where Xref aligns relative to their peers. This is based on performing 1000's of penetration tests, comparing similar in-house built applications, industries, and sized IT departments.

The results of this penetration test are considered excellent. Even though the risk identified pose a low risk, the recommendations in this report should be implemented to follow security best practices. There is minimal risk to the business in releasing this application to the Internet in its current state.

3 Scope

Red Cursor was engaged by Xref from the 28th of February 2022 to the 8th of March 2022 to perform web application penetration testing against their Xref application. The environment used for testing was the 'sandbox' environment.

Red Cursor performed both authenticated and unauthenticated testing of the XREF application and APIs which are located at the following URLs:

- api-app.sandbox.xref.com
- api-candidate.sandbox.xref.com
- api-help.sandbox.xref.com
- api-referee.sandbox.xref.com
- api-questionnaire.sandbox.xref.com
- api-search.sandbox.xref.com
- auth.sandbox.xref.com
- candidate.sandbox.xref.com
- employer.sandbox.xref.com
- help.sandbox.xref.com
- id.sandbox.xref.com
- id.sandbox.xref.io
- login.sandbox.xref.com
- referee.sandbox.xref.com
- search.sandbox.xref.com
- template-builder.sandbox.xref.com
- xref-assets.xref.com
- assets.xref.com
- api.sandbox.xref.io (new exit app)
- a.sandbox.xref.io (new exit app)