Xref Recruiter Web Application Penetration Test Report

Prepared for Xref on the 9th of September 2025

Red Cursor

Table of Contents

1 Document Control

1.1 Revision History

Version	Author	Date
Initial Draft v0.9	John Bird	17th of March, 2025
QA and Final Release v1.0	Chris Stevens	26th of March 2025
Retest v1.1	Gordon Maddern	9th of September 2025

1.2 Document Distribution

Version	Date	Details of Distribution
Final Release v1.0	26th of March 2025	Released to Xref as password protected file. Password sent via SMS
Retest Release v1.1	9th of September 2025	Released to Xref as password protected file. Password sent via SMS

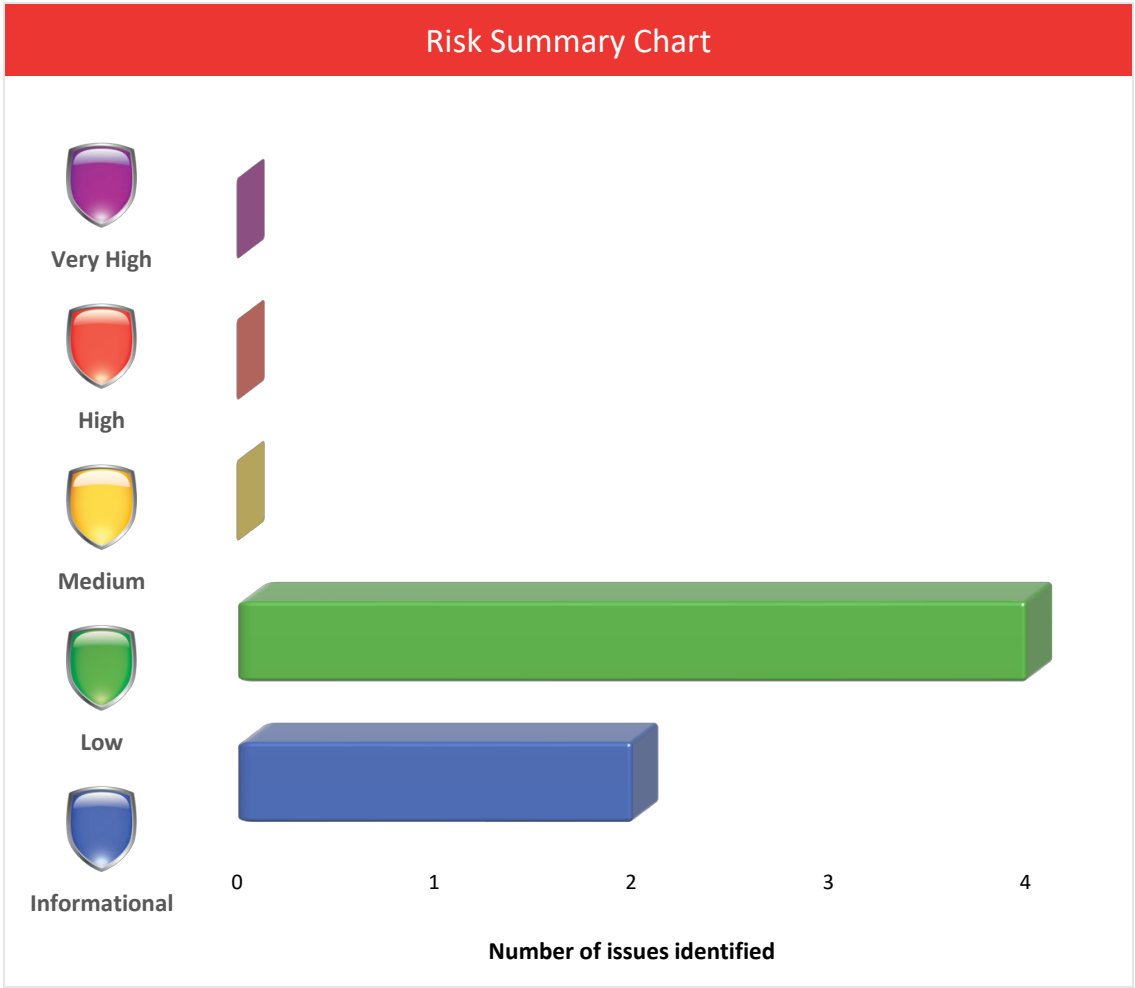
2 Executive Summary

Red Cursor was engaged by Xref on the 17th of March, 2025 to perform web application penetration testing against their Xref Recruiter applications. These application are used by recruiters to manage potential employee references and applications.

Then on the 9th of September 2025 a retest was performed against the initial findings. This report details the results of the retest.

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

After retesting 6 security issues remained. The graph below shows the number and security rating of the risks identified during the engagement:



Of the six vulnerabilities identified, none were rated as high risk.

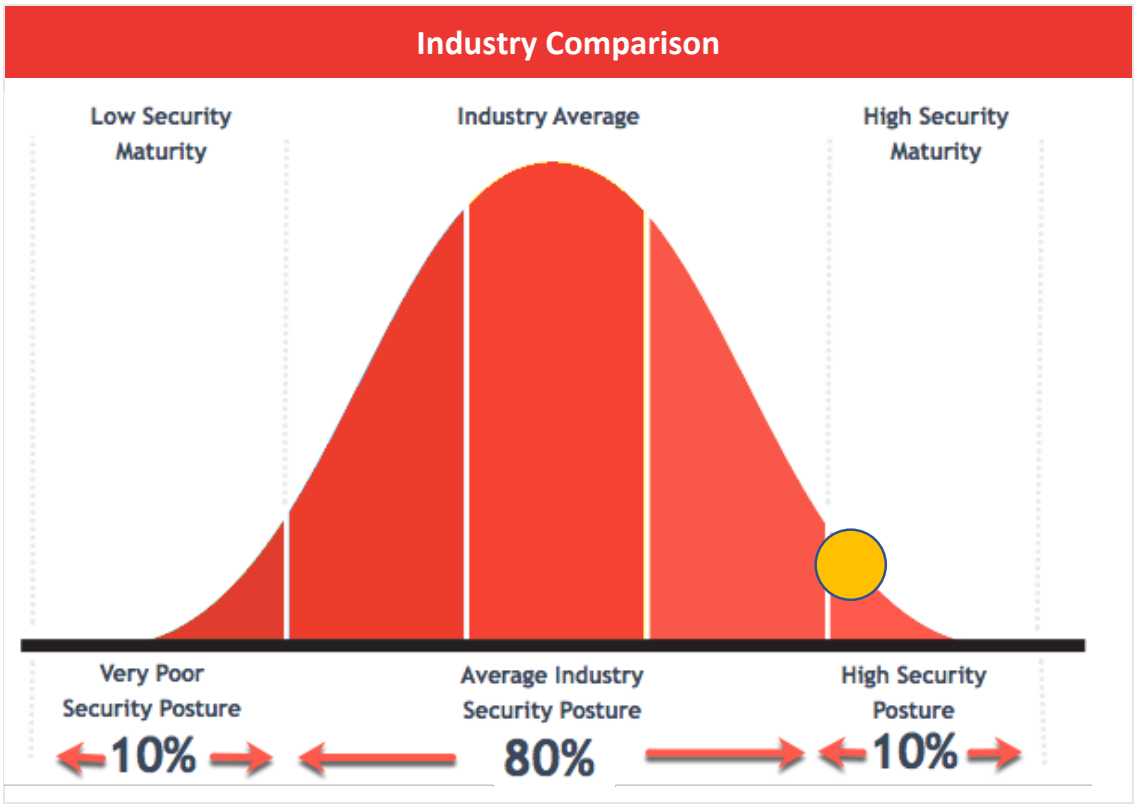


Figure 1. Security posture relative to peers

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

The results of this penetration test are considered above average. There should be minimal risk to the business in exposing this applications to the Internet.

3 Scope

Red Cursor was engaged by Xref to perform web application penetration testing against their Xref Recruiter applications. The environment used for testing was the sandbox environment.

Red Cursor performed both authenticated and unauthenticated testing against the application which is located at the following URLs:

- employer.sandbox.xref.com
- login.sandbox.xref.com
- help.sandbox.xref.com
- api-open.sandbox.xref.com
- report.sandbox.xref.com
- api-app.sandbox.xref.com
- candidate.sandbox.xref.com
- api-candidate.sandbox.xref.com
- referee.sandbox.xref.com
- api-referee.sandbox.xref.com
- api-report.sandbox.xref.com
- search.sandbox.xref.com
- api-search.sandbox.xref.com
- webhook-proxy.xref.com
- webhook.xref.com
- template-builder.sandbox.xref.com
- api-questionnaire.sandbox.xref.com
- api-email.sandbox.xref.com
- api.xref.sandbox.com
- api-router.sandbox.xref.com
- api-xrai.sandbox.xref.com
- api-salesforce.sandbox.xref.com

The following accounts were used during testing:

- pentester1@redcursor.com.au
- john2@redcursor.com.au
- pentester2@redcursor.com.au

Testing was performed from the 17th of March, 2025 to the 24th of March 2025.