20 December 2021

Dovetail
276 Devonshire St
Surry Hills, NSW 2010

Re: Dovetail – Web Application Penetration Test

At the request of Dovetail, CyberCX conducted an independent security assessment on the external facing Dovetail web application. This assessment occurred between the 2nd and the 10th of December 2021. The purpose of the testing was to identify security vulnerabilities within the target of the review and to provide technical details and remediation advice to address these.

The testing included external web application penetration testing and was completed using a combination of automated tools and manual testing techniques. During the assessment CyberCX followed industry recognised best practice methodologies, such as the Open Web Application Security Project (OWASP) guides (which goes beyond the OWASP Top 10 and includes 109 tests) and CWE/SANS Top 25 Most Dangerous Software Errors, in combination with other in-house developed processes and methodologies.

Application testing included verifying and checking of vulnerabilities including; Authentication and Authorisation, Parameter tampering, HTTPS examination, Application mapping, Directory manipulation, Session management, Cookie handling, Cross site scripting, SQL/XML/LDAP Injection and Error handling.

At the conclusion of the review, all identified vulnerabilities were documented along with recommendations on remediation activities that should be completed to improve the overall security posture of the target of the assessment.

Comparing the target of the review to others that CyberCX has reviewed in the past, based on the age, size and complexity of the application, the overall technical risk appraisal of the application was medium, with no high-risk vulnerabilities identified.

Sincerely,

Giles Rothwell

Director, Security Testing & Assurance (UK & US)

CyberCX Pty Ltd