Executive Summary

This report presents the findings of the External Network Infrastructure and Black Box Web Application security assessment conducted on behalf of Thomas International. The assessment was conducted between 28/03/2022 and 31/03/2022.

The systems being assessed were various login forms and API Services.

Overview

The assessment established that the security posture was broadly appropriate to an application of this type. A relatively small number of issues were identified and none were assessed to pose more than a low risk. Nevertheless, it is recommended that these issues are reviewed and addressed in line with a robust defence in depth approach to security.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
External Infrastructure	0	0	0	5	5
Web Application Assessment	0	0	0	3	3
Total	0	0	0	8	8

Assessment Summary

There were no significant issues identified during the external infrastructure assessment, however a number of SSL issues could put information at risk of being decrypted if captured on the network. A clear text service was also discovered however no application was accessible at present. This has the potential to turn into a high risk issue should content be hosted on the service.

The most signification issues within the Web Applications were the misconfiguration of a cookie flag, misconfigured HTTP security headers, and the presence of a username enumeration vulnerability. This could allow an attacker to verify an email address is valid, increasing the risk of a password guessing attack being carried out. Various security headers were not configured to security guidelines and could be used to increase the security posture of the overall system. In addition to this a number of SSL issues were also identified, however the overall risk to the applications is minimal. Thomas International should review the misconfigured SSL services and ensure they are up to date with the latest versions.

The remaining issues were all assessed to pose a low risk or are reported for information only. Nevertheless, it is recommended that these are reviewed and addressed so as to bring the Thomas International's system's within scope into line with security best practice. It is

important to recognise that even low risk issues can be exploited in combination with other issues as part of a wider attack which seeks to compromise an environment or application. In addition, resolving lower risk issues can have the dual benefit of reducing the attractiveness of systems to opportunistic attackers as well as enhancing the overall security posture.

Strategic Recommendations

A number of the identified issues were the result of web servers and applications not configured as securely as possible. Some instances were observed in which weak configurations relating to security headers and a cookie flag were not in use and these configurations are rarely a problem but should be used to bolster the organisations current security. It is recommended that any remedial actions which are undertaken as a result of this assessment should also be reviewed for inclusion in the organisation's secure build standards and deployment procedures for web servers and applications.

Although no significant risks were identified in this assessment, it is recommended that the issues outlined in this report are reviewed in line with a suitably robust defence in depth approach which continuously monitors the organisation's security posture.