

# **| Security Assessment**

**Executive Summary**

This report presents the findings of the External Infrastructure and Web Application Security Assessment conducted on behalf of Thomas International UK. The assessment was conducted between 02/03/2026 and 05/03/2026.

The systems being assessed were a group of web applications and hosts belonging to Thomas International's online estate.

## 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 medium 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 Security Assessment	0	0	1	3	<b>4</b>
External Infrastructure and Web Application Assessment	0	0	0	1	<b>1</b>
Web Application Assessment	0	0	1	2	<b>3</b>
<b>Total</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>6</b>	<b>8</b>

## Assessment Summary

The assessment included an external access check for a number of web applications. The objective was to verify whether these applications were publicly accessible and if they were protected by the authentication portal. The review uncovered a number of accessible applications, and through the use of discovery tools, some hosting files and configuration scripts without authentication were found accessible. The most significant issue found was the presence of a number of publicly accessible URLs, which could be abused through web discovery tools to reveal a range of third party resources, API keys and configuration information. This was coupled with the fact that the web application disclosed sensitive information, whereby API keys used in the hosted web applications were exposed.

The authentication portal used by many of these applications was also reviewed for common vulnerabilities and avenues of attack. No significant threats were identified during this part of the assessment.

Within the external infrastructure assessment, the most significant issue identified was that there were a number of cipher suites which had weak configurations, wherein some of the target hosts used keys with an effective length shorter than 128 bits, which are considered insecure.

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 systems 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**

It is recommended that a further dedicated web application security assessment is performed on the web URLs, from an authenticated perspective. This could give a greater level of assurance than it is possible to provide as a result of a black box security assessment of this type.

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.