

# **| Security Assessment**

**Executive Summary -  
Retest**

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 03/03/2025 and 06/03/2025.

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

## Overview

The security posture of the systems within scope was found to be appropriate to the assets which required protection. Nevertheless, a small number of high risk issues were identified which should be addressed if the organisation’s security model is to maintain an appropriate defence in depth basis. This illustrates the importance of ensuring that an otherwise robust security model cannot be undermined by isolated weaknesses.

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	0	3	<b>3</b>
Web Application Assessment	0	2	0	2	<b>4</b>
<b>Total</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>5</b>	<b>7</b>

## Retest - 23/04/2025

A retest was carried out on the 23/04/2025 to verify the status of the two high severity vulnerabilities. Both of these findings were found to no longer exist, and thus their status was changed to “Fixed”. As a result of this retest, the only remaining vulnerabilities have a low or informational impact, and thus the overall security of the infrastructure has significantly improved.

## 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, in some cases hosting files and configuration scripts without authentication. An issue was raised so that Thomas International can review whether this is expected. In this regard, the most

significant issue found was the presence of hardcoded OAuth credentials in one of these applications. An interim report was created and sent to Thomas International upon the discovery of this issue.

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.

For the external infrastructure assessment the most significant issue identified was Clear-Text Data Transmission, externally facing applications did not use an encrypted transport mechanism. This configuration presented an opportunity for an intercepting party to retrieve credentials, hijack user sessions, and capture other sensitive data.

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**

Consideration should be given to performing an authenticated web application assessment. This will give greater level of assurance than it is possible to provide as a result of a black box security assessment of this type.

Although few 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.