FUJITSU

API Endpoint web app testing

Case study

Comprehensive web application penetration test report + post-engagement presentation and consultation.

Challenge

A financial services company recognised the urgent need to enhance its cybersecurity posture due to the critical nature of its web applications and associated API endpoints which were integral to their operations. With the increasing threats and requirements for annual SOC II assurance processes, the company sought a comprehensive security testing solution to ensure the integrity and security of its web applications.

Solution

To address these needs, the company engaged Fujitsu Cyber Security Services for a detailed web application penetration testing service. This included testing for broken authentication, authorisation, resource consumption restrictions, and identifying flaws in sensitive business flows. Specific testing activities included:

Vulnerability Discovery: External vulnerability scans, service identification and mapping, and vulnerability identification.

Penetration Testing: Testing for vulnerabilities, attempting to exploit any identified vulnerabilities both as unauthenticated and authenticated users.

API Security Testing: Testing for broken authentication, authorisation, and attempting to access sensitive resources through API endpoints.

Outcomes

Following the comprehensive testing, the company received a detailed report outlining the vulnerabilities and recommended remediation steps. The engagement led to significant improvements in the security posture of the company's web applications and API endpoints. This proactive approach not only ensured compliance with SOC II requirements but also fortified the company's defences against potential cyber threats. The company now operates with enhanced confidence in the security of its web applications, supported by continuous collaboration with Fujitsu for ongoing defence optimisation.

Fujitsu Cyber Security Services

fujitsu.com/au/services/security