



# Strengthening security for critical web applications and APIs



**Recognising the critical role of web applications and APIs, a financial services company sought to strengthen its security controls and overall cyber posture.**

## Challenge

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 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.

### Vulnerability discovery

External vulnerability scans, service identification and mapping, and vulnerability identification.

### Penetration testing

Identifying vulnerabilities and attempting to exploit them as both unauthenticated and authenticated users.

### API security testing

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



## Outcomes

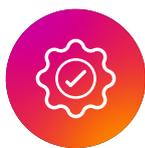
Following the comprehensive testing, the company received a detailed report outlining the vulnerabilities and recommended remediation steps. The engagement led to significant improvements in the security posture of the company's web applications and API endpoints. This proactive approach not only ensured 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.

## Interested in our web app penetration testing?

We use real-world adversary techniques to assess the security of web applications and their infrastructure.

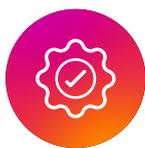
Using OWASP WSTG and focusing on the top 10 threats, it delivers expert-led testing, clear reporting, and remediation guidance to strengthen security and support compliance.



**Delivered** a detailed report highlighting vulnerabilities and recommended remediation steps.



**Achieved** significant improvements in the security posture of web applications and API endpoints.



**Ensured** compliance with SOC II requirements while strengthening defences.



**Enhanced** confidence through ongoing collaboration with Fujitsu for continuous defence optimisation.

## Ready to strengthen your cyber resilience?

Contact us today.

