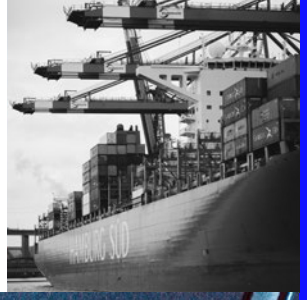

CASE STUDY:
Security Testing

Resolving Website Vulnerabilities Before Go-Live

How penetration testing helped this logistics company resolve critical website security vulnerabilities prior to go-live.

KEY OUTCOMES:

- Critical unauthorised access issue uncovered by penetration testing.
- Issue immediately resolved by the development team.

DELIVERED:

- Security Testing
- Penetration Testing
- Outcome Based

TECHNOLOGIES:

- Silverstripe CMS
- Amazon Web Services

TOOLS:

- Acunetix
- Burp Suite Professional
- SQLmap
- Nikto
- Atlassian Jira

Problem

This logistics company created a new website to support its business. Once the website was completed, the company required a security audit to test for vulnerabilities and provide peace of mind before go-live.

Since the production environment was implemented based on a high performance and availability design, the logistics company needed an external specialist to test the security of the website's functionally within that type of environment.

Solution

The logistics company selected Planit to provide the security audit, testing the website's security on its production environment in the Cloud prior to go-live.

The website has both internal and external gateways allowing for individual user login and administrative access. Therefore, the front-facing component was tested from the perspective of an anonymous, registered, and administrative user.

ABOUT PLANIT:

Following an international best practice methodical approach, we can provide you with in-depth reports into weaknesses that attackers could exploit in your specific systems. We can then work with you to close these loopholes.

Find out how our approach to security testing can help you protect your systems by addressing development, use, and infrastructure!

Contact us →

All webpages and forms of the website were tested over four days against the “Top Ten Web Application Security Risks” by the OWASP (Open Web Application Security Project) Foundation, which are considered the most critical security risks to a web application.

The results from penetration testing were documented and presented to the logistics company. Each of the vulnerabilities was also connected to an identifiable business risk, allowing the company to do budgeting for the fix based on the annualised loss expectancy.

Depending on the severity of the issue, detailed steps to reproduce and fix it were also logged in Jira so the development team could make the necessary changes to the website. Any fixes that needed to be implemented to the website code were first verified on the user acceptance testing (UAT) environment.

Outcome

Our testing found that the high availability and performance configuration of the website’s platform interfered with the authentication mechanism. This issue enabled us to manipulate login sessions and gain unauthorised access to the website.

This issue would not have been detected if the website was simply tested in a UAT environment. It was the in-depth nature of our penetration testing that enabled us to uncover this potentially critical issue.

This issue had to be resolved immediately by the development team, as it interfered with all our interactions on the website. Once fixed, we were able to resume our testing of the website.

Other vulnerabilities uncovered were related to the new code added to the website’s platform by the developer, which caused issues because the new code did not use the in-built capabilities for forms handling and input validation.