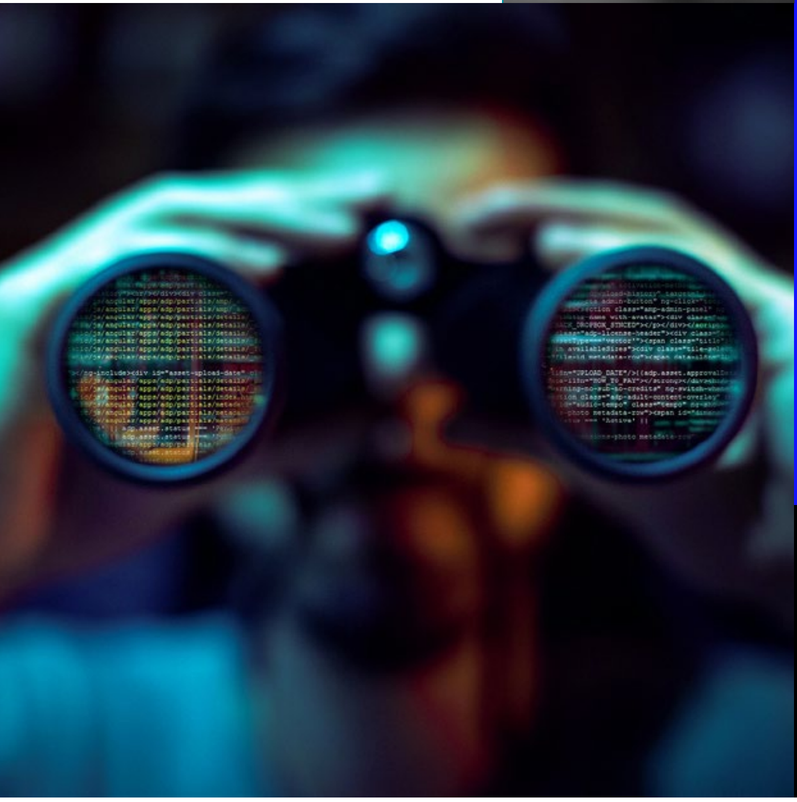
CASE STUDY:
Security Testing

A Safe and Secure Website Experience

How this Government department strengthened the security of its website with our in-depth assessment and consulting.



KEY OUTCOMES:

- Vastly improved security of the website before its go-live date.
- Zero Trust model successfully implemented from improved level of protection.

Problem

This Government department developed a new website portal to replace its legacy one. Since the website would be handling sensitive personal information, the department wanted to ensure the security of the website before go-live, as well as understand how it was integrated and communicating with its other information systems.

Solution

Planit carried out a security assessment of the entire websites and all the backend information systems it integrated with.

When we joined the project, the website was still in development but nearing release. User Acceptance Testing had already been done on the production environment when it was in the build phase.

The goal of our security assessment was to find any vulnerabilities in the following areas:

- The web application itself.
- Integration of the application within the infrastructure, and the application's architecture.
- Its integration with other information systems.

DELIVERED:

- Security Testing
- Penetration Testing
- Outcome Based

TECHNOLOGIES:

- Microsoft Azure Data Explorer (ADX)
- Microsoft Dynamics 365
- Microsoft SharePoint
- Microsoft SQL

TOOLS:

- Burp suite professional
- SQLmap
- Nikto
- Wireshark
- Tcpdump
- Ping
- Telnet
- Microsoft Baseline Security Auditor (MBSA)
- OpenVAS
- GPresult
- WinAudit

- Platform security of the systems on which the application stack was hosted.
- Organisational security maturity.

A three-phase approach was undertaken for optimum coverage and delivery speed of the security testing. Doing so would enable the development team to continue building the production environment where neither the security work nor the other project activities needed to wait for each other.

The first phase consisted of **penetration testing** to assess the security of the Internet-accessible components of the new website. This was done through anonymous and authenticated user access.

Three days of white-box testing was done on the UAT version of the website, which was considered near complete for deployment. This consisted of testing the internal structures and workings of the website, and not its functionality.

The choice of using white-box testing enabled us to gain a very deep understanding of the website and its backend. This then allowed us to test for many potential vulnerabilities in a relatively short period of time, compared to black-box testing, where only the penetration testers' skills are being assessed because only the few weaknesses that the tester has identified are in scope.

The website was also tested 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 this first phase were documented and presented to the department. The summary and detailed steps to reproduce the issues were used by the development team to make fixes to the UAT version of the website before replicating them on the production environment.

The second phase consisted of a three-day security assessment of the website's **integration architecture.** White-box testing was once again carried out, as well as:

- An information systems security audit by an ISACA (Information Systems Audit and Control Association) Certified Information Systems Auditor (CISA).
- Compliance with the ISO 27001 specification for an information security management system (ISMS).
- Compliance with ITIL (Information Technology Infrastructure Library), a globally recognised collection of best practices for managing IT.

As part of this phase, we also interviewed the website's architect and developers, and analysed the documentation of the website's architecture. This provided us with further insights into the ways the website integrated with the other systems.

At the end of this phase, we were able to put together a shortlist of potential entry points to the website which we then analysed further. It was at this point that we identified some potentially critical vulnerabilities with the website's design, such as an unauthorised user being granted full access to all documents on the SharePoint system.

The third phase focused on three days of testing the website infrastructure's **security resilience and configuration.** This consisted of assessing the servers and application stack on which the website had been built, including its network architecture, security zones, Group Policy Objects (GPO), and patch and update mechanisms and procedures.

White-box testing was carried out with a focus on compliance with ITIL and the ISO 27002 standard, which acts as a reference for selecting security controls within the process of implementing an ISMS based on ISO 27001. The back-end architecture was also security tested against the CIS (Center for Internet Security) Critical Security Controls (CSC) and benchmarks.

Outcome

Following the security assessment, the Government department was presented with comprehensive reports for each of the three phases.

The reports contained a summary of found vulnerabilities, in-depth documentation of how they were found, and how to remediate them. Each of the vulnerabilities was also connected to an identifiable business risk, allowing the Government department to carry out budgeting for the fix based on the annualised loss expectancy.

Some of the key issues we discovered related to the website's front-end and were found on the OWASP list. Other vulnerabilities were deeper in the architecture and broke the Zero Trust model the client was pursuing, where anything and everything trying to connect to its systems needs to be verified before granting access.

Thanks to the expertise provided by our security team, the Government department was able to quickly secure the website before its go-live date. Implementing the security fixes was also straightforward with the guidance and expertise of our security team.

By quickly identifying the vulnerabilities and implementing the fixes, the Government department vastly improved the security of the website. They are now able to provide their end-users with a comprehensive online service with a dramatically improved level of protection.

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 →