



## Enhancing security within the development lifecycle ■

CASE STUDY

# 1

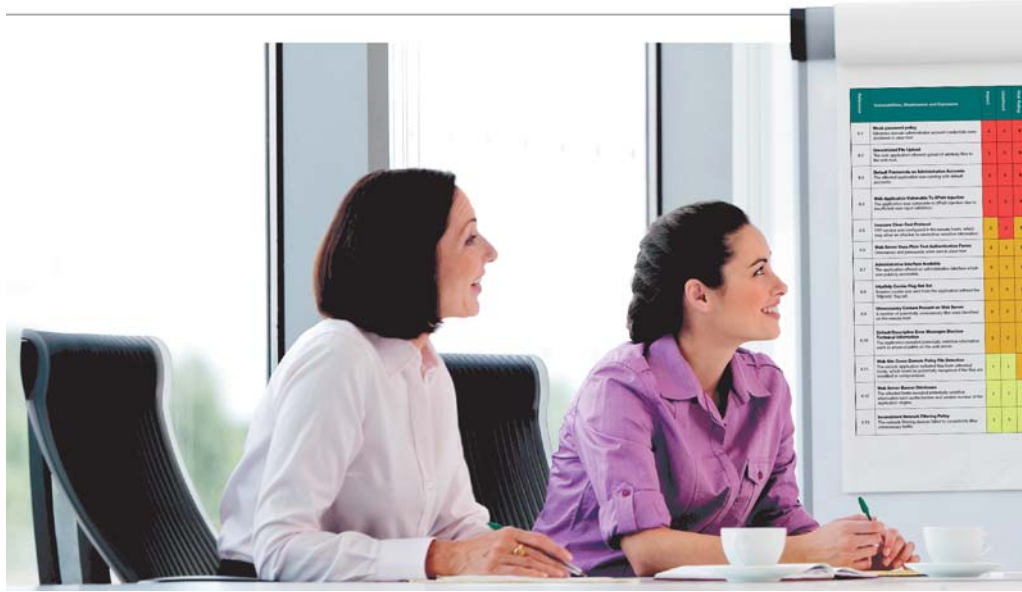


SECFORCE was initially contacted by a large retailer which was in the process of driving sales online and, as such, had an aggressive rapid software development plan in order to achieve this. The nature of our initial engagement was to conduct web application testing against the Organization's applications prior to them going into production.

As a result of our testing, high risk security issues were frequently identified in the applications' logic which required on average, a six week remediation process to resolve. This was a substantial development and financial overhead which caused significant disruption to our Client's hard business deadlines.

## THE PROBLEM

# 2



To address this problem, SECFORCE worked with the Client to embed security into the development lifecycle. This work took the form of a series of workshops, reviews and the implementation of enhanced security practises during a project lifecycle as follows:

- **Defining the security objectives alongside the business objectives**

Conducted as a short workshop using trusted risk assessment methodologies to establish the business criticality and sensitivity of the given system as well as the data it would hold. Key areas of concern were noted, relevant legislation and standards (such as the Data Protection Act and PCI DSS) were also identified. The security objectives were then clearly defined and ratified, and could be stated in the programme plan.

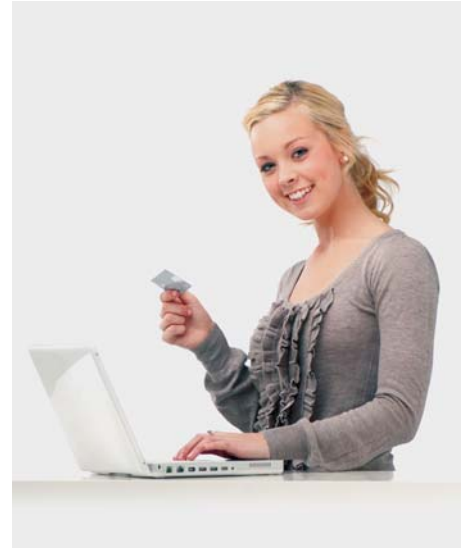
## THE SOLUTION

- **Being on call as an expert security resource throughout the project**

Throughout the project, SECFORCE were on hand as a virtual security programme resource to answer questions, take part in debate and offer insight.

- **Performing early stage threat modelling**

Threat modelling was performed after functionality had been defined and use-case scenarios were documented. At this stage, only a small amount of coding had taken place and it was still possible to make decisions as to what framework and technologies would be finally employed. By combining the use-case scenarios with the security objectives from the previous stage, a trust model was created, mapping out all the trust boundaries, and defining their significance. A security architecture was then defined and coding guidelines drawn up for the security model of the application.



- **Conducting training and knowledge transfer workshops**

In order to effectively utilise the coding guidelines it was necessary to ensure that the development team was comfortable working with them. A workshop was run with the development team to promote awareness of the security concerns, and discuss effective ways of implementing the guideless without compromising the business efficacy of the application. This workshop ensured the effective transfer of knowledge between the SECFORCE security experts, and the project development team.

- **Performing early stage testing and code review**

As soon as early stage code became available, reviews were conducted to ensure elements such as the authentication and authorisation modules were aligned with the security need. Any issues identified at this early stage could then be easily addressed.

- **Conducting a thorough pre-production security assessment**

When the final security assessments were conducted, there were no significant vulnerabilities identified within the application logic. Some low impact issues would be identified with the web server deployment; however these did not represent a significant time or cost impact to resolve.

Our Client now has an effective development lifecycle, with security being well integrated into the programme from the earliest stage. Due to this increased visibility, the Client is able to plan effectively for marketing events, holidays, and other deadlines which affect their business. Projects are delivered to deadline; issue remediation has been cut down to an average of 5 days and is now a planned component of the programme.

- Development deadlines are now achieved
- Application security is enhanced and consistent
- Knowledge transfer has led to shorter project timelines
- Overall development and deployment costs have been reduced

# SECFORCE

SECFORCE is certified by CREST and ISO9001 to ensure the highest standards of security assessment services



## CONTACT US

If you would like further details,  
please get in contact:

SECFORCE UK  
Suite 11, Beaufort Court  
Admirals Way  
E14 9XL London  
TEL +44 (0) 845 056 8694

SECFORCE SOUTH AFRICA  
Palazzo Towers W, Montecasino  
William Nicol Dr, Johannesburg  
Fourways, Gauteng, 2000  
TEL +27 (0) 11 5100 161

[www.secforce.com](http://www.secforce.com)