



Client

A FTSE 250 high street and online retailer.

Project Background

IRM was requested by a client to establish the security profile of their primary business application. Part of this request stemmed from the fact that an ever changing compliance landscape introduced several PCI DSS requirements. IRM recommended a security code review as part of the overall assessment roadmap.

IRM's Approach

Over the years the source code had grown substantially in terms of complexity and lines of code. Reviewing each and every line would have made the engagement impractical and uneconomical. As a result, the first step was to prioritise sensitive areas to focus on for which a list of threats was formulated. Each of the threats was then mapped to sections and classes in the code base where these were most likely to manifest. Once the risk profile and a prioritised list of target classes was developed, IRM consultants subjected the source code to an automated code scanning utility with the aim of indentifying 'low-hanging fruit'. Such tools are generally effective at identifying pattern-based application layer vulnerabilities such as insecure configurations, cross-site scripting, etc. and this appeared to be the case with the engagement.

While developers investigated and implemented bug fixes for findings from the first pass, IRM consultants began manual investigation processes using the prioritised list of areas to focus. On completion, a large number of defects and shortcomings had been unearthed which would have prevented the solution from complying with PCI DSS requirements.

What IRM delivered

IRM delivered a structured report detailing each of the vulnerabilities and shortcomings identified along with how the application fared in comparison to the vendor's secure development guidelines and industry accepted standards such as OWASP Top 10. IRM also included pragmatic approaches to remediating various defects and details on how the application could leverage the development platform's inbuilt defenses to enhance the overall security posture and align itself more closely with applicable standards.

In terms of target audience, information was presented in an actionable intelligent form that enabled various stake holders, ranging from project managers to development teams, to make informed decisions.

Benefits to the Client

On completion, the client was presented with a clear picture of their primary business application's security posture, what was required of them to improve it and inputs on how to progress with its compliance roadmap.

What the Client did next

On account of IRM's input to the project, the client was able to create different remedial work streams using guidance from IRM consultants. Multiple projects were initiated to improve security within the in house development life cycle.

FAST FACTS

Geography

- ▶ UK

Challenges

- ▶ Large and complex source code
- ▶ Lack of previous security profiling

Solutions

- ▶ Risk based Security Code Review

Results

- ▶ Prioritised list of vulnerabilities and how they could be addressed to reduce risk to the business
- ▶ A report that indicated how the code base fared in comparison to industry standards like OWASP Top 10

Information Assurance

Risk Mitigation

Business Resilience

Compliance

