

## **Case Study:                   Application Security Test**

### **Industry Sector:           Retail**

Within the retail sector, web applications play a fundamental role in facilitating business operations. Online e-commerce applications present a multitude of opportunities for an attacker who is interested in gaining access to customers' personal details, subverting the purchasing process to obtain goods or services at less than the advertised prices or simply to cause damage to the retailer's reputation. Poorly-secured web applications can be a liability to a retailer, particularly when consideration is given to legal and regulatory requirements such as the Data Protection Act 1998 and the Payment Card Industry Data Security Standard.

An Application Security Test can help an organisation locate and correct flaws in their applications and application development processes, be they simple coding errors or larger design flaws within the implemented business logic.

#### **Case #1 – How we do business**

IRM was asked to perform an application security test against the website of a large online retailer. Although in many areas the online shop appeared to be secure, IRM discovered that it was possible for users to bypass client-side input validation and enter hidden promotional codes during the checkout process in order to claim student discounts to which they were not entitled. Following the recommendations presented to the client, the error in the application was corrected and proper validation of discount entitlement was conducted thereafter.

Having built a close relationship with the client over the course of a number of similar security tests, IRM was engaged to provide consultancy and assistance with implementing security earlier in the software development lifecycle (SDLC).

#### **Case #2 – Thinking outside the box**

IRM performed an application security test against a well known high-street retailer with an online presence. Functionality within the application allowed customers to reserve stock items for later collection from the retailer's stores. IRM determined it was possible to automate the process of stock reservation such that all items of stock at its stores could be reserved and hence would not be available to be purchased either online or in store – such an action performed maliciously would undeniably cause chaos and could conceivably cause the loss of an entire day's revenue for the retailer whilst the problem was resolved.

This exposure was a direct result of functionality deployed into the application, without consideration for the potential security risks. As specialists in information security, IRM consultants adopted the mindset of an attacker to highlight the design flaw before the threat to business revenue materialised.

#### **Case #3 – The holistic approach**

IRM performed an application security test in response to a security breach in which customer credit card details had been compromised and subsequently used fraudulently. Our consultants were able to gain access to the back-end database holding repeat customer information such as names, addresses and credit card details. In conjunction with a Digital Forensics Investigation, the application security test confirmed the root cause of the compromise.

IRM was able to offer practical remedial advice to the retailer to address the immediate control failures. IRM was also able to provide one of our many PCI Qualified Security Assessors to help ensure that a suitable roadmap to achieving compliance with the PCI Data Security Standard was in place.

#### **About IRM**

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.