

Case Study: Application Security Test

Industry Sector: Gambling

The last ten years have seen the emergence of the online bookmaker, betting exchanges and an explosion of online poker and casinos. The UK gaming market alone is expected to continue to grow in excess of £10bn in 2009, with total turnovers reaching £100bn. Vast sums of money exchange hands daily via electronic means, exposing the gaming industry to risks such as money laundering, fraudulent transactions, denial-of-service attacks, collusion amongst players in online games and automated agents (bots) breaching acceptable use policies.

Furthermore there are legislative commitments as prescribed by the Gambling Act (2005) and the Data Protection Act (1998) combined with regulatory requirements from the UK Gambling Commission and the Payment Card Industry Data Security Standard, all of which can pose technical challenges to the profitability and scalability of an operator.

IRM's Application Security Test can help an organisation to locate and correct flaws in application development, be they simple coding errors or larger design flaws within the implemented business logic.

Case #1 – Understanding the business context

IRM performed an application security test against a bespoke spread betting application. The major finding during the assessment was the ability of a customer to forge a trade request as if it were submitted four seconds previously. Trade requests below a minimum threshold were automatically approved by the system rather than requiring broker intervention; thus it was possible to guarantee profitable trades by waiting for appropriate gaps in the underlying market.

IRM's ability to provide a deeply technical business consultant whose experience of working with investment banks meant that the exploitation of an esoteric vulnerability was presented in terms of meaningful business impact and potential for lost revenue.

Case #2 – Understanding regulatory requirements

IRM performed a routine web application security test for a well known online poker company. IRM consultants were able to rapidly put together a number of detailed security test cases of specific relevance to the client's web application.

Typically operators are required as part of their licensing conditions or through good corporate governance to provide various user protection mechanisms such as deposit limits and self exclusions; these specific controls became a particular focus of the engagement.

Through unauthorised means IRM was able to increase the monthly deposit limit for the test account whilst bypassing the week long cooling-off period. The implications of the client being in breach of licensing conditions clearly resulted in this being more than the typical input validation issue and under IRM's guidance the problem was handled accordingly.

Case #3 – The weakest link

IRM performed an application security test for a UK bookmaker in response to a suspected security breach. Through a marketing site owned by the client IRM was able to leverage a blind SQL injection vulnerability to gain wholesale access to the system, corporate network and data warehouse backend. IRM was also able to gain access to the networked shop floor terminals.

Although the business risks are self-evident in this case, IRM presented some particularly innovative scenarios such as an attacker leveraging access to the web server to replace the online casino and poker software with a 'Trojan horse' designed to stealthily harvest massive amounts of personally identifiable information and payment card details; were such an attack ever to be discovered the reputational damage is clearly business disabling.

Case #4 – Putting it all together

IRM was asked to perform an application test against the website of an online betting company. The website allowed users to register and authenticate to an online account, whereby various online betting games could be played with money from a registered credit or debit card on that account.

A full application layer investigation was conducted, focusing on the registration and authentication mechanisms and the game logic.

IRM found that user accounts could be enumerated via the authentication mechanism using differences in the error responses when valid and invalid usernames were entered. Our consultants wrote a custom script to attempt multiple authentications, using a dictionary of common names such as 'sjones'. Using this technique, we were able to enumerate over 5,000 valid account usernames. Following this a brute-force password guessing attack was launched which identified a poor password policy defined on the application; IRM was able to gain unauthorised access to ~5% of the 5000+ accounts that had been previously enumerated.

Given the unauthorised access achieved, IRM was able to view personal information relating to the account owners and more seriously, was also able to transfer credit from one user's account to another's in the form of a gift donation.

An account lockout was configured upon entry of three invalid passwords for a particular account. IRM was able to demonstrate that combined with the user enumeration issue, it would be possible to cause a denial-of-service to many of the users of the system, ultimately damaging the client revenue stream through reduced business and an increase in load on the offshore helpdesk facility due to customer complaints and troubleshooting calls.

IRM progressed the testing with investigation of the game logic of the various online betting games. By modifying specific game parameters passed between the client machine and the backend servers key errors in the game logic were identified, that in some instances would allow an increase in the probability of winning some of the available games. Abusing this flaw, it was possible to demonstrate though automated play that IRM could potentially utilise this small advantage to defraud the client of relatively large sums of money.

These findings, recommendations and subsequent practical remedial advice ensured that the client could devise a structured and appropriately prioritised approach to address the flaws within the application and game logic.

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.