

Case Study: Secure Application Development Training

Industry Sector: Finance

Application layer vulnerabilities manifest themselves as a result of a lack of a security aware software development lifecycle (SDLC), or simply poorly-written code. Since attackers have shifted focus from network based attacks to exploiting vulnerable applications, it is imperative that organisations introduce processes and controls to minimise the occurrence of code-level security defects.

As vital as code reviews and penetration tests are in improving the overall application security posture, training development staff enhances their level of security awareness and considerably reduces defect density before code undergoes testing and works its way into the production environment.

IRM's secure application development training programmes provide comprehensive coverage of application vulnerabilities at the code level by giving real life examples using an interactive training system. Issues are communicated to developers using their favourite development platforms such as .NET and Java. As a result, IRM's training programmes will help developers understand issues affecting their code, enabling them to be more security aware, both at code and process levels.

Case #1 – Delivering Security

IRM was asked to conduct a workshop for the .NET development team at one of its financial services clients. Prior to the workshop, IRM had conducted a code review on a large scale application used by the client and was aware of issues that the team faced. Using this as input, IRM consultants tailored a workshop to suit the needs of the development team and specifically cover known problem areas.

Using an in-house developed training system consisting of a sample enterprise application, common application vulnerabilities were covered both from a 'black box' perspective and at the source code level. Developers were briefed on what the issues were, how attackers would try to exploit them and how they could remediate against such vulnerabilities. The development platform's security features were also covered, including how these frameworks help to reduce time and effort required to implement security functionality. Furthermore, security processes such as Threat Modelling and how these could be suitably integrated into the client's SDLC were also discussed.

Another key feature of IRM's workshop is the requirement to have a mix of both senior and junior developers present for each session. Throughout the workshop senior developers are prompted on particular topics to provide examples that are material to the client and thus facilitate the knowledge sharing process.

On completion of the workshop, IRM conducted a further code review on a separate application to which the developers had applied a more robust approach to secure development. It was observed that the defect density had reduced considerably and the overall code quality, in terms of security, had been substantially improved.

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.