

Application Security Test

Businesses evolve, grow and change. As part of this evolution IT applications are deployed, improved and optimised. These applications, be they websites, transactional systems or data entry applications, often deal with sensitive information and have a key role in marketing the brand of an organisation.

IRM's Application Security Test provides a comprehensive assessment of the security posture of the application, detailing all vulnerabilities discovered, along with recommendations for mitigation and a clear indication of the risk posed by each issue.

A complete application security test includes the following phases:

- **Functional Review and Threat Assessment**

The application will be evaluated from the perspective of an ordinary application user. Any available documentation will be examined and a detailed picture of the application functionality will be established. Potential threats and attack vectors will be identified in order to position the later stages of the test effectively.

- **Analysis of the Supporting Infrastructure**

The infrastructure hosting the application will be assessed. Relevant networking components such as load balancers, SSL terminators or proxy servers will be identified. Attempts will be made to establish the version of any supporting server software in operation. Once the environment has been enumerated, IRM will determine the infrastructure's susceptibility to vulnerabilities and identify other weaknesses and exposures using manual techniques and automated tools.

- **Application Mapping**

From the perspective of a normal user, IRM will enumerate the functionality present and determine all possible points of interest to an attacker. Any functionality will be thoroughly checked for weaknesses including, but not limited to, SQL injection, cross-site scripting and logic errors which might facilitate unauthorised access to the application or data.

- **Business Logic Review**

A crucial phase of any application test is a review of business logic and the intended functionality of the application. In this phase, the business logic of the application will be assessed with a view to determining whether any logical restrictions within the application can be bypassed, or whether areas of intended business functionality may be abused to cause damage to the business.

- **Subversion Attempts**

Finally, IRM will attempt to leverage any weaknesses discovered in the previous phases to escalate privileges, or to gain unauthorised access to other data or systems.

- **Deliverables**

IRM will deliver a formal report including an executive summary, a risks and recommendations table detailing the high-level results of the assessment and a detailed description of each issue discovered including remediation advice.

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.