

Software Product Review

How do you know what security vulnerabilities are present within the product you have developed? Even the best automated software security auditing products on the market still require expert analysis of the results to remove false-positives.

IRM's Software Product Review service evaluates the security of all areas of your software using a combination of different tools and techniques to ensure maximum code coverage.

A complete software product review includes the following phases:

- **Software Design and Documentation Review**

The design of the software product is reviewed, comparing it to best practices. Attack scenarios are developed with reference to the security requirements of the product, which are used later in the testing phases. This information is gathered through interviews and documentation review.

- **Static Source Code Review**

Security flaws present in the product's source code will be identified using a combination of in-house developed and commercial tools and techniques. The areas of code investigated are focused based on the attack scenarios developed in the initial phase of the assessment. Static analysis will identify vulnerabilities such as:

- Memory corruption bugs (stack overflows / heap overflows etc.)
- Format string errors

- **Manual Analysis and Automated Fuzz Testing**

This phase comprises a 'black box' approach to software assessment using automated fuzzing tools to send structured semi-random data in order to identify vulnerabilities. This approach is more suited to the identification of vulnerabilities such as:

- Race conditions
- Logic errors
- Memory leaks

The second two phases are usually performed concurrently, as vulnerabilities identified using 'black-box' techniques normally require source code analysis to identify the root cause.

- **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.