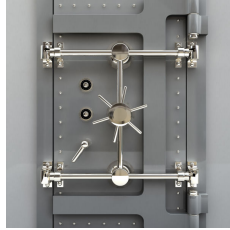


## Web Application Design Review



*For critical e-commerce applications it is important to involve security specialists in the all stages of system development, including design, integration and testing.*

### The Need

Project managers need to understand the principal security concerns and identify the mechanisms and procedures used to counter them.

They want a practical assessment that can be modified in the light of feedback and subsequent, more detailed examinations. The security assessment can also be used to identify and focus our own efforts on the security relevant areas of the system and its development.

### Our Service

We review the design and implementation of the main components of the system in detail. In particular, we concentrate on the engineering of those components of the system considered by a risk and threat assessment to be security relevant.

Particular attention is paid to:

- user registration and authentication
- session management and continuity mechanisms
- input checking and validation techniques
- protection of user and commercially sensitive data
- preserving the integrity of the content
- use and protection of privileged functionality
- interfacing with third parties
- auditing and logging

Security concerns and observations are recorded in a *security risk register*, a test strategy produced, and draft customised guidelines on secure web application development practice are provided.

We also address Operational Acceptance Support, including:

- application level mechanisms for detecting abnormal usage
- mechanisms for detecting unauthorised modification of application configurations
- procedures for handling application security events
- facilities for the management of privileged user accounts
- processes for re-testing the applications after changes

## What You Get

The *Security Risk and Threat Assessment* is a living document, drafted as soon as possible, circulated for review and then maintained in light of comments received and subsequent security reviews and testing.

The *Test Plan and Schedule* identifies the range and types of security testing to be performed. Wherever possible it identifies the details of the tests. However, by its nature much of the user security testing is an exploration of the exploit opportunities as they are discovered. In these cases the plan will not identify specific test cases, just the type of testing and the goals set.

The *Risk Register* is started at the beginning of the project and maintained on through into the lifetime of the system. Essentially, the risk register is a continuation of the Risk and Threat Assessment. While the assessment is a top level document, the risk register is used to capture all of the security issues discovered by the review and testing. In each case remedial options are identified.

The *Final Report* itself is a distillation of the results and findings of the security review and testing. It provides a management summary of the findings and recommendations.

## Our Track Record

We have carried out a full web application assessment for a national newspaper with a significant Internet presence. This encompassed design and procedural review as well as active testing, and required close working with the client's staff and third party developers.

We carried out a similar study for a business-to-business Internet company in Scotland, working with them during development and launch to ensure security at both the platform and application level.

A mobile phone company has engaged our services over a long period to assess a stream of more than 20 web and text messaging applications, covering design review, implementation checking and practical testing.

A European finance ministry used us to check the security of its on-line tax return submission portal.

## Related Services

**Web Application Testing** Classic penetration testing at the network level has its place but many new attacks are aimed at interactive web applications. A thorough external test can minimise these risks.

### **Feel Good About Your Network**

*IDsec is an independent company specialising in network security. We can assess your security and advise on long-term protection: as we have for a range of blue-chip clients since 1997.*

**IDsec**

31-33 College Road, Harrow, Middlesex HA1 1EJ, United Kingdom  
T: +44 20 8861 2001 F: +44 20 8861 3433 W: [www.idsec.co.uk](http://www.idsec.co.uk)

All prices exclude VAT and are subject to confirmation.  
Copyright © 2009 IDsec Limited

[services/testing/application-review.pdf](#) 20091019 (5.09)