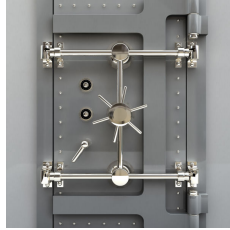


Web Application Security Testing



Penetration testing at the network level has its place but many attacks are aimed at interactive applications or machine-to-machine services. Thorough external testing minimises risks.

The Need

It is important to test whether users of an interactive application such as an on-line bank can carry out unauthorised transactions. Can they gain access to data belonging to other users or the organisation itself, even if this is only at the embarrassment level? Or can they break the application and disrupt the whole service? And what about web services, offering interaction between systems across the Internet?

Application Testing

We explore the ways of breaking security mechanisms that an intruder might try, plus common user errors that may lead to unintended functionality. Some of this is automated but web application testing is mainly a manual exercise, based on experience and an understanding of the context of each interaction.

Testing starts with a discovery phase:

- identification of any *generic products* used and their patch level
- *mapping* the site and the transaction pathways offered
- identification of the mechanisms used for *session* management
- selecting the *key areas* that require security testing

Then, using test user accounts, we probe for known areas of security weakness, based on the Open Web Application Security Project (OWASP) “top ten” but with attention given to the inherent logic of the application:

- parameter and hidden *field tampering*
- reliance on *client side validation*
- *cross site scripting* vulnerabilities
- *cookie tampering* and management
- *session management* vulnerabilities
- appropriate use of *SSL*
- *command injection*
- *buffer overflow*
- bypass and misuse of *registration and authentication* mechanisms
- robustness of the business *logic* in handling misuse and abuse.
- removal of *debugging* and default functionality

Web Services

As well as applications aimed directly at users with web browsers, there is a growing number of web services that provide interaction between systems across the Internet.

Although they do not have the same visibility as the applications that are familiar to all of us as web users, these services are equally susceptible to abuse and therefore need careful design and testing. In fact, it could be argued that web services are more worrisome because they offer a more direct channel to corporate and other sensitive data.

As usual, our approach to testing concentrates on message encryption and other security mechanisms, checking that they have been implemented correctly and completely, with no errors or omissions in configuration.

What You Get

We provide a report listing the tests carried out and detailing each vulnerability found, including our view of the likelihood that an intruder can exploit it to gain access to unauthorised data or facilities.

In analysing the results and putting together a report we pay particular attention to double-checking any vulnerability encountered. We give a *prima facie* view of the severity level of each vulnerability, but we recognise that the overall assessment of risk is beyond the scope of an external testing exercise and is ultimately the responsibility of the client. Where possible, we determine fixes for any vulnerabilities found.

The Price

The cost of this service depends on the complexity of the target site, but a guide price for an entry-level test is £4,500.

Our Track Record

IDsec has been carrying out web application testing projects since 1998, covering the telecoms, finance and government sectors.

We have tested the security of a number of web applications for two UK mobile phone operators.

A business-to-business web site used IDsec to check a commodity selling application.

A City investment management company commissioned us to carry out extensive testing of its on-line portfolio management service.

Related Services

Network Penetration Testing	External penetration testing puts us in much the same position as a potential intruder, trying to break into the Internet gateway and systems behind it.
------------------------------------	--

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

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

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