Web Application Testing

The challenge

Websites and web applications are a popular target for hackers, with almost half of all incidents in the second half of 2004 falling in to this category*. Web site/application hacking is the single most popular type of attack because:

· It’s quick and easy: no special tools are necessary and the attack method can often be as simple as appending a few characters to a URL or form field.

· They bypass traditional security infrastructure: firewall and IDP solutions are ineffective against browser based attacks, which are functionally identical to legitimate web site/application traffic.

· Maximum payoff for minimum effort: incredibly simple attacks can be used to gain or escalate user privileges, bring down sites or to gain a foothold within your network for more extensive probing.

Hundreds of thousands of commercial websites and web applications are vulnerable to one or more of these surprisingly simple exploits. How do you find out if yours is one of them?

* Source: Symantec - 48% of all vulnerabilities in the second half of 2004 appearing in web sites and web based applications.

> “mistakes are a
> fact of life. It is
> the response to
> the error that counts”
>
> - nikki giovanni

evolution

Web Application Testing

The solution

Evolution can scan your website and/or web based applications for the holes used by application level threats, in addition to performing probes much as a hacker attempting to compromise your site or database would.

We partner with global leaders in web application security whose tools form the centre of our web scanning toolkit. By combining tools, knowledge and expertise from a variety of leading sources we can guarantee the best possible assessment of your exposure to this kind of attack.

We perform a non-destructive scan and audit of your site/application, review results and provided detailed reports on your exposure to attacks such as:

- Cross site scripting attacks.
- SQL Injection exploits.
- URL and hidden form field manipulation
- Cookie and session poisoning of spoofing
- Attack via. Back doors in your own or third party applications
- Buffer overflow attacks
- SOAP and web services flaws

Information is presented in plain English alongside resources to help you close any security holes, and is backed up by a detailed technical report available in a variety of formats.

If required our results can be presented in person, giving you a chance to question our consultant and gain a fuller understanding of the issues and challenges of web security.