

Web applications penetration testing



The most rigorous security testing for the most vulnerable part of your network.

Why do you need to review your web applications?

About three quarters of all security breaches are due to vulnerabilities in web applications (Gartner Group estimate). Without a clear picture of coding and application vulnerabilities to your business is open to the malicious or accidental actions of attackers or employees. Strong web application security is vital for protection against potential loss of revenues. And you need to make sure your business is meeting all data protection regulations, especially if you're running e-commerce systems, online payment applications or content management systems.

How web applications penetration testing helps

The testing allows you to identify all unethical hacking weaknesses of the web sites you use. It shows whether a website can be defaced and identifies if a transactional website can be breached. It keeps you compliant with current regulations, safeguards your corporate image and keeps customer details safe.

Our web application review service includes

- Business assessment
- Architecture assessment
- Authentication review
- Non-repudiation evaluation
- Session management audit
- Denial of service (where necessary)
- Web services testing
- Web 2.0 review
- Revision-level review

"Our testers use the same tools and tricks employed by hackers. We typically simulate worst case scenarios, attempting to break into applications both online and internally."

Eamon Flavin, ACSN Technical Director

Benefits for your organisation

- Your brand reputation protected and maintained
- Confidence of best practice applied to the application testing process
- Revenue loss minimised

What we do

We combine functional testing with pre-emptive tests to give you the best possible protection from the consequences of a breach.

We'll review all aspects of your web applications in depth, including type of session management and cross-site scripting (XSS) susceptibility. We often do this 'blind' – to recreate the conditions faced by potential hackers.

We tailor the service to suit each organisation – including the applications used and the specific processes they support. We'll always help you find the best way to deal with any problems we find, and we target high risks immediately, by simulating an escalation to worst case.

At the end we'll put all findings and suggestions in a report, with any vulnerability clearly ordered by risk. Some assessments take only a few days while others (for example a new banking application) involve a longer, more project-based iterative process.

Call us on 0207 324 6250 or email info@acsn.co.uk to learn more.

ACSN is an [Approved Scanning Vendor](#) recognized by the PCI Security Standards Council