



FIRST • BASE  
technologies

Ethical

Pragmatic

Professional

Web Application Testing

## We are Penetration Testers • Full Stop •

- Are your web servers vulnerable to attack?
- Could an attacker obtain credit card details from your back end server?
- Could your web server be used as an entrance point onto your network?

**How do you answer these questions?**

### The Target: Your Web Application

The majority of web applications fall into one of two categories

**E-Commerce Applications:** applications involved in the buying and selling of products or services, or simply providing authenticated access to sensitive information.

**Brochureware Applications:** provide pages of information in a static form, although they may have simple contact forms or a search facility.



### The Threat: Web Application Security Risks

Attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet. These vulnerabilities are being exploited widely to convert trusted web sites into malicious websites serving content that contain client-side exploits. SQL injection and Cross-Site Scripting flaws in open-source and custom-built applications account for more than 80% of the vulnerabilities being discovered.

Despite the enormous number of attacks and the widespread publicity about these vulnerabilities, most web site owners fail to scan effectively for common flaws. They become unwitting tools used by criminals to infect the visitors that trusted them to provide a safe web browsing experience.

### The Solution: A Web Application Penetration Test

No matter how careful you are during development, the only way that you'll be certain that your web site is as secure as possible is to have it independently tested. Professional penetration tests should be conducted before your application goes "live" **and** whenever you make any significant changes **and** on a regular basis (at least annually). By engaging skilled testers, you can ensure that new vulnerabilities are exposed and fixed before the bad guys exploit them.

**This is where we come in...**



FIRST • BASE  
technologies

Ethical

Pragmatic

Professional

Web Application Testing

## We are Penetration Testers • Full Stop •

Our Web Testing Services are conducted by skilled professionals using best practice as described by OWASP and our own proprietary testing techniques.



**Scope:** we discuss your requirements in detail to ensure that tests are appropriate, accurate and cost-effective.

**Testing:** is carried out by one or more of our professional testing team and includes the elements listed in the table below.

**Reporting:** our reports include a management summary, vulnerabilities ranked by severity, recommendations for remediation and detailed technical explanations. The layout and format can be tailored to meet your in-house requirements.

**Quality:** Every test is carried out by a highly trained professional. Their results are subject to both technical review and quality assurance before being securely transmitted to you.

**Post-Test Discussion:** you can discuss your test results with our testing team to ensure that the risks and recommendations are understood in the context of your business.

**Re-Test:** Once you have addressed the reported vulnerabilities, we can check that your fixes have been successful or conduct a full re-test of your site.

### The tests we conduct include:

**Information Gathering:** This first phase of security assessment is focused on collecting as much information as possible about a target application. Information gathering is the essential first step of a penetration test.

**Business Logic:** Business logic can contain security flaws which permit a user to do something that shouldn't be allowed by the business, for example changing the price of an item during the ordering process. Frequently, business logic checks are simply not present in the application.

**Authentication:** Authentication is the process of attempting to verify the user's digital identity, for example during user logon. Testing authentication means understanding how the authentication process works and attempting to circumvent the authentication mechanism.

**Session Management:** The core of any web-based application is how it maintains state and controls user-interaction with the site. Session management broadly covers all controls on a user, from authentication through to leaving the application.

**Data Validation:** The most common web application security flaw is a failure to properly validate input before processing it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

**Access Control:** Authorisation means only allowing access to resources for those permitted to use them. Testing for proper access control involves understanding how the authorisation process works, and using that information to attempt to circumvent the authorisation mechanism.

**Error Handling:** Error codes and how errors are handled can reveal a lot of information. During testing they can inform us about databases, bugs, and other components directly linked with web applications, leading to potential exploits.

**Server Configuration:** Analysis of the infrastructure and architecture can often reveal a great deal about a web application. Source code, permitted HTTP methods, administrative functions, authentication methods and infrastructure configurations can all be informative.

**Job Done:** We pride ourselves with being with you every step of the way in securing your web applications from attack.

Get your quote now

Call Andy on +44 1273 45 45 25 or e-mail [info@firstbase.co.uk](mailto:info@firstbase.co.uk)

[info@firstbase.co.uk](mailto:info@firstbase.co.uk) • [www.firstbase.co.uk](http://www.firstbase.co.uk) • +44 (0)1273 45 45 25