



FIRST • BASE
technologies

Ethical



Pragmatic



Professional

We are Penetration Testers • Full Stop •

- Could an attacker steal credit card details from your database?
- Is your database vulnerable to SQL injection?
- Can anyone - or anything - execute arbitrary commands on your database?
- Can just anyone assume a DBA role on your database?
- Is your Oracle Listener Service listening to everybody?
- Is your sensitive data encrypted in transit and in the database?

How do you answer these questions?

The Threat: Database Security Risks

Database servers often hold some of your organisation's most sensitive and valuable information, such as financial and credit card data, customer or supplier details, or employee records. These servers can be seen as the "crown jewels" of your organisation - the impact in terms of reputation and cost could be significant should such information get into the wrong hands.



You may already undertake regular web application tests, which help protect against remote attacks against the databases behind your web applications. That's essential work. However, there's a bigger threat to your databases - the people that steal information and commit fraud are often internal to an organisation or its business partners.

Of course you'd expect every organisation to have its crown jewels safely locked up against any source of attack. Yet we often find that this is not the case. Database servers advertise themselves on internal networks, sometimes with default passwords and unencrypted data, providing attackers with an open back door. Insiders can steal company secrets, intellectual property or credit card details right off your network, making it critical to test the security of your databases from inside the organisation.

The Solution: A Database Penetration Test

No matter how careful you are, the only way that you'll be certain that your databases are as secure as possible is to have them independently tested. Professional penetration tests should be conducted before a database 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...

Database Security Testing



FIRST • BASE
technologies

Ethical

Pragmatic

Professional

Database Security Testing

We are Penetration Testers • Full Stop •

Our database testing services are conducted by skilled professionals using best practice 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 can include 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.

The tests we can conduct include:

External Testing: can be conducted via your web application - see our web application testing page for more information.

Database Audit: is a full review using legitimate credentials you have provided for us and employing tools and techniques that are appropriate to the devices and products in use. We can also review your database account and access control policies (normally via an on-site meeting with a DBA), and associated security countermeasures against industry best practice. The test report consists of the audit findings and the results of the on-site discussion.

Database Penetration Test: using a variety of tools, the goal of this exercise is to gain access to the database and, if possible, gain administrative control over the database.

Authenticated Server Audit: this examines server operating system patch levels, vulnerabilities associated with running services, best practice for server build standards and security policy settings.

Datastream Analysis: looks at the SQL datastream between the application and database.

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

Get your quote now

Call Andy on +44 1273 45 45 25 or e-mail info@firstbase.co.uk

info@firstbase.co.uk • www.firstbase.co.uk • +44 (0)1273 45 45 25