



FIRST • BASE
technologies

Ethical



Pragmatic



Professional

We are penetration testers • Full stop •

- Can anyone steal **customer details** from your database?
- Is your **SQL database** vulnerable to injection?
- Can just anyone assume a **DBA role** on your database?
- Is your **Oracle Listening Service** listening to everybody?

Answer these questions by using our database security testing services

The Issues: Why Do I Need Database Security Testing?

Your database servers usually hold some of your organisation's most sensitive and valuable data: client, customer, supplier or employee details, financial information and credit card data being just some examples. As such, these servers may be considered to be the "crown jewels" of an organisation - the impact in terms of reputation and cost could be significant should such information get into, and be exploited by, the wrong hands.

You may be familiar with external web application testing. Such testing provides an organisation with a good level of assurance as to their security status against **remote** attackers being able to access a database behind a web application. But, whilst it is indeed essential to test and then ensure adequate countermeasures are in place to prevent remote attacks, the most common threat to your database is not from an external source - in fact the people that steal the information necessary to commit crimes such as fraud are frequently **internal** to an organisation rather than external.

However, whilst you would expect an organisation to have its "crown jewels" safely "locked up", against *any* sources of attack, we have frequently found that this is not truly the case concerning internal attacks. Database servers advertise themselves on internal networks offering default unsecured TCP port services. An attacker on the network could attempt to circumvent any controls that are in place in order to steal whatever interesting data is on your database such as credit card details. Thus, it is **as** important - if not **more** important - to test the security of your databases from an internal attack perspective as it is to test them from an external attack perspective.

The Solution: First Base Technologies' Database Security Testing Team

Our expert Database Security Testing Team (DSTT) can assist you in obtaining full assurance against the issues raised above by:

- **Externally** testing for vulnerabilities that would permit an attacker to compromise your database remotely via your front end web application
- **Internally** testing for vulnerabilities that would permit an attacker to compromise your database via your internal network

The reports we produce, which can be tailored to your requirements, will inform you of the vulnerabilities found and provide information as to how to fix them. And, we will provide you with post-test discussions and meetings to assist you on your journey towards being able to answer "no" to the types of question posed at the top of this page.

Database Security Testing

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



FIRST • BASE
technologies

Ethical



Pragmatic



Professional

Database Security Testing

We are penetration testers • Full stop •

The Services: So what can we offer?

The following services can be offered individually or as a package depending on your requirements:

1. External testing via your web application - see [here](#) for more information.
2. We can run a complete Database Audit 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.
3. We can conduct a penetration test of your database 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.
4. We can conduct an infrastructure test of the server that hosts the database (as per the above). Firstly this will examine TCP and UDP services for security vulnerabilities. Secondly we will examine whether it is possible to gain administrative control of the server. If we succeed in the latter, we will then attempt to gain administrative access of the database itself.
5. We can conduct an authenticated server audit which examines patching levels, vulnerabilities associated with TCP and UDP services, best practice concerning server build quality and group/local policy settings.
6. We can conduct a security analysis of the SQL datastream between the application and database.

Every test is carried out by a highly trained professional. Their findings are reviewed by a senior technical member of staff and the final report, which can be in a format tailored to your requirements, is inspected by a partner before being sent to you.

Once you've received your report, we provide an in-depth discussion of our findings to ensure that the vulnerabilities and solutions are relevant and properly understood. We will also provide support and advice in the future.

Thus, at First Base Technologies, we pride ourselves in ensuring that we are with you every step of the way in attempting to secure your databases from attack.

Want more information?

- **Phone Andy** on +44 (0)1273 45 45 25
- **Visit** <http://www.fbtechies.co.uk/Content/WhoWeAre/contactform.php>
- **E-mail** info@firstbase.co.uk

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