



About Enex TestLab

“The world’s premier independent testing laboratory.”

Since 1989 Enex TestLab has helped the world’s biggest companies minimise risk, improve products and save money.

Enex TestLab provides high quality independent testing services and advice.

Our range of testing include:

- Software <
- Hardware <
- Systems <
- Security <

Usability & Accessibility <

Gaming, Wagering, <

Lotteries & Casinos

Media & Communications <

Physical & Materials <

Test with Enex TestLab, not your customers!

Penetration Testing

About Penetration Testing

The best way to understand the security of your systems is by testing them, using the real-world tools and techniques of sophisticated hackers.

Enex TestLab’s professional penetration testing fuses ethical hacking with a methodology designed to identify meaningful information about the specific risks to your business systems and data. Appropriate mitigation strategies can then be recommended.

Our holistic test approach also focuses on the related people and processes; addressing social engineering principles through the methodology.

About Vulnerability Assessments

Vulnerability assessments are a more simplified exercise to simply discover potential security weaknesses, whereas penetration testing attempts to go further, validating and exploiting these weaknesses.

About Enex TestLab Penetration Testing Services

Enex TestLab is a global leader in security and security testing. We specialise in high quality, cost-effective penetration testing and vulnerability assessment services designed to truly target each component of your system.

Enex’s penetration testing and vulnerability assessment services are designed to provide complete flexibility, enabling you to undertake security evaluation and testing at a level relevant for your organisation.

Our penetration testing and vulnerability assessments encompass:

- > Applications and databases including web facing, in-house and bespoke
- > Infrastructure components such as firewalls, gateways, routers, proxies and wireless devices
- > Systems including mobile and fixed devices, from a simple, single server right up to an entire n-tier ISP or data centre environment
- > All software and hardware platforms.

Enex TestLab blends automated toolsets with sophisticated manual processes and testing techniques to eliminate false-positive results, ensuring maximum value for our customers.

Systems can be externally tested (remotely over public and/or private networks) and/or internally assessed (on customer sites) ensuring no disruption to your operations, and that every angle is considered.

Enex TestLab is serious about quality, we adhere to Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) peer reviewed standards.



Testing

A Typical Penetration Test

Rules of engagement

The type of testing is entirely defined by the customer (applications, infrastructure, systems or a combination of all three).

All testing targets are identified (by type, IP address and/or physical location) and documented during project scoping. Instructions are outlined for type of assessment to be used for each target (typically passive scanning with or without active exploitation and/or fuzzing).

The level of target/system prior knowledge to be revealed to the tester is defined (white/grey/black box testing).

Additional considerations including any white-listing of attack devices, source (attacker) IP addresses, and a time window (office hours and/or out-of-hours) for testing are also formally defined.

Authorisation and legal requirements

Enex TestLab treats authorisation extremely seriously. Testing only begins once formal confirmation of the scope and activities is agreed and comprehensively signed off. This includes establishing that all targets (and any related infrastructure) are your own, and testing against each target within the scope is thoroughly understood.

This stage also identifies and addresses any relevant legislation applicable to the tests and locations.

Success: An Example

Recent Enex testing for a well-known media publisher identified and successfully exploited six high priority vulnerabilities. Each of these vulnerabilities would have enabled a malicious hacker to take control of the organisation's core systems, including, alarmingly, its web application database.

Our testing and evaluation processes alerted the publisher to these risks and enabled the most appropriate mitigation steps to be taken. Importantly, this customer was also able to use Enex's findings to improve its entire security strategy and posture for the long term.

Information and data backup tasks

Backups of all systems and data are mandatory prior to testing. Testing will not begin unless fully restorable backups are verified.

Discovery scan of targets and vulnerabilities

Enex TestLab performs a scan of the targets using a combination of tools and techniques. Results are manually verified.

Exploitation and fuzzing of targets

If agreed and authorised as part of scoping, Enex TestLab will attempt to exploit targets using real-world hacker tactics – providing the ultimate insight into your systems' security.

Reporting and results

A comprehensive report is provided, detailing technical and risk priority assessment results, as well as a summary report suitable for a non-technical audience.

Effective communication and understanding of results is vital. Enex TestLab uses clear, concise language throughout its reports, and expert testers are available to provide further clarification.

> Website

www.enextestlab.com
enquiries@enextestlab.com

> Australia

+61 3 9436 7454

> China

+852 8125 2550

> United States

+1 415 287 0992

> United Kingdom

+44 1633 647 898