Our Web Application Vulnerability Assessment services

Our team of ethical hackers can identify security vulnerabilities within your web application before the cyber criminals do and provide you with valuable remediation advise.

Safeguarding your network infrastructure with ethical hacking can improve business profitability.

Your organisation faces complex challenges every day. Keeping focused on business objectives whenever and wherever you are across the globe requires secure web applications to support you, whether that is on-premise or in the cloud.

Exciting new ways of working and new channels to market mean the company board are delighted, but will security be an enabler to this strategy? How vulnerable is your business today and into the future?

Is it a straightforward process to find weak spots in your business-critical systems, procedures, policies and behaviours of your employees? Or does the news of a new piece of regulation or legislation mean significant work which will cost time and money and potentially introduce new security weaknesses?

So what is required?

It's about ensuring proactive protection of your brand, reputation and valuable electronic assets around the clock worldwide.

Secondly, it's about having a clear view of your overall risk profile from any potential impact, or as loss of customer trust which is very hard to recover.

At an operational level, it's also about understanding the countermeasures and actions that you need to take to properly protect your network infrastructure and associated data, as well as about having full visibility of your own security estate, your service providers and the services they are managing.

All of these combine to better support your organisation's business strategy.

Assessing your web application

The intent of testing is to utilize the skills and techniques of an attacker to identify vulnerabilities and security flaws within the target application. BT has developed a documented, proprietary methodology for conducting vulnerability assessments of web-based applications, which focuses exclusively on manual testing of the application.

Our methodology incorporates a wide array of tests which seek to identify both exploitable vulnerabilities within the target application as well as deviations from a proper defence-in-depth posture. Some of the aspects covered during testing include:

- Testing of authentication and authorization mechanisms, seeking to identify weaknesses which would allow an attacker to circumvent authentication requirements or bypass authorization controls (horizontal or vertical).
- Testing of the application's session management – how session state is maintained between requests to the server.
- Testing of all application components for injection-based vulnerabilities, including checks for Cross-Site Scripting, Remote Code Execution, SQL Injection, Cross-Site Request Forgery, and Cross-Origin Resource Sharing vulnerabilities.
- Testing of all application components for business logic vulnerabilities – areas where an attacker may bypass intended business logic controls, creating issues with data integrity, availability, and/or confidentiality.
- Test the strength and implementation of any encryption used by the application.

Penetration testing

Once we've gone through all steps and have an accurate picture of your web application and its security posture, our hackers can try to exploit the vulnerabilities they've found. Why? To show the business impact of having vulnerabilities in your web application.

Banking on trust

Over the next five years, our ethical hackers will be running assessments for a large bank with European headquarters. We're testing the systems that manage billions of euros every day, on a global and local scale.

It's so they can show their auditors they've carried out the right checks. And so they can show their customers that they're a trustworthy brand. The bank remains compliant and in control of their infrastructure and applications; they've got a lot of both, and they're often classified.

Why us?

We're experienced

In fact, we're one of the biggest security and business continuity practices in the world. We've got 3,600 security professionals working for us across the globe. And when it comes to ethical hacking, our team has more than 30 years' experience.

We operate across many industries, including industries that are significantly more advanced in dealing with cyber threats. This means we are ideally placed to bring expertise and know-how acquired with customers on the leading-edge of cyber security.

We're recommended

We're recognised as a Leader in ISG Provider Lens™ – Cyber Security – Solutions and Services 2024 in the UK. The report highlighted our strengths in managed security services, strategic security services, and technical security services in the UK.

BT has been named a Leader for the 20th consecutive year* in the 2024 in the Gartner Magic Quadrant™ for Global WAN Services based on its "Ability to Execute and Completeness of Vision".

*Magic Quadrant for Global WAN Services was previously named Magic Quadrant for Network Services, Global

We're qualified and security cleared

Our consultants hold industry certifications like CISSP, CISA, OSCE, and OSCP.

Where appropriate, our consultants possess national security clearance for delivery to government customers.

We're accredited for ISO27001:2013 covering our security testing services to both internal and external customers. Next to our ISO27001 accreditation we're also accredited for global consulting by Lloyd's Register Quality Assurance for the ISO9001 quality management system. We've held that since 2003 – proof of our long-term commitment to improving our services.

We have first-hand experience

As a large organisation, operating in around 180 countries, we know all about keeping our intellectual property, customers, people and premises safe.

We work hard to protect our networks, systems and applications – our ethical hackers and red team specialists test everything. Additionally, we work closely together with our blue team to test the effectiveness of our defences by carrying out multi-layered simulated attacks against both our physical and cyber security infrastructure.

This unrivalled experience, gained over many years of full spectrum testing of our policies, processes and defences, keeps our brand safe.

Find out more about ethical hacking

Learn more

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

JN: 1611673531 | November 2024.