Means Business

Datasheet

Our Mobile Basic Review services

Our team of ethical hackers can spot any potential underlying security vulnerabilities in your mobile applications which could lead to more significant security exposure.

Exploring the mobile application

By proactively identifying weak spots in your mobile application and underlying application models, we can help you keep your customer's data secure and the reputation of your business intact. If the issues located in the report go undetected, they could form the foundation for more serious and potentially dangerous security flaws at a later date.

Our basic assessment helps you to identify the issues and allows you to fix them before they become a bigger problem. It may also help you decide whether it would be beneficial to perform a more extensive penetration test assessment of this mobile application or others.

Our Basic Review Approach

We've developed a standard methodology to look at your mobile applications to identify whether there are any significant security threats associated with the application itself or its interaction with your core network.
Our approach is based on a simplified version of our extensive mobile application security testing methodology and draws on our many years of experience in security testing.

So what is it and whats involved?

Our basic review is not meant as a full penetration test, but aims to pick out any obvious security issues within the mobile application which could introduce significant risks to your business.

All testing activities are performed using our own test devices on which we'll install your mobile application directly from either the Apple App Store or Google Play Store. We can perform our basic review on either Android, iOS or even both platforms. We use a 'black-box' approach as we will not have any other information available to us.

If you're worried about any potential issues related to your live environment: rest assured, we will not target your core infrastructure.

Our hackers will take three days to complete the basic review. This involves several different steps and processes.

The tester will identify any potential issues by using these steps and their experience, but because this assessment is performed as a black-box test, they will not have credentials to authenticate or login into the system. The seriousness or validity of some issues therefore cannot be confirmed, but would be fully validated if a full penetration test was subsequently carried out.

After the assessment is completed, we'll assess the findings and present these in a summary report. This high-level report is based on our defined processes and enables us to deliver a high-quality overview of any identified and projected vulnerabilities.

Our Approach

We perform an analysis of the underlying codebase and configuration values. This is done without executing the application. Issues discovered at this stage help to guide the next steps.

We look to:

- identify weak encryption or hardcoded secrets
- find areas where customer or user information could be at risk
- check application and binary data protections
- spot misconfigurations in the development process that may aid a foothold further into the application.

After finding any code issues we try to leverage these and look to see how we can use them to delve deeper into the application's inner workings.

This may include:

- ways to abuse the application functionality or user journey
- insecure storage of application and user data
- investigation of any database or local files
- reverse engineering any encryption mechanisms.

Our testers understand that the application doesn't end at the device level and that there are often complex workings that underpin the internal components.

That's why we don't just stop at what the user sees, we also examine the communications between the client and servers to ensure these other interactions are secure too.

We also review the following:

- identification of possible forms of sensitive data
- details about the transmission of username and password values
- use of weak certificate pinning, or lack of password complexity requirements
- leakage of server responses or status messages which may be a sign of further issues.

As our testers don't have the credentials to enable them to access the platform as a standard user, any issues behind authentication mechanisms, such as user accounts or functions will not be investigated.
Once the basic assessment is complete, and if any vulnerabilities are discovered, we might recommend having a full penetration test carried out.

The outcome of such a test will give you a complete view of the security posture, any associated risks to your business, and ways to remediate any issues.

The next steps: Penetration testing

Our extensive mobile application penetration testing assessment is made up of a series of different tests, each helping to paint a better picture of the strength of your mobile application. Altogether, there are six phases to the penetration testing assessment.

Once we've gone through all phases of the assessment, our hackers can try to exploit the holes they've found. Why? To show the consequences to the business of having weak points in your mobile application or associated central infrastructure.

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

JN: 1611673531 | November 2024.