Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Red Team
Mobile Application Security Testing

Mobile applications are increasing in numbers every day. More than **90%** of government services in UAE can be transacted through mobile applications. Increase in the use of mobile applications means, application vulnerabilities and thus security incidents that may impact the client device or backend systems that support the mobile application.

Many mobile applications we have assessed recently across the region, indicate the need for continuous security assessment of mobile applications. Poorly hardening and securely configured mobile applications by the software developers, often outsourced by organizations, do not even follow the most basic of security guidelines.

Mobile Application vulnerabilities often lead to customer privacy violations and/or data loss. Considering this, it is important to perform a holistic security review as part of your mobile application deployment strategy.

DTS expert team of mobile application security consultants offers a detailed security analysis of your mobile application as part of our **Mobile Application Security Assessment** service. Our testing methods use both automated testing as well as manual testing using a combination of **Mobile Application Security Framework (MobSF), OS simulators and SDK kits**. Our "automated tests" detects many of the common vulnerabilities of your mobile application. However, manual testing by our security experts uncovers much more issues than the automated tests especially during a grey-box test.

Our **Mobile Application Security methodology** is based on the **OWASP Mobile Security** project and performs tests both client application as well as the server-side testing.

Application Mapping

The initial step in the Mobile application security assessment is the mapping of the application for each type of the Operating System architecture. This will provide a detailed understanding of the application and the data flow, within the application as well as to the server.

- Application understanding
- Data Flow mapping

Client-Side Attacks

In this stage, the focus of the testing is to understand the weaknesses on the client side. This includes the analysis of temporary storage, sensitive information and client-side encryption.

- Binary Analysis and Identification of insecure APIs
- File system analysis for identification of sensitive files and weak encryption implementation
- Memory and Process analysis

Network Attacks

In this stage, the communication channel between the client and the server undergoes the review and attack. Sensitive plain text traffic is retrieved by analyzing

- Installation traffic
- Run time traffic

Server-Side Attacks

The final phase of a mobile application security assessment is to assess the security of the server. In this, the server-side application would be tested to find out how it responds to various malicious requests.

- TCP attacks are performed to identify vulnerabilities such as Buffer Overflows
- HTTP Attacks are performed to identify application vulnerabilities such as XSS, SQL injection and other OWASP listed vulnerabilities

Test Types	
M1. Weak Server-Side Control	M6. Broken Cryptography
M2. Insecure Data Storage	M7. Client-Side Injection
M3. Insufficient Transport Layer Protection	M8. Security Decisions Via Untrusted Inputs
M4. Unintended Data Leakage	M9. Improper Session Handling
M5. Poor Authorization and Authentication	M10. Lack of Binary Protections

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com