Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Red Team
Web Application Security Testing

Vulnerable internet-facing web applications are rapidly becoming the most popular attack vector of malicious hackers. Application code vulnerabilities and design flaws in content-rich, web-based, thick-client, and mobile applications can be targeted to penetrate networks and steal sensitive information.

Web applications are now also subject to sophisticated attacks whereby delivery of payload no longer is required to obtain Remote Code Execution, the popularity and rise of file-less malware such as Apache Struts give hackers the ability to obtain root access on systems by simply targeting vulnerable web application by sending crafted HTTP request and responses. To mitigate these threats, web and application security assessments must be built into the development and release lifecycle.

Our **application security assessments** identify weaknesses in your proprietary or third-party applications and propose fixes that will enhance your system's security posture. By combining the use of leading tools with targeted, expert manual analysis of your application, we diagnose threat susceptibility and provide you with repeatable, measurable, transparent, and actionable results.

DTS expert Red Team have extensive experience in testing web applications and more than 90% of the work we do is manual, as much as we like to use commercial and open source tools, a human interaction with the web applications always gives the best results – this is particularly true when it comes to performing grey-box web application tests.

Web Application Assessments

- Assess your application from an adversarial standpoint
- Assessment against all OWASP Top 10 security attack vectors
- Perform different assessment types - black-box, grey-box or white-box
- Evaluate your application for misconfigurations, logic attacks, and input validation issues

Application Program Interfaces (APIs)

- Perform in-depth API mapping and manual analysis
- Ensure consistent boundary checking for API requests
- Evaluate your APIs for misconfigurations, logic attacks, and input validation issues

Mobile Applications (iOS and Android)

- Analyze application data storage routines
- Evaluate the usage of platform protections
- Identify permission boundary checking and analysis

Thick Application Clients and Interfaces

- Analyze network traffic patterns for external communications
- Reverse engineering application to determine if vulnerabilities exist
- Conduct input validation checking and fuzzing activities

Application Program Interfaces (APIs)

- Evaluate code quality and implementation from functional and security perspectives
- Manually verify findings and provide context as necessary
- Develop proof-of-concept code to show impact of vulnerabilities

Web Application Threat Modeling

- Conduct deep threat modeling exercise for your critical web applications
- Identify input and output flows and communication matrix
- Perform an attack surface analysis
- Build the relevant protection mechanisms, controls and use cases for monitoring

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