JDS SECURITY

APPLICATION PENETRATION TESTING

JDS is CREST (International) certified as a penetration testing service provider, offering expert advice and consulting for a range of security requirements. We utilise the latest globally recognised standards, benchmarks and methodologies to ensure our tests and audits are relevant to today's security risks. JDS uses proactive, detailed and industry-best practice threat intelligence to increase your organisation's resilience against cyber threats, on time and on budget.

WEB APPLICATION PENETRATION TESTING

Web applications are widely used throughout organisations to service clients, staff, and other infrastructures, and are therefore prime targets for threat actors.

Threat actors could leverage intercepted or otherwise stolen information for financial gain, business disruption, or other criminal activities.

Web Application Penetration Testing is a process of identifying and, where in scope, exploiting vulnerabilities found in the application.

Utilizing modern techniques, tools, and methodologies to assess the overall security posture of the web application, JDS will simulate a real-world attack, including Authenticated Testing (Grey Box) and Un-authenticated Testing (Black Box).

This includes testing the web application's input validation, authentication, and access controls, as well as other common web vulnerabilities such as SQL injection, cross-site scripting, and file inclusion.

API PENETRATION TESTING

In modern web applications APIs can make up the bulk of the way data is transferred and modified. As such, they are a prime target for threat actors to be able to steal, modify or delete data that is important to business function. Given that APIs are a key component in almost all web and mobile applications, it is critical that API penetration testing be considered in your security testing strategy.

The purpose of an API penetration test is to identify and demonstrate real-world attack scenarios that could be used to compromise the security of the application's API calls.

The comprehensive JDS approach involves testing for API vulnerabilities such as injection, input validation, authentication, session management, and access controls. Where possible, the configuration of the application and its API will be evaluated.

Once the findings are delivered, remediation can be prioritised to improve any discovered API compliance vulnerabilities and security gaps.

SECURE SOURCE CODE REVIEW

When carrying out a Secure Code Review, JDS perform a systematic and thorough examination of application source code for the purpose of identifying security vulnerabilities. We then determine how these vulnerabilities may interact with other aspects of the application and its connected infrastructures, such as communications with servers, devices, databases, or even other applications. A Secure Source Code Review can be executed on any of your applications, including Mobile, Web, and Thick applications.

MOBILE APPLICATION PENETRATION TESTING

Mobile applications are now seen as business-critical channels by many organisations, as they offer convenient ways to engage customers, manage staff and interact with businesses. However, specialised assessments are required to validate the security controls of mobile applications. Regular mobile application penetration tests not only look at the source configuration and API calls, but also tests the application's network communication, data storage, and interactions with the device's operating system, intended or otherwise. The goal of the test is to identify and demonstrate real-world attack scenarios that could be used to compromise the security of the user data, your organisation's data, or the device the application runs on.

By identifying security weaknesses, organisations can mitigate potential vulnerabilities and avoid costly data breaches.

THICK APPLICATION PENETRATION TESTING

A Thick Client, also known as a Fat Client, is an application that, independent of the server to provide data, has most of its major processing and functionality done on the client side. While Thick Client Applications are useful and provide a great user experience, exploitable vulnerabilities exist on both the local and server side, which results in the attack surface being larger and requiring a different, more complex approach than web application penetration testing.

The JDS approach to testing both Two-Tier and Three-Tier Thick Client Applications is to identify and demonstrate real-world attack scenarios that could be used to compromise the security of the device hosting the Thick Client Application. This includes the security of the data and functionality of the application itself, and the security of the application server and/or database.

Established in 2003, JDS Australia delivers specialist services in a set of technologies and capabilities that ensure critical IT systems work.

JDS focuses on IT Monitoring (Observability), Security, Service Management, Quality Assurance and Automation as areas that enterprises and government departments need to increase the value of their investments. With an entirely local team of 100+ employees, JDS has the trusted skills and experience to ensure IT works and Australian business carries on.

Melbourne
Level 8, 2 Russell Street
Melbourne VIC 3000

Sydney
Level 10, 50 Park Street
Sydney NSW 2000

Brisbane
Level 37, 123 Eagle Street
Brisbane QLD 4000

Toll Free
1300 780 432

Email
contactus@jds.net.au

Web
www.jds.net.au