VinCSS
Trusted Cybersecurity Pioneer

PENETRATION TESTING

DESCRIBE

VinCSS offers Penetration Testing services for application systems. Penetration Testing allows enterprises to assess the exploitability and penetration potential of their application systems. It identifies whether the application systems have vulnerabilities or chains of vulnerabilities that could be exploited in reality. Unlike Cyber Security Assessment services, Penetration Testing focuses on leveraging the real-world experience of experts in manually searching and experimenting with exploiting identified issues, with only partial support from automated tools, to accurately determine the risk of each security issue. The service also includes in-depth consulting to help enterprises remediate detected issues.

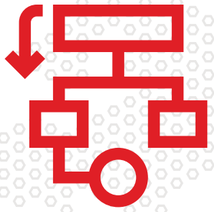
VinCSS has particularly extensive experience in Penetration Testing for IoT/SCA-DA systems.

Trusted Cybersecurity Pioneer

FUNCTION

BLACK BOX PENETRATION TESTING

VinCSS's experts will conduct a penetration testing for the designated system or application from the outside, without being provided any internal information about the system.



GRAY BOX PENETRATION TESTING

VinCSS's experts will perform a penetration testing for the designated system or application after being provided with some internal technical information, such as architectural descriptions, operation flows, API specification documents, etc.

WHITE BOX PENETRATION TESTING

VinCSS's experts will study the application's source code along with all other information about the application system, combined with experimental work on the system, to identify vulnerabilities.

VinCSS
Trusted Cybersecurity Pioneer

PROCEDURE

SCOPE DEFINITION

VinCSS will conduct a survey to identify the target system or application for testing, as well as the scale and duration of the project.

INFORMATION HANDOVER

In cases of Graybox or Whitebox testing, VinCSS works with the client to receive the necessary information before assessment. For example, staging information, technical documentation.

SCOPE DEFINITION

VinCSS performs the testing according to the agreed timeline.

REPORTING

VinCSS reports the testing results, presenting evidence of vulnerability exploitation. VinCSS also provides scripts to help preproduce the issue if needed.

VERIFICATION OF REMEDIATION STATUS

VinCSS collaborates with the client in advising on remediation and verifying the status of remediation for reported security weaknesses until they are resolved. A confirmation report is provided post-remediation.

Trusted Cybersecurity Pioneer

RESULT

The Penetration Testing report will list all existing security issues for the application system, including potential ones. For each identified security issue, VinCSS will classify and rate the impact level of the issue based on both technical criteria and business impact.

Security issues will also come with a description of exploitation test results, describing the capability and level of impact when successfully exploited, along with proposed remediation plans.

Trusted Cybersecurity Pioneer

BENEFIT

DETECTING AND ADDRESSING SECURITY ISSUES EXISTING IN APPLICATION SYSTEMS

Enterprises can implement regular Penetration Testing or before releasing a new version of an application or launching a new system. This allows for early detection and remediation of security issues before bad actors can discover and exploit them.

EVALUATING THE LASSIFICATION AND RATING OF SECURITY ISSUES

In addition to identifying security issues, based on Penetration Testing reports, enterprises can gain a proper understanding of the level of impact and real-world exploitability of these issues, seeing how they may be leveraged in practice.

Trusted Cybersecurity Pioneer

ADVANTAGE

MAXIMUM SUPPORT DURING THE POST-REPORT REMEDIATION PROCESS

VinCSS closely follows and collaborates with the client throughout the security issue remediation process, offering guidance and assistance to verify the status of remediation until all reported issues have been addressed.

EXPERIENCED TEAM

Red Team engagemVinCSS boasts a team of highly experienced experts who have earned numerous reputable security certifications in the industry, such as SANS and Offensive Security certifications. They have practical experience in various security testing projects, including specialized systems like IoT/SCADA, Automotive (Off-vehicle), devices, and mobile operating systems.ents actively detect and mitigate security issues, particularly latent security problems that could form part of an exploitation chain in reality or newly emerging issues during continuous organizational operations.

COMPREHENSIVE TESTING METHODOLOGY

VinCSS adheres to industry-leading standards and checklists for conducting detailed manual testing. As a result, the testing process minimizes the chances of overlooking any security issues.

VinCSS
Trusted Cybersecurity Pioneer

THANK YOU!

VINCSS INTERNET SECURITY SERVICES JSC

• Floor 20A, Vincom Center Dong Khoi Building, No 45A Ly Tu Trong Street, Ben Nghe Ward, Dist. 1, HCMC, Vietnam.

• Email: sales@vincss.net • Website: www.vincss.net