Report

External **Penetration Test** 2020 **Thinkwise Platform**

think wise. | Low-Code for core systems

www.thinkwisesoftware.com

nSEC/Resilience

IT Security | IT Performance

External Penetration Test 2020

Thinkwise Platform

Statement of outcomes

Version 1.1, September 10th 2020 (updated version based on customer feedback)

Context and contents

Thinkwise B.V. (from hereon: Thinkwise) is creator and owner of the Thinkwise Low Code software platform. To be able to prove to customers that the Thinkwise Low Code platform is secure, Thinkwise has mandated nSEC/Resilience to perform a penetration test on the platform.

The penetration test was performed in the start of 2020. This document describes the scope, approach and outcomes of the penetration test in a condensed form. A more detailed description of the tests that were performed and technical details of any findings can be found in the separate penetration test report.

The penetration test was augmented with a number of audit activities, in which security controls, secure configuration and secure development were discussed in interview form. The following topics were covered in this audit:

- Secure design and architecture (both network and application level)
- Secure software development (SAST, DAST, threat modeling etc.)
- IT Security Controls: authorization , authentication, password management
- IT Security Controls: secure communication and encryption; data protection at rest
- IT Security Controls: access control / default deny

The audit did not result in any serious concerns in relation to the Thinkwise platform software. The full outcomes of these audits are available in a separate document.

Description of test scope

Because the attack surface of applications built using the Thinkwise low code platform is defined by the components available at runtime, the penetration test was performed using an example application (the “Insights” application).

The attack surface (areas of the information system that an attacker or security evaluator can choose to initiate an attack) for the penetration test was defined as, and limited to:

- The Thinkwise Insights application as hosted on https://nsec.thinkwise.app/universal/
- The OpenID implementation on the Thinkwise Insights application (https://nsec.thinkwise.app/indicium/connect/token)

In addition to the attack surface defined above, the testers also received VPN access to the server hosting the frontend and indicium components.

The “web” version of the Thinkwise user interface is due to be phased out on short to middle term and was therefore not included in the scope of the test.

It was explicitly allowed as part of the penetration test to investigate and exploit vulnerabilities in the web application as long as direct attack surface was limited to the definition above.

During the penetration test forensic research, code reviews and exhaustive DDOS testing were out of scope.

Due to the nature of the test (using an example application) findings on the example application related to infrastructure or configuration of web servers only applied to the example application and would probably not be a finding in an environment where the client would host the application.

Also, some findings did not require changes to the actual platform software but could be fixed in a specific configuration of the example application. These considerations have been taken into account where possible when assessing potential impact and the severity for any findings done.

Test approach, methodology and process

For the test, the testers received three test accounts for the Insights application, each with different access rights, so that proper tests for access control could take place. As such, the penetration test was executed grey-box. The test was originally planned to be performed in 32 hours of effective testing, spread over a period of 5 working days.

The testers also received credentials for testing OpenID (client ID and client secret) and credentials for connecting through VPN.

Reconnaissance for the penetration test was performed with industry-standard tooling (scanners and scripts) and by manually searching through public available sources. At network level also open ports and active services were investigated.

During the execution- and exploitation phase various tools were used. However, majority of the checks were performed manually, where internet traffic was investigated and manipulated with proxy tooling.

The OWASP top 10 was the base for the performed interactive checks on application level. The test was executed in line with ASVS level 2 guidelines, using two testers with at least two relevant security testing certifications.

The OWASP ASVS (Application Security Verification Standard) provides an independent basis for determining standards for security testing and secure development. ASVS level 2 is for applications that contain sensitive data which requires protection and is the recommended level for most applications (ASVS level 3 is for the most critical applications such as high value transactions, military etc). However many of the checks in the area of secure coding etc. were also covered in the audit activities, resulting in partial coverage of ASVS level 3 requirements as well.

The tools used in the initial phase of the penetration test included Nessus, nmap, Burp suite Pro, NetSparker, OWASP ZAP and DIRB.

Each potential vulnerability category was tested for manually as well. The full penetration test report contains a description per vulnerability category of the tests executed for that category, together with a rationale of why the application was or was not vulnerable. Where required, specialized tools such as SQLMap were used.

For each specific technology that was identified, the proper corresponding tests were performed. An example is the OData standard that was used in the Indicium layer; for this technology specific manual checks were performed on secure configuration of OData interface layers.

After the initial penetration test a number of findings have been addressed, after which a retest was performed. The conclusions in this document are based on the situation after the retest.

Description of outcomes

During the penetration test on the Insights application the testers have not succeeded in breaching data or taking control of the server; this is already a good result. Also, most findings were related to webserver configuration, and therefore are specific to the Insights application and not applicable to the Thinkwise platform in general.

After the initial penetration test was performed, findings were addressed by Thinkwise and were then retested by nSEC/Resilience. After this retest (and at the time of writing this document) no findings remained open.

Even taking into account that all penetration tests describe the security of the system under test at a specific moment in time, and that security testing should always be seen as a continuous process, the testers do not see any vulnerabilities in the application (platform) at this point, which is a very positive result.

Presented per category (based on OWASP categories):

Topic/area	Test result
Network level	Good – no vulnerabilities detected
Broken Access Control	Good – no vulnerabilities detected
Unrestricted File Upload	Good – no vulnerabilities detected
Directory traversal / File inclusion	Good – no vulnerabilities detected
Cross-site scripting (XSS)	Good – no vulnerabilities detected
SSL/TLS	Good – no vulnerabilities detected
SQL injection	Good – no vulnerabilities detected
Error handling	Good – no vulnerabilities detected
Sensitive data exposure	Good – no vulnerabilities detected
Security (mis)configuration	Good – no vulnerabilities detected
Authentication and sessionmgnt	Good – no vulnerabilities detected