securing

www.securing.biz

PENETRATION TESTS OF
NETWORK INFRASTRUCTURE
FOR SURFSHARK

REPORT

document version: 1.1

document ID: Classified information

author: Adam Hołod (SecuRing)

test time period: 2025-12-01 – 2025-12-10

report date: 2025-12-12

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

1.1. Testing overview

The security tests of Network Infrastructure were meant to verify whether the proper security mechanisms were in place to prevent unauthorized users from accessing the client's data and infrastructure and to detect the vulnerabilities which could cause financial losses to the client or their customers.

Security tests were performed using the following methods:

- Penetration testing – simulated attacks on Network Infrastructure from the perspective of an anonymous and standard VPN user.

1.2. Summary of test results

- During the penetration testing, no vulnerabilities with critical risk impact were found.
- The identified vulnerabilities do not result in the manifestation of key threats.
- Moreover, 1 vulnerability with medium risk impact was found:
  - Possibility of intercepting communication between the client and the server due to improper SSL/TLS configuration (F1).
- Additionally, 1 recommendation has been proposed that does not have any direct risk impact. However, it is suggested to implement it due to good security practices.

2. SUMMARY OF IDENTIFIED VULNERABILITIES

2.1. Terminology

This section explains the terms that are related to the methodology used in this report.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[1]

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.[1]

Risk

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.[1]

[1] NIST FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

2.2. Risk classification

The risk impact in this report is estimated based on the complexity of exploitation conditions (representing the likelihood) and the severity of exploitation results.

		Complexity of exploitation conditions		
		Simple	Moderate	Complex
Severity of exploitation results	Major	Critical	High	Medium
	Moderate	High	Medium	Low
	Minor	Medium	Low	Low

The findings in this report have been categorized as vulnerabilities (findings with risk impact) and recommendations – methods of increasing the security of the system by implementing good security practices or eliminating weaknesses, for which no direct risk impact has been identified.

2.3. Risk handling recommendations

Vulnerabilities	
Risk impact	**Description**
Critical	It is recommended to take immediate mitigating actions or limit the possibility of vulnerability exploitation.
High	It is recommended to take mitigating actions as soon as possible.
Medium	The mitigating actions should be taken after eliminating the vulnerabilities with critical and high risk impact.
Low	The mitigating actions should be taken after eliminating the vulnerabilities with critical, high, and medium risk impact.
Recommendations	
The decision whether to take mitigating actions should be made by the client.	

2.4. Identified vulnerabilities

Vulnerability	Risk impact
SCRNG-3533-F1 Improper SSL/TLS configuration	**Medium**
Recommendations	
SCRNG-3533-R1 Restrict redirects to hosts from the specific domain	

3. PROJECT DESCRIPTION

3.1. Basic information

Testing team	Adam Hołod Jakub Korepta
Testing time period	2025-12-01 – 2025-12-10
Report date	2026-01-02
Document ID	Classified information
Document version	1.1

The report was prepared in accordance with SecuRing's internal standards for security testing.

About SecuRing

SecuRing is a cybersecurity company founded in 2003 in Kraków, Poland. Our mission is to help improve the security of IT solutions that power today's digital world.

We have delivered over 10,000 security testing projects in more than 20 countries, working with leading banks, fintechs, insurance companies, healthcare and telecom organizations, government & public institutions, as well as B2B, SaaS providers and software houses.

Our services and trainings cover a wide range of security areas — from web and mobile application security testing, through infrastructure and cloud security, to red teaming and AI security.

We also maintain a free Knowledge Base, where we openly share our expertise, research, and practical security insights to support the wider security community.

In 2025, SecuRing was recognized as CYSSDE Grand Winner, and since 2023, we have been listed as a Top Cybersecurity Company on Clutch.

3.2. Target in scope

The object being analyzed was public facing Network Infrastructure accessible from the URL address listed below:

```
Redacted for public version of the report.
```

In addition, the infrastructure available behind the VPN was analyzed, and the scope is

listed below:

```
Redacted for public version of the report.
```

The tests were performed via VPN provided by the client.

3.3. Threat analysis

The key threats were identified as follows:

- Unauthorized access to confidential data, including personal or financial information,
- Lateral movement within the internal network leading to privilege escalation or compromise of additional assets.

3.4. Methodology

The testing team applied the methodology of grey-box penetration tests. A penetration test is a controlled attempt to break through security controls applied in a particular system. In a grey-box test, the testing team has access to the same set of information as a typical user of the tested system as well as local technical staff support.

The tests were aimed at identification of vulnerabilities occurring in the application and defining possible attack scenarios conducted with techniques typical for attacks on web applications.

The report utilizes OWASP Application Security Verification Standard (ASVS) 4.0 and Common Vulnerability Scoring System (CVSS) 3.1.

3.5. Scope

Following the specification, the tests covered:

- A full range of security tests on external resources without any initial privileges,
- Security assessment on internal resources conducted via VPN.

4. LIST OF PERFORMED TESTS

4.1. Server environment testing

1. OSINT – exploring sources of publicly available information related to tested application, implemented technologies, server paths, subdomains, and cloud identifiers:
   - DNS Zones,
   - Certificate Transparency logs,
   - Hosting services (i.e., GitHub, Pastebin).
2. Scanning most popular TCP/UDP ports:
   - Establishing visibility of services on the Internet,
   - Measuring response of the system to scanning attempts,
   - Probing all ports.
3. Reconnaissance of network environment:
   - Determining IP addresses of services,
   - Establishing route to services,
   - Resolving reverse DNS names,
   - Determining size and the owner of subnetwork in ARIN WHOIS database,
   - Passive identification of potentially related services which were not the subject of scope.
4. Fingerprinting of systems and services:
   - Collecting headers and responses of active services,
   - Attempting to identify implemented technologies,
   - Attempting to determine presence of WAF filters, CDN networks and other reverse proxy servers,
   - Measuring system's reaction by providing unexpected inputs.
5. Vulnerability scanning:
   - With public scripts for Nmap NSE.
6. Configuration assessment of popular services (i.e., HTTP, FTP etc.):
   - Determining available methods,
   - Attempts to log in with default/popular/leaked passwords,
   - Attempts to list publicly available directories.
7. SSL configuration assessment:
   - Determining offered protocols and cipher suites,
   - Verification of prevention methods to known attacks and problems,

- Examining configuration attributes and chain of trust of certificates,
- Attempting to connect to the system without encryption, to establish the presence of headers enforcing the use of encryption protocols and system' response.

8. Exploration of hidden resources:
   - Brute-force attacks on files and directories,
   - Accessing links to cloud resources, establishing their public permissions.

5. VULNERABILITIES

F1. Improper SSL/TLS configuration

Risk impact	Medium	CVSS	5.3	ASVS	V9
Exploitation conditions	Access to the network traffic exchanged between the client and the server.				
Exploitation results	Possibility of intercepting communication between the client and the server.				
References	CWE-326: Inadequate Encryption Strength https://cwe.mitre.org/data/definitions/326.html CWE-327: Use of a Broken or Risky Cryptographic Algorithm https://cwe.mitre.org/data/definitions/327.html CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') https://cwe.mitre.org/data/definitions/757.html OWASP Transport Layer Protection Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html OWASP Top 10 A02:2021 Cryptographic Failures https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ Mozilla SSL Configuration Generator https://ssl-config.mozilla.org/				
Remediation	Disable cryptographically weak cipher suites. Disable insecure SSL/TLS protocol versions (SSLv2, SSLv3, TLSv1.0, TLSv1.1).				

Vulnerability description:

A number of weaknesses in SSL/TLS configuration were identified, which in the presence of favorable conditions can lead to the interception of communication between the client and the server or to performing a Denial of Service attack.

Test case:

The identified issues have been included in the excel file attached to the report.

6. RECOMMENDATIONS

R1. Restrict redirects to hosts from the specific domain

Description:

The server uses URI parameter in the redirection mechanism. The attacker provides arbitrary address as a value, and because this parameter is not properly validated, it is possible to redirect user to any domain (simplifying further phishing attacks) or even access resources without authorization.

Attacker modifies URI path in a malicious way as shown below:

```
GET /q4vfj0cz181bwdlk9fy12soia9g04usj.[REDACTED]%2F%2F HTTP/1.1
Host: [REDACTED]
[…]
```

As a result, the server responds with a redirect to the attacker's website:

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.22.1
Date: Thu, 11 Dec 2025 15:08:55 GMT
Content-Length: 0
Connection: keep-alive
Location: https:///q4vfj0cz181bwdlk9fy12soia9g04usj.[REDACTED]
```

How to implement:

If redirects are necessary, restrict URL to specific domains, or even local files that are used by the application.

References:

OWASP Unvalidated Redirects and Forwards Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

7. CONTACT

Person responsible for providing explanations:

Adam Hołod
e-mail: adam.holod@securing.pl
tel.: +48 12 425 25 75
mob.: [REDACTED]

securing
https://www.securing.pl
e-mail: info@securing.pl
Kalwaryjska 65/6
30-504 Kraków
tel./fax.: +48 (12) 425 25 75