

Vulnerability Assessment Report

28/6/2025

Contents

1. Executive Summary	2
2. Introduction	2
3. Methodology.....	2
4. Detailed Findings.....	3
5. Risk Assessment.....	9
6. Recommendations	10
7. Timeline	10



1. Executive Summary

- The purpose of this vulnerability scanning is to discover the existing vulnerabilities on the servers operating the company's services.
- The Nessus program was used to conduct the scan.
- The implementation was carried out on 28/06/2025.
- After the scan process, several vulnerabilities were discovered as follows:
 - **11** classified as Info severity
 - **2** vulnerabilities classified as low severity.
 - **0** vulnerability classified as medium, high, and critical severities.
- A meeting of the cybersecurity committee was held to discuss the vulnerabilities, verify them, and adopt the appropriate treatment methods if needed to be applied within the time frame specified in the policies and procedures.
- Several external sources have been adopted to assess vulnerabilities, such as NIST, and CVSS.

2. Introduction

The goal of vulnerability scanning is to identify weaknesses on the main servers that operate Taqnyat's services.

The scope of scanning all servers hosting any services or databases that run the services provided to Taqnyat's clients.

3. Methodology

In this scan, the Nessus application was used to scan all open ports, collect information, correlate it with vulnerabilities and generate a report.

The report issued by applying Nessus is discussed within the cybersecurity committee and in the presence of the internal auditor to discuss the risks associated with the report, reclassify the vulnerabilities based on the server's importance degree and the services it provides, in addition to evaluating the vulnerabilities through external sources and excluding false-positive vulnerabilities.

