



# TECHDEFENCELABS

Your Trusted **Cyber Security** Partner

**A CERT-In Empanelled Information Security Organisation**

**No:- 3(15)/2004-CERT-In**



## Document Authorization, Revision History, and Control

Document Preparation	
Document Title	External Infrastructure Vulnerability Assessment and Penetration Testing Report
Evaluated Organization	LKP Securities Limited
Document ID	TDL-LSL-NB-04/26/0040
Report Version	v1.0
Assessment Approach	Black Box Infrastructure VAPT Audit Report
Type of Audit Report	First Audit Report
Primary Assessment Period	23-Jan-2026
Re-Assessment Period	Follow Up Audit Not Performed
Report Prepared by	Kunal Patil
Reviewed by	Heet Kakadiya
Approved by	Rohit Soni
Released by	Pavan Saxena
Date of Release	15-Apr-2026

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	15-Apr-2026	First Audit Report

Document Distribution List			
Name	Organization	Designation	Email Id
Dhruv Chauhan	TechDefence Labs	Manager – Enterprise Business	dhruv.chauhan@techdefence.com
Umair Patel	LKP Securities Limited	Assistant manager information security	Umair.patel@lkpsec.com

## Confidentiality and Disclaimer

---

This report is prepared exclusively for the management of the Evaluated organization and is intended solely for internal use. TechD Cybersecurity Limited disclaims any liability to third parties for the unauthorized use or distribution of this document or its contents. The findings, information, data, advice, and recommendations are based on the cooperation of the Evaluated organization and the data provided during the assessment period. Any limitations due to environmental constraints, access restrictions, or insufficient information may have impacted the thoroughness of our analysis and could result in unidentified vulnerabilities.

The report assesses the initial security controls implemented by the Evaluated organization, specifically focusing on the security of the defined domain and systems in-scope. TechD Cybersecurity Limited highlights areas for potential improvement; however, the responsibility for implementing and maintaining robust security measures lies with the management of the Evaluated organization. The information provided in this document reflects the state of the security environment at the time of preparation and is not an exhaustive evaluation.

**Note:** *For the purpose of this report, the term “Evaluated organization” refers to the client organization for which this assessment was conducted.*

©TechD Cybersecurity Limited, 2026  
9th Floor, Abhishree Adroit,  
Near Mansi Circle, Vastrapur,  
Ahmedabad-380015.

## Table of Contents

Document Authorization, Revision History, and Control .....	2
Document Preparation .....	2
Document Change History .....	2
Document Distribution List .....	2
Confidentiality and Disclaimer .....	3
1. Assessment Details .....	5
1.1 Engagement Scope .....	5
1.2 Scope Exclusions .....	6
1.3 Project Team .....	6
1.4 Tools used during the assessment .....	7
2. VAPT Audit Methodology and Standards .....	8
2.1 Phases of the Assessment .....	8
2.2 Standards and Methodologies .....	8
2.3 Vulnerability Risk Rating Metrics and Remediation SLA .....	9
3. Executive Summary .....	10
3.1 Visual Representation of Assessment Results .....	10
4. Detailed Vulnerability Observations .....	11
Annexure A - Engagement Limitations .....	12
Annexure B - Retesting Statement .....	12
Annexure C - Disclaimer and Precautions for Patch Implementation .....	13
Annexure D - CERT-In Reporting and Remediation Compliance .....	13

## 1. Assessment Details

The evaluated organization engaged TechD Cybersecurity Limited to assess the security of its infrastructure. The evaluation focused on identifying infrastructure-level vulnerabilities, testing security mechanisms, and resilience against unauthorized access. The assessment followed industry standards, including NIST 800-115 and Penetration Testing Execution Standard (PTES).

### 1.1 Engagement Scope

The following Infrastructure IPs provided by the Evaluated organization were identified as in scope for this security assessment, as defined during the engagement.

In Scope of Assessment			
Type of Infrastructure	IP Address	No. of Devices	Internal/External
Server	51.162.178.225, 51.162.178.229, 51.162.178.242, 51.162.178.230, 51.162.178.232, 51.162.178.249, 51.162.178.226, 51.162.178.235, 51.162.178.250, 51.162.178.254	10	External



## 1.2 Scope Exclusions

1. Security assessment or Vulnerability Assessment and Penetration Testing (VAPT) of applications hosted on systems within the scoped IP range is outside the scope of this network VAPT engagement unless explicitly specified.
2. Detailed configuration reviews or hardening assessments of network devices (e.g., firewalls, routers, switches) are excluded unless specifically included within the scope.
3. For production environments, any test cases or activities that may cause service disruption, instability, or downtime will be avoided during the assessment.
4. Exploitation of identified vulnerabilities will be limited to proof-of-concept (PoC) validation only. Full exploitation or actions that may impact system availability or integrity will not be performed.
5. Any IP addresses, network segments, systems, or management interfaces not explicitly provided or approved by the Evaluated organization will be considered out of scope.

## 1.3 Project Team

Below are the TechD Cybersecurity Limited Auditing team members who played a key role in this engagement:

Name	Designation	Email-ID	Qualifications/ Certifications	Listed in CERT-In Snapshot? (Yes/No)
Pavan Saxena	Team Lead - VAPT	pavan@techdefence.com	BCA, OSWP, OSCP (ISC)2 - CC, AZ-900, CEHv12, eJPT-v2, CAP, CNSP, CAPen, KLCP, ISO-27001: Lead Auditor	Yes
Rushikesh Patil	Sr. Security Analyst	Rushikesh.patil@techdefence.com	CEH Master, ISO27001	No
Kunal Patil	Security Analyst	kunal.p@techdefence.com	Bsc, CAP, CNSP	No

## 1.4 Tools used during the assessment

Sr. No	Name of Tool /Software used	Version of the tool /Software used	Open Source /Licensed
01	Nessus Professional	v10.11.0	Licensed
02	Nmap	v7.98	Open Source

## 2. VAPT Audit Methodology and Standards

---

### 2.1 Phases of the Assessment

- **Pre-engagement Phase:** This is the stage where the logistics and the rules of engagement of the test are discussed.
- **Reconnaissance/ Discovery Phase:** To simulate a cyber-attack on a infrastructure, the penetration tester needs access to information about the target. They gather this information in the reconnaissance stage.
- **Vulnerability Analysis:** This phase consists of testing the infrastructure for known vulnerabilities. Using an automated and manual approach for uncovering new and hidden vulnerabilities on the infrastructure.
- **Exploitation and Post Exploitation:** The goal here is establishing access to a system using the loopholes uncovered in the earlier phases of Pen testing. The penetration tester tries to identify an entry point and then look for assets that can be accessed through that.
- **Reporting and Recommendations:** All the previous penetration testing phases contribute to this phase where a VAPT report is created and shared with the client.
- **Remediation and Rescan:** Once the vulnerabilities are fixed, we would carry out the round of rescans to identify any security loopholes that might have been left unattended.

### 2.2 Standards and Methodologies

- **National Institute of Standards and Technology - NIST 800-115:** NIST 800-115 provides guidelines for conducting structured information security testing and assessments, focusing on vulnerability scanning, penetration testing, and overall security evaluations. The methodology involves assessing the organization's network infrastructure, identifying vulnerabilities, and generating detailed reports with actionable recommendations. Emphasizing continuous improvement, it ensures a systematic approach to strengthening network security through effective testing and mitigation strategies.
- **Penetration Testing Execution Standard (PTES):** The Penetration Testing Execution Standard (PTES) provides a structured methodology for conducting comprehensive penetration testing. It includes seven essential phases—planning, information gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation, and reporting—ensuring thorough coverage of vulnerabilities and helping organizations enhance their security posture through systematic testing and analysis.



## 2.3 Vulnerability Risk Rating Metrics and Remediation SLA

This section outlines the methodology used to assess and classify vulnerabilities based on the Common Vulnerability Scoring System (CVSS), along with the corresponding risk ratings. In addition, it defines the recommended remediation timelines for identified vulnerabilities based on their severity and potential business impact.

The Recommended Remediation Timelines provided in this report are suggested by TechD Cybersecurity Limited, based on industry best practices, risk exposure, and experience from similar engagements. These timelines are intended to assist the Evaluated organization in prioritizing remediation efforts effectively and reducing overall security risk.

Risk Exposure	CVSS Score	Remediation Timeline	Description
Critical	9.0 – 10.0	Within 7 Days	Immediate risk of severe impact on confidentiality, integrity, or availability.
High	7.0 – 8.9	Within 15 Days	High risk of system or data compromise requiring urgent remediation.
Medium	4.0 – 6.9	Within 30 Days	Moderate risk with potential for exploitation under certain conditions.
Low	0.1 – 3.9	Within 60 Days	Low risk with limited impact and specific exploitation requirements.
Informational	0	As per Business Priority	No direct risk; improvement recommendations for security posture.

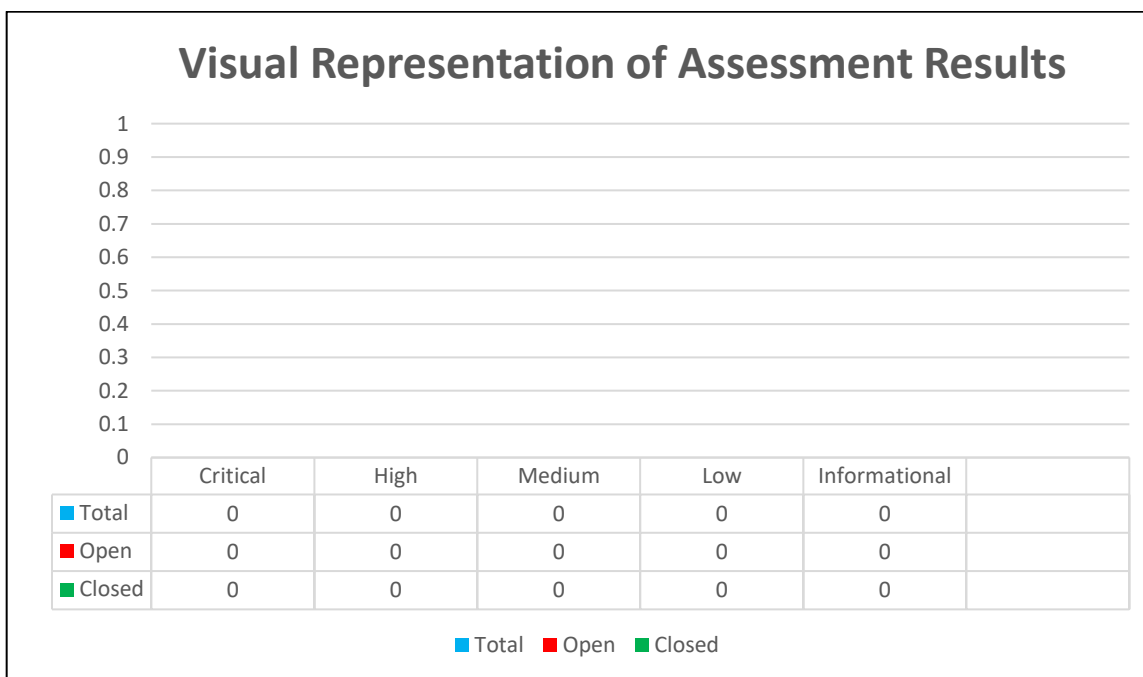
**Risk Factors:** Risk is assessed based on two primary factors: Likelihood and Impact.

- **Likelihood:** This factor measures the probability of a vulnerability being exploited. Ratings are determined by the attack difficulty, the availability of tools, the skill level of potential attackers, and the environment.
- **Impact:** This factor evaluates the potential consequences of a vulnerability on operations, including its effect on confidentiality, integrity, and availability of systems/data, as well as any reputational or financial damage.

### 3. Executive Summary

The following section provides an Executive Summary of the vulnerabilities identified during this Security Audit. Detailed recommendations for each observation are outlined in Section 4 of this report.

#### 3.1 Visual Representation of Assessment Results



## 4. Detailed Vulnerability Observations

---

We have performed a detailed VAPT scan on the above-mentioned IP using Nessus Professional and the Black Box scanning methodology. Our analysis observed no major impactful vulnerabilities on the specified IP. Additionally, to ensure security, we conducted a manual security check on the IP and found no significant vulnerabilities. However, it is recommended to periodically perform assessment and keep the configurations up-to-date.

## **Annexure A - Engagement Limitations**

---

The security assessment was conducted within the scope and timeline agreed upon during the engagement with the Evaluated organization. Due to time limitations and operational constraints, it may not have been possible to identify every potential vulnerability present within the environment.

Testing activities were limited to the systems, endpoints, and functionalities that were made accessible by the Evaluated organization during the defined assessment period. The findings presented in this report represent the security posture of the evaluated systems at the time of testing and should not be interpreted as a guarantee that no additional vulnerabilities exist.

## **Annexure B - Retesting Statement**

---

Upon completion of remediation activities by the Evaluated organization, a re-assessment may be conducted to verify whether the identified vulnerabilities have been successfully mitigated. The purpose of the re-assessment is limited to validating the remediation of the specific findings documented in this report.

The Evaluated organization is expected to address the identified vulnerabilities within a period of ninety (90) days from the date of report issuance, in accordance with the agreed remediation service level timelines. Re-assessment requests submitted within this period will be accommodated as part of the engagement to verify the implemented fixes.

Requests for re-assessment submitted after the ninety (90) day remediation window may be subject to a separate engagement or additional scope, as the validity and relevance of the original findings may change over time due to updates in the application environment.

## Annexure C - Disclaimer and Precautions for Patch Implementation

---

Before implementing any remediation, actions based on this report, the following precautions should be observed:

- **Backup & Recovery:** Ensure complete backups of systems, applications, and data are taken prior to changes, along with a defined rollback plan to restore services in case of failure.
- **Controlled Testing:** Validate all fixes in a UAT or staging environment before deploying to production to avoid service disruption.
- **Third-Party References:** External links provided for remediation guidance are for reference only; their accuracy and availability are not guaranteed.
- **Assessment Limitations:** Findings are based on testing performed within the defined scope, timeline, and accessible environment. Certain vulnerabilities, especially those requiring intrusive testing, may not have been identified.
- **Point-in-Time Evaluation:** This report reflects the security posture at the time of assessment. New vulnerabilities may emerge due to system changes or evolving threats.
- **Ongoing Security Responsibility:** Security is a continuous process. The responsibility for implementing fixes and maintaining security controls rests with the Evaluated organization.

## Annexure D - CERT-In Reporting and Remediation Compliance

---

As a CERT-IN empanelled organization, we have received communication stating that all CERT-IN empanelled organizations are required to submit audit-related data (including Cyber Audits, IS Audits, Regulatory audits, and VAPT audits) to CERT-IN starting from the fiscal year 2024. We will be sharing this VAPT Audit Reports or related details with CERT-IN. According to CERT-IN regulations, a period of 90 days is provided for the remediation/patching process from the release date of the audit reports. Therefore, we kindly request you to address all mentioned vulnerabilities within the 90-day timeframe and to inform us for the follow-up audit.