Internal Network Pentest Findings Report

Date

1/26/202

Document Details

PENTEST REPORT

Access to *https://front.stage.platform.lndx.ai/*
and all related data, content, systems, and materials are strictly confidential and intended only for authorized users. Any information accessed through this platform must not be disclosed, shared, copied, or used for any purpose other than approved project activities without prior written consent. Unauthorized use or disclosure may result in legal action.

Document Type	FInding Report
Client	Example Corp
Document Version	Version 1.0
Creation Date	1/25/2026
Delivery Date	1/26/2026

Version History

Version	Date	NOTES	Author
0.1 Draft	26/01/2026	Draft Report	Sumon Das
0.1 Draft	26/01/2026	Import Pentest Report	Sumon Das
Final	26/01/2026	Delivered Final Report	Sumon Das

Contact Information

Name	Title	Email Address
Sumon		
Sumon Das	Lead Penetration Tester	sumonraj1613@gmail.com
Client		
Sajol Biswas	Client Title Here	email@examplecorp.tld

Document Details

Pentest Report

Overview

On January 26, 2026, an external penetration test was conducted on the web application hosted at *https://front.stage.platform.lndx.ai/* to evaluate its security posture against current industry best practices. The assessment focused on discovering vulnerabilities and weaknesses within the publicly accessible application. All testing activities were performed using industry-standard security tools and methodologies, with our team accessing the environment through authorized and secure channels.

Methodology

The penetration testing assessment was conducted using industry-standard security testing methodologies and tools. The approach included reconnaissance, vulnerability identification, and validation of potential security weaknesses within the target web application. Testing was performed in a controlled manner to avoid service disruption and followed recognized best practices for ethical hacking and web application security testing.

Planning -This initial phase established the engagement scope, objectives, and testing boundaries while coordinating with key stakeholders to ensure minimal operational impact.
Reconnaissance - During this phase, we mapped the target environment to understand the network architecture and identify potential entry points through both passive and active information gathering.
Testing - The core assessment phase combines automated security tools with manual testing techniques to identify and validate potential security vulnerabilities within the defined scope.
Reporting - The final phase involved analyzing findings, assigning risk ratings, and developing actionable remediation recommendations documented in this report.

Scope

Asset Details	Scope Details
Domain Name	front.stage.platform.lndx.ai

Executive Summary

On January 26, 2025, an external penetration test was performed on *https://front.stage.platform.lndx.ai/* to evaluate the security posture of the web application against current industry best practices. The assessment aimed to identify potential vulnerabilities and security weaknesses that could be exploited by unauthorized parties. Testing was conducted using industry-standard tools and methodologies in a controlled and authorized environment. The results of this assessment provide actionable insights to help improve the overall security and resilience of the application.

Testing Summary

The security assessment identified a limited number of low-risk findings within the tested web application. A total of two issues were detected, including one **low-severity** and one **Informational** finding. No high or critical vulnerabilities were observed during the testing period. The identified issues primarily relate to configuration and security header best practices and do not pose an immediate threat to the application. Overall, the application demonstrates a stable security posture, with recommended improvements to enhance defense-in-depth and security hardening.

Document Details

Pentest Report

Key Observations

No critical or high-risk vulnerabilities were identified during the assessment.
The application demonstrates a generally stable and secure configuration.
Testing was completed without causing service disruption or instability.
Identified findings are limited to low-risk and informational issues, indicating a strong baseline security posture.
Secure access controls and environment isolation were observed during testing.

Weaknesses

Minor configuration and security header issues were observed.
Limited low-risk vulnerabilities could be further mitigated to strengthen the overall security posture.
Absence of certain best-practice security controls (e.g., HTTP headers) was noted.
Findings do not pose immediate threats but should be addressed to enhance defense-in-depth.

Recommendations

Implement missing security headers (e.g., Content-Security-Policy, X-Frame-Options) to strengthen defense-in-depth.

Review and harden application configuration to reduce low-risk exposures.

Regularly monitor and update system components to maintain a stable security posture.

Conduct periodic security assessments to ensure early detection of potential vulnerabilities.

Finding Severity Ratings

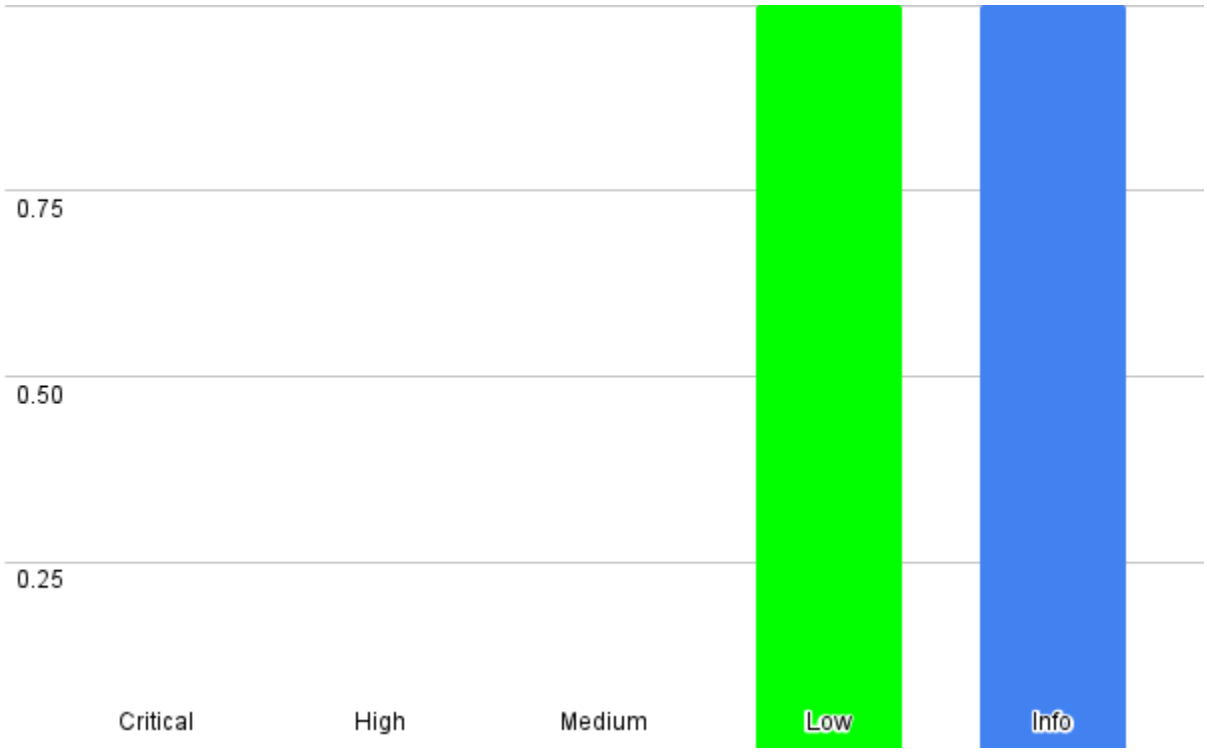
The following table defines severity levels and the corresponding CVSS score ranges used throughout the document to assess vulnerability and risk impact. CVSS Scores are used when applicable.

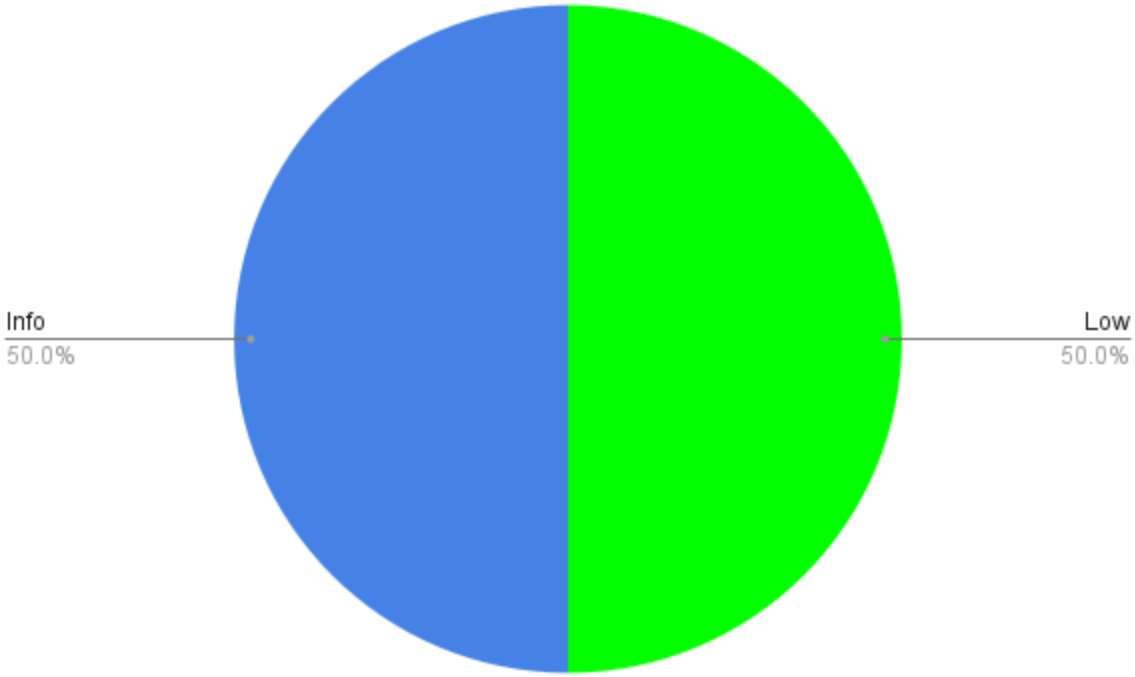
Severity	CVSS Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Info	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Vulnerability Summary

The following section details our findings categorized by severity level. Each vulnerability has been assessed based on its potential impact to the environment and likelihood of exploitation. Recommended remediation steps are provided for each finding to guide the mitigation process.

Critical	High	Medium	Low	Info
0	0	0	1	1





Description	Severity	Recommendation
virtual host found	**Low**	This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.
Permissions-Policy header not implemented	**Info**	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Technical Findings

virtual host found

Risk: low	https://front.stage.platform.lndx.ai/
CVSS Score: 3.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
EndPoint/URL	https://front.stage.platform.lndx.ai/

Description:

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same hostname.

This web server is responding differently when the Host header is manipulated, and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

Attack Details:

Virtual host: localhost
Response:
<html>
<head><title>403 Forbidden</title></head>
<body>
<h1>403 Forbidden</h1>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error pa

Impact:

sensitive information disclosure.

Recommendation:

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

References

1.https://en.wikipedia.org/wiki/Virtual_hosting

Permissions-Policy header not implemented

Risk: info	https://front.stage.platform.lndx.ai/
CVSS Score: 3.5	3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N
EndPoint/URL	https://front.stage.platform.lndx.ai/

Description:
The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Discovered by Permissions-Policy header check

Attack Details:
Locations without Permissions-Policy header:
https://front.stage.platform.lndx.ai/

References:

1.https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

2.https://www.w3.org/TR/permissions-policy-1/