Sensiba

Sundial

COMPLETE PENETRATION TEST REPORT

June 22nd, 2026

Table of Contents

Background & Confidentiality

Cybersecurity threats are constantly evolving, with attackers seeking opportunities to exploit weaknesses in systems, applications, and processes. These threats can impact the confidentiality, integrity, and availability of information, as well as disrupt business operations.

By undertaking penetration testing, organizations demonstrate a proactive approach to understanding their security posture. This type of assessment provides valuable insight into potential vulnerabilities and areas for improvement, enabling leadership to take informed steps to strengthen defenses and reduce risk.

In addition, penetration testing supports broader security and compliance objectives by providing independent validation. Regular testing helps organizations align with industry expectations, regulatory requirements, and leading practices, while building confidence among stakeholders that security risks are being addressed with diligence and accountability.

This report is intended to provide actionable information to assist in prioritizing remediation efforts and guiding continued improvements to the organization's security posture.

The report contains confidential and proprietary information and is intended solely for the use of Sundial. Distribution of this document should be limited to individuals or third parties on a need-to-know basis and only with appropriate authorization.

Executive Summary

Project Overview

Sensiba was engaged for the period of June 15th, 2026 through June 17th, 2026 to perform independent, third-party security testing for Sundial. This engagement encompassed a structured assessment and controlled testing of defined in-scope systems and environments to proactively identify security control deficiencies, system weaknesses, and exploitable vulnerabilities. All testing activities were conducted in alignment with recognized information security best practices and industry-standard penetration testing methodologies.

The primary objective of the engagement was to evaluate the organization's security posture by identifying and safely validating vulnerabilities that could result in material risk, including critical infrastructure service disruption, operational degradation, unauthorized system access, or compromise of sensitive data and systems.

Scope

The scope of the engagement included the following:

Activity	Definition
External	*.trysundial.ai

Results

Sundial engaged Sensiba to assess the security of their infrastructure environment. Sensiba found a total of 1 vulnerabilities.

External

Summary of Findings		
ID	**Vulnerability**	**Severity**
EXT.1	Use of Components With Known Vulnerabilities	Low

Assumptions and Constraints

- **Authorized Scope Only**: Testing was conducted only within the systems, networks, and applications explicitly defined in the agreed-upon scope. No testing was performed outside of this scope.
- **Access Provided**: The client provided accurate and complete information regarding system access, user accounts, and network configurations needed to perform testing.
- **Normal Operations**: It is assumed that the client's systems were operating under normal production conditions during testing unless otherwise specified.
- **Point-in-Time**: Results represent the security posture of the environment at the time of testing. Changes to systems or configurations after the engagement may alter these results.
- **Representative Accounts**: Any test accounts provided by the client are assumed to be representative of typical user roles and permissions.
- Four of the in-scope subdomains are restricted to only internal infrastructure.
- Automated destructive and intrusive testing methodologies were outside the authorized scope of this engagement, as directed by the Point-of-Contact.

Severity Ratings Calculation

Severity ratings are assigned based on the potential impact and exploitability of a vulnerability. The following categories are used:

Critical: Vulnerabilities that could lead to immediate, widespread, and severe impact on the system, data, or business operations. Exploitation is often straightforward and requires minimal technical skill. Examples include remote code execution, unauthenticated sensitive data exfiltration, or complete system compromise.

High: Vulnerabilities that could lead to significant impact on the system, data, or business operations, but may require more specific conditions or technical skill to exploit. Examples include authentication bypass, privilege escalation, or significant data loss.

Medium: Vulnerabilities that could lead to moderate impact on the system, data, or business operations. Exploitation might require specific user interaction or be limited in scope. Examples include cross-site scripting (XSS), insecure direct object references (IDOR) with limited data exposure, or information disclosure that could aid further attacks.

Low: Vulnerabilities that have a minor impact on the system or data or are difficult to exploit in a practical scenario. These often require significant preconditions or user interaction. Examples include minor configuration weaknesses, unauthenticated information disclosure with no direct impact, or verbose error messages.

Informational: Observations that are not direct vulnerabilities but provide useful information, highlight best practice deviations, or suggest potential areas for improvement. These findings do not pose a direct security risk. Examples include outdated software versions without known critical vulnerabilities, missing security headers (without a direct impact), or public-facing internal IP addresses.