SARRAL SECURITY

127.0.0.1

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-076
Version 1.0

Confidentiality Statement

This document is the exclusive property of the Client and Sarral Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Contact Information

Name	Title	Contact Information
Sarral Scan	Automated Scanner	support@sarral.io
Client	Security Team	security@127.0.0.1

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range used throughout the document.

Severity	CVSS V3 Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and data loss.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps.
Low	0.1-3.9	Vulnerabilities are non-exploitable but reduce attack surface.
Informational	N/A	No vulnerability exists. Additional information provided.

Executive Summary

Sarral Security evaluated 127.0.0.1's security posture on December 01, 2025. The following sections provide a high-level overview of vulnerabilities discovered.

Testing Summary

The assessment evaluated the target's external network security posture. The team performed vulnerability scanning and reconnaissance to identify potential risks such as exposed services, misconfigurations, and sensitive information disclosure.

Vulnerability Summary & Report Card

0	0	1	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Outdated OpenSSH Version	Medium	Upgrade OpenSSH to the latest stable version. Regularly patch and update software to address known vulnerabilities.

Technical Findings

Finding SAR-001: Outdated OpenSSH Version (Medium)

Description:	The scan identified OpenSSH version 10.0p2 running on the target. This version may be vulnerable to known security exploits. Using outdated software increases the risk of exploitation by attackers.
Risk:	Likelihood: Medium Impact: Medium
System:	127.0.0.1
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 Vulnerable and Outdated Components CWE: CWE-1104: Use of Unmaintained Third-Party Components
Evidence:	`OpenSSH 10.0p2 Debian 8 (protocol 2.0)`

Remediation

Upgrade OpenSSH to the latest stable version. Regularly patch and update software to address known vulnerabilities.