SARRAL SECURITY

127.0.0.1

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-081
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	2	2
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SAR-001: Outdated OpenSSH Version	Medium	Upgrade OpenSSH to the latest stable version.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 mitigate known vulnerabilities.
SAR-002: Connection Refused	Low	Verify that the intended services are running on the target IP address and that no firewall rules are blocking the connection. Check DNS configuration for www.127.0.0.1.
SAR-003: Connection Refused	Low	Verify that the web services are running and properly configured. Check firewall rules to ensure that traffic to ports 80 and 443 is allowed. Investigate any network connectivity issues.
SAR-004: Domain Enumeration	Info	Review the identified domain and ensure that all subdomains are properly secured and configured.
SAR-005: WHOIS Information Disclosure	Info	No remediation is necessary as this is standard information for loopback addresses.

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 attack surface and potential for exploitation.
Risk:	Likelihood: Low Impact: Medium
System:	127.0.0.1
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1189 - Reliance on Obsolete Function
Evidence:	`Nmap scan report: OpenSSH 10.0p2 Debian 8`

Remediation

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

Finding SAR-002: Connection Refused (Low)

Description:	WebScraperRecon failed to connect to the target 127.0.0.1 on both HTTP and HTTPS ports. This indicates that either no service is listening on those ports, or a firewall is blocking the connection. Additionally, attempts to resolve www.127.0.0.1 failed, indicating a DNS resolution issue.
Risk:	Likelihood: High Impact: Low
System:	127.0.0.1
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: OWASP-CM-002: Default Credentials CWE: CWE-200
Evidence:	`Connection refused errors for 127.0.0.1 on ports 80 and 443. Name resolution failure for www.127.0.0.1.`

Remediation

Verify that the intended services are running on the target IP address and that no firewall rules are blocking the connection. Check DNS configuration for www.127.0.0.1.

Finding SAR-003: Connection Refused (Low)

Description:	The scan tools were unable to establish connections to the target host on ports 80 and 443. This could indicate that the services are not running, are blocked by a firewall, or are otherwise inaccessible.
Risk:	Likelihood: Medium Impact: Low
System:	127.0.0.1
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A03:2021 - Injection CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`WhatWeb: Connection refused errors. WafW00f: Connection refused errors. SSLScan: Connection refused errors.`

Remediation

Verify that the web services are running and properly configured. Check firewall rules to ensure that traffic to ports 80 and 443 is allowed. Investigate any network connectivity issues.

Finding SAR-004: Domain Enumeration (Info)

Description:	The tool Subfinder successfully enumerated the domain projectdiscovery.io. This information can be used for further reconnaissance and attack surface mapping.
Risk:	Likelihood: High Impact: Info
System:	127.0.0.1
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: OWASP-DV-008: Information Disclosure CWE: CWE-200
Evidence:	`Domain: projectdiscovery.io`

Remediation

Review the identified domain and ensure that all subdomains are properly secured and configured.

Finding SAR-005: WHOIS Information Disclosure (Info)

Description:	WHOIS information for the target IP address range (127.0.0.0/8) reveals the organization responsible is Internet Assigned Numbers Authority (IANA). This is standard for loopback addresses.
Risk:	Likelihood: High Impact: Info
System:	127.0.0.1
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: OWASP-DV-008: Information Disclosure CWE: CWE-200
Evidence:	`WHOIS record for 127.0.0.0/8 showing IANA as the responsible organization.`

Remediation

No remediation is necessary as this is standard information for loopback addresses.