SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-077
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@sarral.io

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 sarral.io'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	1	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Outdated Software Component	Medium	Upgrade OpenSSH and Apache to the latest stable versions. Regularly patch and update software to mitigate known vulnerabilities.
SAR-002: Information Disclosure - Email Address	Low	Consider removing or obfuscating the email address from public web pages. Implement measures to protect against phishing and social engineering attacks.
SAR-003: Web Application Firewall Detection	Info	Implement a web application firewall (WAF) to protect the web server from common web attacks.

Technical Findings

Finding SAR-001: Outdated Software Component (Medium)

Description:	The scan identified the versions of OpenSSH (9.6p1) and Apache (2.4.58). These versions may be vulnerable to known exploits. An attacker could leverage these vulnerabilities to compromise the server.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`OpenSSH 9.6p1 Ubuntu 3ubuntu13.11, Apache httpd 2.4.58`

Remediation

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

Finding SAR-002: Information Disclosure - Email Address (Low)

Description:	The scan identified an email address (info@sarral.io) associated with the domain. This information could be used for phishing attacks or social engineering.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`Email[info@sarral.io]`

Remediation

Consider removing or obfuscating the email address from public web pages. Implement measures to protect against phishing and social engineering attacks.

Finding SAR-003: Web Application Firewall Detection (Info)

Description:	The web application firewall fingerprinting tool (WafW00f) did not detect a web application firewall (WAF) in front of the web server. This increases the attack surface.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-200
Evidence:	`No WAF detected by the generic detection`

Remediation

Implement a web application firewall (WAF) to protect the web server from common web attacks.