

SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025

Project: SAR-069

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	3	1	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Outdated Web Server Software	Medium	Upgrade to the latest stable version of Apache to patch known vulnerabilities. Regularly check for security updates.
SAR-002: Outdated SSH Server Software	Medium	Upgrade to the latest stable version of OpenSSH to patch known vulnerabilities. Regularly check for security updates.
SAR-003: No Web Application Firewall Detected	Medium	Implement a Web Application Firewall (WAF) to protect the web application from common web exploits such as SQL injection and cross-site scripting (XSS).
SAR-004: Email Address Exposure	Low	Consider obfuscating or removing the email address from the website to reduce the risk of it being harvested by malicious actors.

Technical Findings

Finding SAR-001: Outdated Web Server Software (Medium)

Description:	The web server is running Apache version 2.4.58. This version may contain known vulnerabilities. Attackers could potentially exploit these vulnerabilities to compromise the server.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1035 - Improperly Configured Application Settings
Evidence:	Apache httpd 2.4.58

Remediation

Upgrade to the latest stable version of Apache to patch known vulnerabilities. Regularly check for security updates.

Finding SAR-002: Outdated SSH Server Software (Medium)

Description:	The SSH server is running OpenSSH 9.6p1. This version may contain known vulnerabilities. Attackers could potentially exploit these vulnerabilities to compromise the server.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1035 - Improperly Configured Application Settings
Evidence:	OpenSSH 9.6p1 Ubuntu 3ubuntu13.11

Remediation

Upgrade to the latest stable version of OpenSSH to patch known vulnerabilities. Regularly check for security updates.

Finding SAR-003: No Web Application Firewall Detected (Medium)

Description:	The scan indicates that no Web Application Firewall (WAF) was detected. A WAF provides a layer of security to protect against common web exploits.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A04:2021 - Insecure Design CWE: CWE-200
Evidence:	No WAF detected by the generic detection

Remediation

Implement a Web Application Firewall (WAF) to protect the web application from common web exploits such as SQL injection and cross-site scripting (XSS).

Finding SAR-004: Email Address Exposure (Low)

Description:	The website exposes an email address (info@sarral.io). This information can be used for reconnaissance or phishing attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	Email[info@sarral.io]

Remediation

Consider obfuscating or removing the email address from the website to reduce the risk of it being harvested by malicious actors.
