SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-083
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SAR-001: Outdated Apache Version	Medium	Upgrade to the latest stable version of Apache httpd.
SAR-002: No WAF Detected	Low	Consider implementing a Web Application Firewall (WAF) to protect against common web application attacks.
SAR-003: Web Server Information Leak	Info	Configure the web server to suppress the display of the server version in HTTP responses.

Technical Findings

Finding SAR-001: Outdated Apache Version (Medium)

Description:	The server is running Apache httpd 2.4.58. While not immediately vulnerable, outdated software may contain unpatched security vulnerabilities. Newer versions often include security enhancements and bug fixes.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104 - Use of Unmaintained Third-Party Components
Evidence:	`Apache httpd 2.4.58`

Remediation

Upgrade to the latest stable version of Apache httpd.

Finding SAR-002: No WAF Detected (Low)

Description:	The scan did not detect a Web Application Firewall (WAF) in front of the web server. While not a vulnerability in itself, the absence of a WAF increases the attack surface and potential impact of web application vulnerabilities.
Risk:	Likelihood: Low Impact: Low
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

Consider implementing a Web Application Firewall (WAF) to protect against common web application attacks.

Finding SAR-003: Web Server Information Leak (Info)

Description:	The server is leaking information about the web server software and version (Apache/2.4.58 (Ubuntu)). This information can be used by attackers to identify known vulnerabilities in the server software.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)]`

Remediation

Configure the web server to suppress the display of the server version in HTTP responses.