SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-086
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	2	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Outdated Apache Web Server	Medium	Upgrade to the latest stable version of Apache httpd. Monitor security advisories for any vulnerabilities related to the current version.
SAR-002: Weak SSL Certificate Key Strength	Low	Reissue the SSL certificate with a stronger ECC key strength (256 bits or higher).
SAR-003: No WAF Detected	Low	Consider implementing a Web Application Firewall (WAF) to protect against common web application attacks.
SAR-004: OpenSSH version information disclosure	Info	Consider disabling version information disclosure in the SSH configuration.

Technical Findings

Finding SAR-001: Outdated Apache Web Server (Medium)

Description:	The server is running Apache httpd 2.4.58. While this version is relatively recent, older versions of Apache may contain known vulnerabilities. Regularly updating to the latest stable version is crucial for security.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A09-Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`Nmap scan identified Apache httpd 2.4.58`

Remediation

Upgrade to the latest stable version of Apache httpd. Monitor security advisories for any vulnerabilities related to the current version.

Finding SAR-002: Weak SSL Certificate Key Strength (Low)

Description:	The SSL certificate uses an ECC key with a strength of 128 bits. While functional, stronger key strengths (e.g., 256 bits or higher) are recommended for enhanced security and resistance against cryptographic attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	SSLScan
References:	OWASP: A02-Cryptographic Failures CWE: CWE-326
Evidence:	`SSLScan reported ECC Key Strength: 128`

Remediation

Reissue the SSL certificate with a stronger ECC key strength (256 bits or higher).

Finding SAR-003: No WAF Detected (Low)

Description:	A Web Application Firewall (WAF) was not detected. While not always necessary, a WAF can provide an additional layer of security against common web application attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WafW00f
References:	OWASP: A06-Security Misconfiguration CWE: CWE-200
Evidence:	`WafW00f reported no WAF detected.`

Remediation

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

Finding SAR-004: OpenSSH version information disclosure (Info)

Description:	The server is running OpenSSH 9.6p1 Ubuntu 3ubuntu13.11. While not inherently a vulnerability, disclosing the version allows attackers to identify potential vulnerabilities associated with that specific version.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A06-Security Misconfiguration CWE: CWE-200
Evidence:	`Nmap scan identified OpenSSH 9.6p1 Ubuntu 3ubuntu13.11`

Remediation

Consider disabling version information disclosure in the SSH configuration.