SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-084
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	2	4	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers on the web server. For example, use the Strict-Transport-Security header to enforce HTTPS, the X-Frame-Options header to prevent clickjacking, and the X-Content-...
SAR-002: Outdated Apache version	Medium	Upgrade Apache httpd to the latest stable version.
SAR-003: Publicly Accessible Email Addresses	Low	Consider obfuscating email addresses on the website or using a contact form instead. Implement measures to protect against spam and phishing attacks.
SAR-004: Unresponsive Subdomain	Low	Investigate the DNS configuration for www.pay.sarral.io and ensure it is correctly configured. If the subdomain is no longer in use, remove the DNS record to prevent potential subdomain takeover.
SAR-005: TRACE Method Enabled	Low	Disable the TRACE method on the web server to prevent potential information leakage.
SAR-006: Information Leak: Email Address Disclosure	Low	Review the website content and remove or obfuscate the email address if it is not intended for public disclosure.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The target is missing several security headers, including HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. These headers help protect against common web attacks such as cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`pay.sarral.io, sarral.io and sophie.sarral.io are missing security headers`

Remediation

Implement the missing security headers on the web server. For example, use the Strict-Transport-Security header to enforce HTTPS, the X-Frame-Options header to prevent clickjacking, and the X-Content-Type-Options header to prevent MIME sniffing.

Finding SAR-002: Outdated Apache version (Medium)

Description:	The server is running Apache httpd 2.4.58. While not immediately critical, running the latest version ensures that all security patches are applied. Older versions may contain known vulnerabilities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`Apache httpd 2.4.58`

Remediation

Upgrade Apache httpd to the latest stable version.

Finding SAR-003: Publicly Accessible Email Addresses (Low)

Description:	Email addresses (Info@sarral.io, info@sarral.io) have been found on the website. This information can be used by attackers for spamming, phishing, and social engineering attacks.
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 addresses Info@sarral.io and info@sarral.io found on www.sarral.io and sarral.io`

Remediation

Consider obfuscating email addresses on the website or using a contact form instead. Implement measures to protect against spam and phishing attacks.

Finding SAR-004: Unresponsive Subdomain (Low)

Description:	The subdomain www.pay.sarral.io is not resolving, indicating a potential misconfiguration or abandoned subdomain. This could lead to subdomain takeover vulnerabilities if not properly managed.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`www.pay.sarral.io fails to resolve`

Remediation

Investigate the DNS configuration for www.pay.sarral.io and ensure it is correctly configured. If the subdomain is no longer in use, remove the DNS record to prevent potential subdomain takeover.

Finding SAR-005: TRACE Method Enabled (Low)

Description:	The HTTP TRACE method is enabled on pay.sarral.io and sophie.sarral.io. This method can be used to potentially expose sensitive information, such as cookies, when combined with cross-site scripting (XSS) attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`TRACE method enabled on pay.sarral.io and sophie.sarral.io`

Remediation

Disable the TRACE method on the web server to prevent potential information leakage.

Finding SAR-006: Information Leak: Email Address Disclosure (Low)

Description:	The WhatWeb scan identified an email address (info@sarral.io) publicly accessible on the website. This information can be used for reconnaissance or targeted 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
Evidence:	`Email[info@sarral.io]`

Remediation

Review the website content and remove or obfuscate the email address if it is not intended for public disclosure.