SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-072
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	3	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Configure the web server to send the following security headers: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. Refer to the documentati...
SAR-002: Outdated Nginx Version	Medium	Upgrade Nginx to the latest stable version to patch any known security vulnerabilities.
SAR-003: Exposed Email Addresses	Low	Consider using a contact form instead of directly exposing email addresses on the website. If email addresses must be displayed, implement measures to prevent scraping and reduce the risk of spam.
SAR-004: Exposed Phone Numbers	Low	Consider using a contact form instead of directly exposing phone numbers on the website. If phone numbers must be displayed, implement measures to prevent scraping and reduce the risk of spam.
SAR-005: HTTP TRACE Method Enabled	Low	Disable the HTTP TRACE method on the web server to prevent potential information leakage.
SAR-006: Unresponsive Subdomain	Info	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 future abuse.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The web server is not sending several security headers, including HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. These headers can help protect against various 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: A07:2021 – Identification and Authentication Failures CWE: CWE-16: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Evidence:	`sarral.io, www.sarral.io, and sophie.sarral.io are missing multiple security headers.`

Remediation

Configure the web server to send the following security headers: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. Refer to the documentation for your web server for instructions on how to configure these headers.

Finding SAR-002: Outdated Nginx Version (Medium)

Description:	The subdomain sophie.sarral.io is running an outdated version of Nginx (1.18.0). This version may contain known security vulnerabilities that could be exploited by attackers.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 – Vulnerable and Outdated Components CWE: CWE-1189: Improper Prevention of Unexpected High Resource Consumption (Resource Exhaustion)
Evidence:	`sophie.sarral.io is running Nginx version 1.18.0.`

Remediation

Upgrade Nginx to the latest stable version to patch any known security vulnerabilities.

Finding SAR-003: Exposed Email Addresses (Low)

Description:	Email addresses (Info@sarral.io, info@sarral.io) were found on the sarral.io and www.sarral.io websites. While not a direct vulnerability, this information can be used for phishing attacks or spam campaigns.
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 addresses found on sarral.io and www.sarral.io.`

Remediation

Consider using a contact form instead of directly exposing email addresses on the website. If email addresses must be displayed, implement measures to prevent scraping and reduce the risk of spam.

Finding SAR-004: Exposed Phone Numbers (Low)

Description:	Phone numbers (303035 100) were found on the sarral.io and www.sarral.io websites. While not a direct vulnerability, this information can be used for social engineering attacks or spam campaigns.
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:	`Phone numbers found on sarral.io and www.sarral.io.`

Remediation

Consider using a contact form instead of directly exposing phone numbers on the website. If phone numbers must be displayed, implement measures to prevent scraping and reduce the risk of spam.

Finding SAR-005: HTTP TRACE Method Enabled (Low)

Description:	The HTTP TRACE method is enabled on pay.sarral.io, sarral.io, www.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: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`HTTP TRACE method is enabled on pay.sarral.io, sarral.io, www.sarral.io and sophie.sarral.io.`

Remediation

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

Finding SAR-006: Unresponsive Subdomain (Info)

Description:	The subdomain www.pay.sarral.io is not resolving, indicating a potential misconfiguration or decommissioned service. This could lead to user confusion or a potential attack vector if the domain is later acquired by a malicious actor.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09:2021 – Security Logging and Monitoring Failures CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
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 future abuse.