SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-073
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	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers on the web server. Specifically, configure HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protection headers ...
SAR-002: TRACE method enabled	Low	Disable the TRACE HTTP method on the web server. This can typically be done by configuring the server to not accept TRACE requests.
SAR-003: Exposed Phone Numbers and Social Media Links	Info	Review the content of sophie.sarral.io and remove any sensitive information that should not be publicly available. Consider implementing measures to prevent automated scraping of contact information.
SAR-004: Unresolvable Subdomain	Info	Investigate the DNS configuration for www.pay.sarral.io and ensure that it is properly configured. If the subdomain is no longer in use, remove the DNS record to prevent confusion.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The target domain and subdomain are missing several security headers, including HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protection. These headers help protect against various attacks, such as cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A07:2021 - Identification and Authentication Failures CWE: CWE-16
Evidence:	`sarral.io, www.sarral.io, and sophie.sarral.io are missing security headers.`

Remediation

Implement the missing security headers on the web server. Specifically, configure HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protection headers with appropriate values to mitigate potential attacks.

Finding SAR-002: TRACE method enabled (Low)

Description:	The TRACE HTTP method is enabled on the server. This method can be used to 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:	`The TRACE method is enabled on sarral.io, www.sarral.io, and pay.sarral.io.`

Remediation

Disable the TRACE HTTP method on the web server. This can typically be done by configuring the server to not accept TRACE requests.

Finding SAR-003: Exposed Phone Numbers and Social Media Links (Info)

Description:	The subdomain sophie.sarral.io exposes numerous phone numbers and social media links. This information could be used for social engineering or other malicious purposes.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`sophie.sarral.io exposes numerous phone numbers and social media links.`

Remediation

Review the content of sophie.sarral.io and remove any sensitive information that should not be publicly available. Consider implementing measures to prevent automated scraping of contact information.

Finding SAR-004: Unresolvable Subdomain (Info)

Description:	The subdomain www.pay.sarral.io does not resolve to an IP address. This could indicate a misconfiguration or an abandoned resource.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`www.pay.sarral.io does not resolve.`

Remediation

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