SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-070
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	2	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: Publicly Accessible API Endpoints	Medium	Implement proper authentication and authorization mechanisms for the API endpoints. Ensure that the endpoints do not expose sensitive information without proper access controls.
SAR-003: Information Leak - Phone Numbers	Low	Review the content of 'sophie.sarral.io' and remove any unnecessary or sensitive phone numbers. Implement input validation and sanitization to prevent the accidental exposure of phone numbers.
SAR-004: TRACE method enabled	Low	Disable the TRACE method on the web server.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The subdomains 'pay.sarral.io', 'sophie.sarral.io', 'sarral.io' and 'www.sarral.io' are 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 various attacks, such as man-in-the-middle attacks, clickjacking, and cross-site scripting.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`Security headers are null in the WebScraperRecon output for the identified subdomains.`

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: Publicly Accessible API Endpoints (Medium)

Description:	The website 'www.sarral.io' exposes API endpoints '/api.js' and '/api.js?render=6LfwfTgrAAAAAF8FCXh_3WsE_uYRB_9I9f6Qx_9R'. These endpoints may reveal sensitive information or provide unauthorized access to functionalities if not properly secured.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`The 'api_endpoints' field in the WebScraperRecon output for 'www.sarral.io' contains a list of API endpoints.`

Remediation

Implement proper authentication and authorization mechanisms for the API endpoints. Ensure that the endpoints do not expose sensitive information without proper access controls.

Finding SAR-003: Information Leak - Phone Numbers (Low)

Description:	The subdomain 'sophie.sarral.io' has a large number of phone numbers scraped from the page. While many appear to be test data, the presence of valid-looking numbers could lead to potential privacy concerns or 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:	`The 'phones' field in the WebScraperRecon output for 'sophie.sarral.io' contains a list of phone numbers.`

Remediation

Review the content of 'sophie.sarral.io' and remove any unnecessary or sensitive phone numbers. Implement input validation and sanitization to prevent the accidental exposure of phone numbers.

Finding SAR-004: TRACE method enabled (Low)

Description:	The HTTP TRACE method is enabled on 'pay.sarral.io', 'sophie.sarral.io' and 'www.sarral.io'. This method can be used to expose sensitive information, such as cookies, via cross-site tracing (XST) 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 'http_methods' field in the WebScraperRecon output for 'pay.sarral.io', 'sophie.sarral.io' and 'www.sarral.io' contains TRACE.`

Remediation

Disable the TRACE method on the web server.