SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-071
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	3	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers on the web server configuration. Specifically, enable HSTS, set appropriate X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-X...
SAR-002: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server. This can typically be done by configuring the web server to not allow the TRACE method.
SAR-003: Information Disclosure - Emails and Phone Numbers	Low	Review the website content and remove any unnecessary email addresses or phone numbers. Implement measures to protect against email harvesting.
SAR-004: reCaptcha Key Exposure	Low	Ensure the reCaptcha key is properly configured and consider implementing server-side validation to prevent abuse. Monitor reCaptcha usage for any suspicious activity.
SAR-005: Outdated Browser Warning	Info	Consider using a more generic message or a dynamic approach to detect and inform users about outdated browsers without explicitly mentioning specific versions.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The subdomains 'pay.sarral.io', 'sophie.sarral.io' and the main domain '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:	`The security_headers section in the WebScraperRecon output shows null values for these headers on 'pay.sarral.io', 'sophie.sarral.io' and 'sarral.io'.`

Remediation

Implement the missing security headers on the web server configuration. Specifically, enable HSTS, set appropriate X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection headers.

Finding SAR-002: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on 'pay.sarral.io', 'sophie.sarral.io' and 'www.sarral.io'. This method can be used in cross-site tracing (XST) attacks to steal cookies or other sensitive information.
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 section in the WebScraperRecon output includes TRACE for 'pay.sarral.io', 'sophie.sarral.io' and 'www.sarral.io'.`

Remediation

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

Finding SAR-003: Information Disclosure - Emails and Phone Numbers (Low)

Description:	The web scraper identified email addresses (Info@sarral.io, info@sarral.io) and phone numbers (303035 100) on the 'www.sarral.io' and 'sarral.io' websites. This information can be used for phishing attacks or other malicious purposes.
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 emails and phones sections in the WebScraperRecon output for 'www.sarral.io' and 'sarral.io' contain the identified email addresses and phone numbers.`

Remediation

Review the website content and remove any unnecessary email addresses or phone numbers. Implement measures to protect against email harvesting.

Finding SAR-004: reCaptcha Key Exposure (Low)

Description:	The website exposes the reCaptcha site key (6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee) in the HTML source code. While this key is intended for public use, it's best practice to avoid direct exposure to prevent potential abuse or misuse.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The comments section in the WebScraperRecon output for 'www.sarral.io' and 'sarral.io' contains the HTML code with the reCaptcha site key.`

Remediation

Ensure the reCaptcha key is properly configured and consider implementing server-side validation to prevent abuse. Monitor reCaptcha usage for any suspicious activity.

Finding SAR-005: Outdated Browser Warning (Info)

Description:	The website includes a warning message for users with outdated Internet Explorer versions (<= IE 9), suggesting they upgrade their browser. While this is a good practice, it also reveals information about the technologies used and the target audience.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The comments section in the WebScraperRecon output for 'www.sarral.io' and 'sarral.io' contains the HTML code for the outdated browser warning.`

Remediation

Consider using a more generic message or a dynamic approach to detect and inform users about outdated browsers without explicitly mentioning specific versions.
