SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 29, 2025
Project: SAR-064
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 November 29, 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	4	1
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: Exposed Email Addresses	Low	Consider obfuscating email addresses on the website or using a contact form instead.
SAR-003: Exposed Phone Numbers	Low	Consider removing or obfuscating phone numbers on the website.
SAR-004: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server.
SAR-005: reCaptcha Key Exposure	Low	Ensure that the reCaptcha key is properly protected and not directly exposed in client-side code if possible. Consider implementing server-side validation of reCaptcha responses.
SAR-006: Internal Comments Exposed	Info	Remove internal comments from the production code.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The target domain and subdomains 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-Security Misconfiguration CWE: CWE-16
Evidence:	`Security headers are null for sarral.io, www.sarral.io and pay.sarral.io`

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: Exposed Email Addresses (Low)

Description:	Email addresses (Info@sarral.io, info@sarral.io) were found on the website. 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-Broken Access Control CWE: CWE-200
Evidence:	`Email addresses found on sarral.io and www.sarral.io`

Remediation

Consider obfuscating email addresses on the website or using a contact form instead.

Finding SAR-003: Exposed Phone Numbers (Low)

Description:	Phone numbers (303035 100) were found on the website. This information can be used for unsolicited calls or social engineering attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A01-Broken Access Control CWE: CWE-200
Evidence:	`Phone numbers found on sarral.io and www.sarral.io`

Remediation

Consider removing or obfuscating phone numbers on the website.

Finding SAR-004: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on pay.sarral.io and sophie.sarral.io. This method can be used to conduct cross-site tracing (XST) attacks, potentially allowing an attacker to steal cookies or other sensitive information.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`TRACE method enabled on pay.sarral.io and sophie.sarral.io`

Remediation

Disable the TRACE HTTP method on the web server.

Finding SAR-005: reCaptcha Key Exposure (Low)

Description:	The reCaptcha site key (6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee) is exposed in the source code of contact-us.html. While this key is intended for public use, its exposure could potentially be abused by attackers to automate requests or bypass reCaptcha protection.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`reCaptcha key found on contact-us.html`

Remediation

Ensure that the reCaptcha key is properly protected and not directly exposed in client-side code if possible. Consider implementing server-side validation of reCaptcha responses.

Finding SAR-006: Internal Comments Exposed (Info)

Description:	Internal comments such as 'TODO: replace with variable/translation for this' are exposed in the source code of pay.sarral.io. These comments may reveal information about the development process or internal structure of the application.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A01-Broken Access Control CWE: CWE-200
Evidence:	`Internal comments found on pay.sarral.io`

Remediation

Remove internal comments from the production code.