SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 03, 2025
Project: SAR-110
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 03, 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	2	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: Exposed Email Addresses	Low	Consider using a contact form instead of directly exposing email addresses. Implement email obfuscation techniques if direct exposure is necessary.
SAR-003: reCAPTCHA Client-Side Implementation	Low	Implement server-side reCAPTCHA validation to ensure that the reCAPTCHA response is verified on the server before processing the form submission. Consider using a more robust bot detection mechanism.
SAR-004: Domain Name Resolution Errors	Info	Verify the DNS configuration for the affected subdomains and ensure the web servers are running correctly.
SAR-005: Publicly Accessible Social Media Profiles	Info	Review the privacy settings of the identified social media profiles and limit the amount of publicly available information.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The target domain sophie.sarral.io is 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 man-in-the-middle attacks, cross-site scripting (XSS), and clickjacking.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16: Improper Neutralization of Input During Initialization
Evidence:	`Security headers are null for hsts, csp, x_frame_options, x_content_type_options, referrer_policy, permissions_policy, and x_xss_protection.`

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 enhance security.

Finding SAR-002: Exposed Email Addresses (Low)

Description:	The web scraper found email addresses (Info@sarral.io, info@sarral.io) on the sarral.io domain. While not a critical vulnerability, exposing email addresses can lead to spam and targeted phishing attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`Email addresses Info@sarral.io and info@sarral.io were found on the sarral.io domain.`

Remediation

Consider using a contact form instead of directly exposing email addresses. Implement email obfuscation techniques if direct exposure is necessary.

Finding SAR-003: reCAPTCHA Client-Side Implementation (Low)

Description:	The contact page on sarral.io uses a client-side implementation of reCAPTCHA. While this provides some protection against automated bots, it can be bypassed by sophisticated attackers. The site key is also exposed.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A07:2021 - Identification and Authentication Failures CWE: CWE-602: Client-Side Enforcement of Server-Side Security
Evidence:	`The contact page includes a reCAPTCHA with site key 6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee.`

Remediation

Implement server-side reCAPTCHA validation to ensure that the reCAPTCHA response is verified on the server before processing the form submission. Consider using a more robust bot detection mechanism.

Finding SAR-004: Domain Name Resolution Errors (Info)

Description:	The web scraper encountered name resolution errors for www.sophie.sarral.io and www.pay.sarral.io. This indicates a potential misconfiguration or downtime of these subdomains.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-359: Exposure of Arbitrary Memory Location
Evidence:	`NameResolutionError for www.sophie.sarral.io and www.pay.sarral.io.`

Remediation

Verify the DNS configuration for the affected subdomains and ensure the web servers are running correctly.

Finding SAR-005: Publicly Accessible Social Media Profiles (Info)

Description:	The web scraper identified publicly accessible social media profiles associated with the organization and its employees. This information can be used for social engineering attacks.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`LinkedIn profiles of employees and GitHub links were found on the sarral.io domain.`

Remediation

Review the privacy settings of the identified social media profiles and limit the amount of publicly available information.