SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 03, 2025
Project: SAR-107
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	3	3	3
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the following security headers: HSTS to enforce HTTPS, X-Frame-Options to prevent clickjacking, X-Content-Type-Options to prevent MIME sniffing, Referrer-Policy to control referrer informati...
SAR-002: Outdated Libraries	Medium	Update all libraries to their latest versions to patch known vulnerabilities. Implement a process for regularly monitoring and updating dependencies.
SAR-003: reCaptcha Key Exposure	Medium	Ensure that the reCaptcha implementation is properly configured and that the site key is not being misused. Consider implementing server-side validation of reCaptcha responses.
SAR-004: Publicly Accessible Email Addresses	Low	Implement measures to protect against spam and phishing attacks, such as using a dedicated email address for public inquiries and educating users about phishing awareness.
SAR-005: Unsanitized Phone Numbers	Low	Sanitize and validate phone numbers to ensure they are valid and do not contain sensitive information. Remove any test data or invalid phone numbers.
SAR-006: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server to prevent XST attacks.
SAR-007: Information Exposure via WHOIS	Info	Consider the privacy implications of WHOIS data. Ensure that only necessary information is publicly available. Monitor WHOIS records for unauthorized changes.
SAR-008: Subdomain Enumeration	Info	Regularly audit and monitor subdomains to ensure they are properly secured and configured. Remove any unused or outdated subdomains to reduce the attack surface.
SAR-009: Publicly Accessible Social Media Profiles	Info	Review the content and security settings of the linked social media profiles. Ensure that employees are aware of social engineering risks.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The subdomain 'pay.sarral.io' is missing several security headers, including HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protection. This can leave the application vulnerable to various attacks, including man-in-the-middle attacks, clickjacking, and cross-site scripting.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05-Security Misconfiguration CWE: CWE-16
Evidence:	`Missing HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protection headers on pay.sarral.io`

Remediation

Implement the following security headers: HSTS to enforce HTTPS, X-Frame-Options to prevent clickjacking, X-Content-Type-Options to prevent MIME sniffing, Referrer-Policy to control referrer information, Permissions-Policy to control browser features, and X-XSS-Protection to enable XSS filtering.

Finding SAR-002: Outdated Libraries (Medium)

Description:	The 'sophie.sarral.io' subdomain uses outdated libraries, specifically core-js. This can expose the application to known vulnerabilities in these libraries.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A09-Using Components with Known Vulnerabilities CWE: CWE-1035
Evidence:	`References to outdated core-js library.`

Remediation

Update all libraries to their latest versions to patch known vulnerabilities. Implement a process for regularly monitoring and updating dependencies.

Finding SAR-003: reCaptcha Key Exposure (Medium)

Description:	The 'www.sarral.io' website exposes a reCaptcha site key in the HTML source code. While this key is intended for client-side use, it could potentially be abused by attackers to automate requests or bypass reCaptcha protection.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200

Evidence:	`reCaptcha site key found in HTML source code:`
	`6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee`

Remediation

Ensure that the reCaptcha implementation is properly configured and that the site key is not being misused. Consider implementing server-side validation of reCaptcha responses.

Finding SAR-004: Publicly Accessible Email Addresses (Low)

Description:	Email addresses (Info@sarral.io, info@sarral.io) were found on the 'www.sarral.io' website. This increases the risk of spam and targeted phishing attacks.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: OWASP-10 CWE: CWE-200
Evidence:	`Email addresses found: Info@sarral.io, info@sarral.io`

Remediation

Implement measures to protect against spam and phishing attacks, such as using a dedicated email address for public inquiries and educating users about phishing awareness.

Finding SAR-005: Unsanitized Phone Numbers (Low)

Description:	The 'sophie.sarral.io' subdomain exposes a large number of phone numbers, some of which appear to be test data or invalid. This could potentially be used for enumeration or other malicious purposes.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: OWASP-10 CWE: CWE-200
Evidence:	`Large number of phone numbers found on sophie.sarral.io, including test data.`

Remediation

Sanitize and validate phone numbers to ensure they are valid and do not contain sensitive information. Remove any test data or invalid phone numbers.

Finding SAR-006: 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 exposing sensitive information.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`TRACE method is enabled on pay.sarral.io and sophie.sarral.io`

Remediation

Disable the TRACE HTTP method on the web server to prevent XST attacks.

Finding SAR-007: Information Exposure via WHOIS (Info)

Description:	WHOIS information reveals domain registration details, including registrar, creation/expiry dates, and administrative contacts. While much is redacted via Domains By Proxy, the registrar and abuse contact information are exposed.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Whois
References:	OWASP: OWASP-10 CWE: CWE-200
Evidence:	`Domain Name: sarral.io, Registrar: GoDaddy.com, LLC, Registrar Abuse Contact Email: abuse@godaddy.com`

Remediation

Consider the privacy implications of WHOIS data. Ensure that only necessary information is publicly available. Monitor WHOIS records for unauthorized changes.

Finding SAR-008: Subdomain Enumeration (Info)

Description:	Multiple tools identified several subdomains associated with the target domain. This information can be used to map the attack surface and identify potential vulnerabilities in different parts of the infrastructure.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Subfinder (Passive), Amass Passive, Assetfinder
References:	OWASP: OWASP-10 CWE: CWE-200
Evidence:	`Discovered subdomains: www.sarral.io, www.pay.sarral.io, sophie.sarral.io, pay.sarral.io`

Remediation

Regularly audit and monitor subdomains to ensure they are properly secured and configured. Remove any unused or outdated subdomains to reduce the attack surface.

Finding SAR-009: Publicly Accessible Social Media Profiles (Info)

Description:	Social media profiles were found on the 'www.sarral.io' website. This information can be used for social engineering attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: OWASP-10 CWE: CWE-200
Evidence:	`Social media profiles found: LinkedIn profiles of employees`

Remediation

Review the content and security settings of the linked social media profiles. Ensure that employees are aware of social engineering risks.