SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 05, 2025
Project: SAR-112
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 05, 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	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing HTTP Strict Transport Security (HSTS) Header	Medium	Implement HSTS header with a sufficient max-age value on all HTTPS responses. Consider including subdomains and preloading HSTS.
SAR-002: Information Disclosure: Server Version	Low	Disable the server signature in the nginx configuration file to prevent version information disclosure.
SAR-003: reCAPTCHA Client-Side Implementation	Low	Implement server-side validation of the reCAPTCHA response to prevent bypass attacks.
SAR-004: Unresolved Subdomains	Low	Verify and correct the DNS records for the affected subdomains. Ensure that the subdomains are properly configured and point to the correct resources.
SAR-005: 404 Not Found	Low	Verify the configuration of the pay.sarral.io subdomain and ensure that the resource is available. If the resource is no longer available, remove the link or redirect it to a valid resource.
SAR-006: Publicly Accessible Email Addresses and Social Media Profiles	Info	Review the website content and remove or obfuscate any sensitive information that is not intended for public consumption. Implement measures to protect against phishing and social engineering attacks.
SAR-007: Subdomain Enumeration	Info	Regularly audit and monitor subdomains. Ensure all subdomains are properly secured and configured.

Technical Findings

Finding SAR-001: Missing HTTP Strict Transport Security (HSTS) Header (Medium)

Description:	The HTTP Strict Transport Security (HSTS) header is missing on pay.sarral.io and sophie.sarral.io. This allows man-in-the-middle attacks to downgrade the connection to HTTP, potentially exposing sensitive information.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-614 - Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
Evidence:	`Security headers for pay.sarral.io and sophie.sarral.io show hsts: null`

Remediation

Implement HSTS header with a sufficient max-age value on all HTTPS responses. Consider including subdomains and preloading HSTS.

Finding SAR-002: Information Disclosure: Server Version (Low)

Description:	The server version (nginx/1.18.0 (Ubuntu)) is exposed in the HTTP headers of sophie.sarral.io. This information can be used by attackers to identify known vulnerabilities in the specific version of the server software.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A03:2021 - Injection CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`Headers for sophie.sarral.io show Server: nginx/1.18.0 (Ubuntu)`

Remediation

Disable the server signature in the nginx configuration file to prevent version information disclosure.

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

Description:	The reCAPTCHA implementation on www.sarral.io appears to be client-side, making it potentially vulnerable to bypass techniques. This could allow attackers to submit forms without solving the CAPTCHA.
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:	`www.sarral.io includes client-side reCAPTCHA script and form elements.`

Remediation

Implement server-side validation of the reCAPTCHA response to prevent bypass attacks.

Finding SAR-004: Unresolved Subdomains (Low)

Description:	The subdomains www.pay.sarral.io and www.sophie.sarral.io are not resolving correctly, indicating a potential misconfiguration or outdated DNS records. This can lead to denial of service or subdomain takeover if the DNS records point to an unowned resource.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`WebScraperRecon reports NameResolutionError for www.pay.sarral.io and www.sophie.sarral.io.`

Remediation

Verify and correct the DNS records for the affected subdomains. Ensure that the subdomains are properly configured and point to the correct resources.

Finding SAR-005: 404 Not Found (Low)

Description:	The pay.sarral.io subdomain returns a 404 status code, indicating that the resource is not found. This could indicate a misconfiguration or a broken link.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`WebScraperRecon reports 404 status code for pay.sarral.io.`

Remediation

Verify the configuration of the pay.sarral.io subdomain and ensure that the resource is available. If the resource is no longer available, remove the link or redirect it to a valid resource.

Finding SAR-006: Publicly Accessible Email Addresses and Social Media Profiles (Info)

Description:	Email addresses (Info@sarral.io, info@sarral.io) and social media profiles (LinkedIn, GitHub) are publicly accessible on www.sarral.io. This information can be used for phishing attacks or social engineering.
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:	`www.sarral.io contains emails and social media profiles in its scraped content.`

Remediation

Review the website content and remove or obfuscate any sensitive information that is not intended for public consumption. Implement measures to protect against phishing and social engineering attacks.

Finding SAR-007: Subdomain Enumeration (Info)

Description:	Multiple subdomains were discovered, increasing the attack surface. While not a direct vulnerability, it provides more targets for potential attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Subfinder (Passive), Amass Passive
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`Subfinder and Amass Passive tools identified multiple subdomains.`

Remediation

Regularly audit and monitor subdomains. Ensure all subdomains are properly secured and configured.
