SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 02, 2025
Project: SAR-098
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 02, 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	2	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Information Disclosure - Phone Numbers	Medium	Review the content of sophie.sarral.io and remove any unnecessary phone numbers. Implement measures to prevent accidental exposure of sensitive information.
SAR-002: Missing HTTP Strict Transport Security (HSTS) Header	Medium	Configure the web server to include the HSTS header with a reasonable max-age value. Consider including the 'includeSubDomains' and 'preload' directives.
SAR-003: Outdated Software - Nginx	Medium	Upgrade Nginx to the latest stable version to patch any known security vulnerabilities.
SAR-004: Information Disclosure - Email Addresses	Low	Review the content of sarral.io and remove any unnecessary email addresses. Implement measures to prevent accidental exposure of sensitive information.
SAR-005: Unresponsive Subdomain	Low	Investigate the DNS configuration for www.pay.sarral.io and ensure it is correctly configured. If the subdomain is no longer in use, remove the DNS record to prevent potential misuse.
SAR-006: Deprecated Technology - Internet Explorer 9 Warning	Info	Consider removing the IE9 browser upgrade warning and focusing on supporting modern browsers with up-to-date security features.

Technical Findings

Finding SAR-001: Information Disclosure - Phone Numbers (Medium)

Description:	The sophie.sarral.io subdomain exposes a large number of phone numbers within the scraped content. This information could be used for malicious purposes such as spamming or social engineering.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01-Broken Access Control CWE: CWE-200
Evidence:	`sophie.sarral.io contains phone numbers: 0 0 0 9999, 0 0 12 12, etc.`

Remediation

Review the content of sophie.sarral.io and remove any unnecessary phone numbers. Implement measures to prevent accidental exposure of sensitive information.

Finding SAR-002: Missing HTTP Strict Transport Security (HSTS) Header (Medium)

Description:	The pay.sarral.io subdomain is missing the HTTP Strict Transport Security (HSTS) header. This header forces browsers to use HTTPS, protecting against man-in-the-middle attacks.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05-Security Misconfiguration CWE: CWE-614
Evidence:	`pay.sarral.io security_headers: hsts: null`

Remediation

Configure the web server to include the HSTS header with a reasonable max-age value. Consider including the 'includeSubDomains' and 'preload' directives.

Finding SAR-003: Outdated Software - Nginx (Medium)

Description:	The sophie.sarral.io subdomain is running an outdated version of Nginx (1.18.0). This version may contain known vulnerabilities that could be exploited.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06-Vulnerable and Outdated Components CWE: CWE-1104
Evidence:	`sophie.sarral.io headers: Server: nginx/1.18.0 (Ubuntu)`

Remediation

Upgrade Nginx to the latest stable version to patch any known security vulnerabilities.

Finding SAR-004: Information Disclosure - Email Addresses (Low)

Description:	The sarral.io domain exposes email addresses within the scraped content. This information could be used for malicious purposes such as spamming or phishing.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01-Broken Access Control CWE: CWE-200
Evidence:	`sarral.io contains email addresses: Info@sarral.io, info@sarral.io`

Remediation

Review the content of sarral.io and remove any unnecessary email addresses. Implement measures to prevent accidental exposure of sensitive information.

Finding SAR-005: Unresponsive Subdomain (Low)

Description:	The subdomain www.pay.sarral.io is not resolving, indicating a potential misconfiguration or abandoned resource. This could lead to confusion or be exploited by malicious actors.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05-Security Misconfiguration CWE: CWE-16
Evidence:	`www.pay.sarral.io errors: Failed to resolve 'www.pay.sarral.io' ([Errno -2] Name or service not known)`

Remediation

Investigate the DNS configuration for www.pay.sarral.io and ensure it is correctly configured. If the subdomain is no longer in use, remove the DNS record to prevent potential misuse.

Finding SAR-006: Deprecated Technology - Internet Explorer 9 Warning (Info)

Description:	The sarral.io domain includes a warning message suggesting users upgrade their browser if they are using Internet Explorer 9 or earlier. While not a direct vulnerability, supporting or mentioning such outdated browsers can indicate a lack of focus on modern security practices.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06-Vulnerable and Outdated Components CWE: CWE-1104
Evidence:	`sarral.io contains comment: [if lte IE 9]> ... upgrade your browser`

Remediation

Consider removing the IE9 browser upgrade warning and focusing on supporting modern browsers with up-to-date security features.
