SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-094
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 01, 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	4	6	3
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers on the web server. Specifically, enable HSTS, configure X-Frame-Options, set X-Content-Type-Options to nosniff, define a Referrer-Policy, configure Permissions-P...
SAR-002: Outdated Software	Medium	Upgrade Nginx to the latest stable version to patch any known vulnerabilities and improve security.
SAR-003: Outdated Apache Version	Medium	Upgrade Apache to the latest stable version to patch any known vulnerabilities. Monitor security advisories for Apache.
SAR-004: Missing Security Headers	Medium	Implement the missing security headers with appropriate configurations. For example, enable HSTS to enforce HTTPS, configure CSP to prevent XSS, and set X-Frame-Options to prevent clickjacking.
SAR-005: Information Disclosure - Phone Numbers	Low	Review the content of sophie.sarral.io and remove any unnecessary or sensitive phone numbers. Implement measures to prevent accidental exposure of phone numbers in the future.
SAR-006: 404 Response	Low	Investigate the pay.sarral.io subdomain and ensure it is properly configured and functioning as intended. If the subdomain is not needed, consider removing it.
SAR-007: TRACE method enabled	Low	Disable the TRACE HTTP method on the web server to prevent attackers from using it to expose sensitive information.
SAR-008: Open Ports	Low	Review the necessity of each open port. Disable any unused services to reduce the attack surface. Implement firewall rules to restrict access to necessary ports only.
SAR-009: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the server. This can typically be done in the server configuration file.

SAR-010: Domain Name Resolution Failure	Low	Investigate the DNS configuration for 'www.pay.sarral.io' to ensure it is correctly configured and resolving to the appropriate IP address. Monitor the domain for uptime and availability.
SAR-011: Subdomain Enumeration	Info	Review the discovered subdomains and ensure they are all properly secured and configured. Remove any unused or unnecessary subdomains.
SAR-012: Information Disclosure - Email Addresses	Info	Consider obfuscating or masking email addresses on the website to prevent automated harvesting by bots.
SAR-013: Outdated Browser Warning	Info	Evaluate the necessity of supporting outdated browsers like IE9. If no longer required, remove the warning and any compatibility code. If support is still needed, ensure that the website is properly s...

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The target is 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:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`The security_headers section in the WebScraperRecon output shows null values for several security headers for sarral.io and www.sarral.io.`

Remediation

Implement the missing security headers on the web server. Specifically, enable HSTS, configure X-Frame-Options, set X-Content-Type-Options to nosniff, define a Referrer-Policy, configure Permissions-Policy, and enable X-XSS-Protection.

Finding SAR-002: Outdated Software (Medium)

Description:	The sophie.sarral.io subdomain is running an outdated version of Nginx (1.18.0). Older versions of software may contain known vulnerabilities that could be exploited by attackers.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104
Evidence:	`The headers section in the WebScraperRecon output for sophie.sarral.io shows the Server is nginx/1.18.0 (Ubuntu).`

Remediation

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

Finding SAR-003: Outdated Apache Version (Medium)

Description:	The server is running Apache version 2.4.58. While not immediately vulnerable, older versions may contain known vulnerabilities that could be exploited. Regular updates are crucial for security.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WhatWeb
References:	OWASP: A06-Vulnerable and Outdated Components CWE: CWE-1104
Evidence:	`Apache[2.4.58]`

Remediation

Upgrade Apache to the latest stable version to patch any known vulnerabilities. Monitor security advisories for Apache.

Finding SAR-004: Missing Security Headers (Medium)

Description:	The application 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 cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	DNS Resolver
References:	OWASP: A07:2021 - Identification and Authentication Failures CWE: CWE-16: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
Evidence:	`sophie.sarral.io and www.sarral.io are missing security headers`

Remediation

Implement the missing security headers with appropriate configurations. For example, enable HSTS to enforce HTTPS, configure CSP to prevent XSS, and set X-Frame-Options to prevent clickjacking.

Finding SAR-005: Information Disclosure - Phone Numbers (Low)

Description:	The sophie.sarral.io subdomain exposes a large number of phone numbers. While many appear to be test data, the exposure of any phone numbers can be a privacy concern and could potentially be used for social engineering attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`The phones array in the WebScraperRecon output for sophie.sarral.io contains a large list of phone numbers.`

Remediation

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

Finding SAR-006: 404 Response (Low)

Description:	The pay.sarral.io subdomain returns a 404 Not Found error. This could indicate a misconfiguration or a broken link, potentially leading to a negative user experience.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The http_probe section in the WebScraperRecon output for pay.sarral.io shows a status_code of 404.`

Remediation

Investigate the pay.sarral.io subdomain and ensure it is properly configured and functioning as intended. If the subdomain is not needed, consider removing it.

Finding SAR-007: TRACE method enabled (Low)

Description:	The TRACE HTTP method is enabled on pay.sarral.io and sophie.sarral.io. The TRACE method can be used to expose sensitive information, such as cookies, in the HTTP request headers. This information can be used by attackers to compromise the security of the web application.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The http_methods section in the WebScraperRecon output for pay.sarral.io and sophie.sarral.io shows that the TRACE method is enabled.`

Remediation

Disable the TRACE HTTP method on the web server to prevent attackers from using it to expose sensitive information.

Finding SAR-008: Open Ports (Low)

Description:	Several ports are open, including FTP (21), SSH (22), RTSP (554), and PPTP (1723). While not inherently vulnerable, open ports increase the attack surface. FTP, RTSP, and PPTP are often unnecessary.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A01-Broken Access Control CWE: CWE-200
Evidence:	`21/tcp open ftp? 22/tcp open ssh 554/tcp open rtsp? 1723/tcp open pptp?`

Remediation

Review the necessity of each open port. Disable any unused services to reduce the attack surface. Implement firewall rules to restrict access to necessary ports only.

Finding SAR-009: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on the server. This method can be used for cross-site tracing (XST) attacks, allowing an attacker to potentially steal cookies or other sensitive information.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`The TRACE HTTP method is enabled on pay.sarral.io and sophie.sarral.io`

Remediation

Disable the TRACE HTTP method on the server. This can typically be done in the server configuration file.

Finding SAR-010: Domain Name Resolution Failure (Low)

Description:	The domain 'www.pay.sarral.io' failed to resolve during the scan, indicating a potential DNS configuration issue or downtime.
Risk:	Likelihood: High Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`www.pay.sarral.io failed to resolve.`

Remediation

Investigate the DNS configuration for 'www.pay.sarral.io' to ensure it is correctly configured and resolving to the appropriate IP address. Monitor the domain for uptime and availability.

Finding SAR-011: Subdomain Enumeration (Info)

Description:	Multiple subdomains were discovered, including www.sarral.io, pay.sarral.io, www.pay.sarral.io and sophie.sarral.io. While not a direct vulnerability, subdomain enumeration can expand the attack surface.
Risk:	Likelihood: Info Impact: Info
System:	sarral.io
Tools Used:	Subfinder (Passive), Amass Passive
References:	OWASP: N/A CWE: N/A
Evidence:	`The domains arrays in the Subfinder (Passive) and Amass Passive outputs list the discovered subdomains.`

Remediation

Review the discovered subdomains and ensure they are all properly secured and configured. Remove any unused or unnecessary subdomains.

Finding SAR-012: Information Disclosure - Email Addresses (Info)

Description:	The website exposes email addresses (Info@sarral.io, info@sarral.io) in its content, which could be used for spamming or phishing attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	DNS Resolver
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 are found on www.sarral.io`

Remediation

Consider obfuscating or masking email addresses on the website to prevent automated harvesting by bots.

Finding SAR-013: Outdated Browser Warning (Info)

Description:	The website displays a warning message for users with Internet Explorer 9 or lower, suggesting they upgrade their browser. While this is a good practice, it also indicates that the website may still be supporting or considering compatibility with very old and potentially vulnerable browsers.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	DNS Resolver
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-93: Improper Neutralization of CRLF Sequences (aka 'CRLF Injection')
Evidence:	`www.sarral.io contains code to display a browser upgrade warning for IE9 or lower.`

Remediation

Evaluate the necessity of supporting outdated browsers like IE9. If no longer required, remove the warning and any compatibility code. If support is still needed, ensure that the website is properly secured against vulnerabilities in these browsers.