SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-088
Version 1.0

Copyright © Sarral Security

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

Copyright © Sarral Security

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.

Copyright © Sarral Security

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.

BUSINESS CONFIDENTIAL
Copyright © Sarral Security

Vulnerability Summary & Report Card

0	0	4	3	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Configure the web server to send the following security headers: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy and X-XSS-Protection. Ensure that the headers are configured with a...
SAR-002: Deprecated Software	Medium	Upgrade the browser to the latest version to patch known vulnerabilities. Remove the outdated browser compatibility code from the website.
SAR-003: Outdated Apache Version	Medium	Upgrade to the latest stable version of Apache httpd to patch any known vulnerabilities.
SAR-004: Lack of Web Application Firewall	Medium	Implement a Web Application Firewall (WAF) to protect against common web vulnerabilities.
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 subdomain takeover.
SAR-006: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server. This can typically be done by configuring the web server to not allow the TRACE method.
SAR-007: Cleartext HTTP Redirect to HTTPS	Low	Ensure HSTS is enabled to prevent man-in-the-middle attacks during the initial HTTP request. Consider using HSTS preload.
SAR-008: Phone Number Exposure	Info	Review the phone numbers exposed on sophie.sarral.io and determine if any of them are sensitive. If so, remove them from the website or implement measures to protect them from unauthorized access.

Copyright © Sarral Security

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The web server is not sending several security headers, including HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-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: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A07:2021 - Identification and Authentication Failures CWE: CWE-16: Improper Neutralization of Input During Initialization
Evidence:	`www.sarral.io and sarral.io are missing HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy and X-XSS-Protection headers.`

Remediation

Configure the web server to send the following security headers: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy and X-XSS-Protection. Ensure that the headers are configured with appropriate values for the application's security requirements.

Copyright © Sarral Security

Finding SAR-002: Deprecated Software (Medium)

Description:	The website includes comments indicating the use of an outdated browser version (IE 9 or earlier). Using outdated software can expose the system to known vulnerabilities.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104: Use of Unmaintained Third Party Components
Evidence:	`Comments found on www.sarral.io and sarral.io indicate support for IE 9 or earlier.`

Remediation

Upgrade the browser to the latest version to patch known vulnerabilities. Remove the outdated browser compatibility code from the website.

Copyright © Sarral Security

Finding SAR-003: Outdated Apache Version (Medium)

Description:	The server is running Apache httpd 2.4.58. Using outdated software can expose the system to known vulnerabilities. While this version is relatively recent, it's crucial to stay updated with the latest patches.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A06-Vulnerable and Outdated Components CWE: CWE-1035
Evidence:	`Apache httpd 2.4.58`

Remediation

Upgrade to the latest stable version of Apache httpd to patch any known vulnerabilities.

Copyright © Sarral Security

Finding SAR-004: Lack of Web Application Firewall (Medium)

Description:	No Web Application Firewall (WAF) was detected. A WAF provides an additional layer of security against common web attacks.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	WafW00f
References:	OWASP: A09-Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`No WAF detected by the generic detection`

Remediation

Implement a Web Application Firewall (WAF) to protect against common web vulnerabilities.

Copyright © Sarral Security

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 subdomain takeover vulnerabilities if not properly managed.
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:	`www.pay.sarral.io fails to resolve.`

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 subdomain takeover.

Copyright © Sarral Security

Finding SAR-006: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on pay.sarral.io, www.sarral.io and sarral.io. TRACE is used for debugging purposes, but when enabled, it can be exploited to steal cookies or other sensitive information via Cross-Site Tracing (XST) attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`TRACE method is enabled on pay.sarral.io, www.sarral.io and sarral.io.`

Remediation

Disable the TRACE HTTP method on the web server. This can typically be done by configuring the web server to not allow the TRACE method.

Copyright © Sarral Security

Finding SAR-007: Cleartext HTTP Redirect to HTTPS (Low)

Description:	The server redirects HTTP requests to HTTPS. While this is generally good practice, the initial redirect over HTTP could be intercepted. However, HSTS is not explicitly reported as missing, so the risk is reduced.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WhatWeb
References:	OWASP: A02-Cryptographic Failures CWE: CWE-319
Evidence:	`http://sarral.io [301 Moved Permanently] RedirectLocation[https://sarral.io/]`

Remediation

Ensure HSTS is enabled to prevent man-in-the-middle attacks during the initial HTTP request. Consider using HSTS preload.

Copyright © Sarral Security

Finding SAR-008: Phone Number Exposure (Info)

Description:	The subdomain sophie.sarral.io exposes numerous phone numbers, which may or may not be sensitive. This information could be used for social engineering or other malicious purposes.
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:	`sophie.sarral.io exposes numerous phone numbers.`

Remediation

Review the phone numbers exposed on sophie.sarral.io and determine if any of them are sensitive. If so, remove them from the website or implement measures to protect them from unauthorized access.

Copyright © Sarral Security