SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-087
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	2	3	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement and configure the missing security headers on the web server. Specifically, enable HSTS, configure a strict CSP, set X-Frame-Options to 'sameorigin' or 'deny', enable X-Content-Type-Options,...
SAR-002: Outdated Apache Version	Medium	Upgrade to the latest stable version of Apache httpd.
SAR-003: TRACE method enabled	Low	Disable the TRACE HTTP method on the web server.
SAR-004: Outdated Browser Warning	Low	Consider removing or updating the outdated browser warning to avoid revealing potentially sensitive information. Ensure the website is compatible with modern browsers and encourage users to use them.
SAR-005: Open SSH	Low	Ensure strong SSH password policies are in place. Consider using key-based authentication and limiting access to trusted networks.
SAR-006: Unresolvable Subdomain	Info	Investigate the DNS configuration for www.pay.sarral.io. If the subdomain is no longer in use, remove the DNS record to prevent potential confusion or future exploitation.
SAR-007: Contact Information Exposure	Info	Consider using a contact form instead of directly exposing email addresses. Implement measures to prevent abuse of contact information, such as rate limiting and CAPTCHAs.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The web server is not enforcing recommended security headers, such as HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy and X-XSS-Protection. This can lead to increased risk of various attacks like XSS, clickjacking, and data injection.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A07:2021 - Identification and Authentication Failures CWE: CWE-16
Evidence:	`The security_headers section in the WebScraperRecon output shows null values for hsts, csp, x_frame_options, x_content_type_options, referrer_policy and x_xss_protection for sarral.io and www.sarral.io.`

Remediation

Implement and configure the missing security headers on the web server. Specifically, enable HSTS, configure a strict CSP, set X-Frame-Options to 'sameorigin' or 'deny', enable X-Content-Type-Options, set a Referrer-Policy, and enable X-XSS-Protection.

Finding SAR-002: Outdated Apache Version (Medium)

Description:	The server is running Apache httpd 2.4.58. While not immediately vulnerable, running the latest version ensures that all known vulnerabilities are patched. Older versions may contain security flaws that could be exploited.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000, WhatWeb
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1035 - Use of a Potentially Dangerous Function
Evidence:	`Apache httpd 2.4.58`

Remediation

Upgrade to the latest stable version of Apache httpd.

Finding SAR-003: TRACE method enabled (Low)

Description:	The TRACE HTTP method is enabled on the server. This method can be used in cross-site tracing attacks to steal cookies or other sensitive information.
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 shows TRACE method is enabled for sarral.io, www.sarral.io and pay.sarral.io.`

Remediation

Disable the TRACE HTTP method on the web server.

Finding SAR-004: Outdated Browser Warning (Low)

Description:	The website includes a warning message for users with outdated Internet Explorer versions (<= IE 9), suggesting they upgrade their browser. While this is intended to improve user experience and security, it also reveals information about the technologies and potentially targeted user base.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The comments section in the WebScraperRecon output contains the HTML comment '[if lte IE 9]>. You are using an outdated browser. Please upgrade your browser to improve your experience and security.</[endif]' for sarral.io and www.sarral.io.`

Remediation

Consider removing or updating the outdated browser warning to avoid revealing potentially sensitive information. Ensure the website is compatible with modern browsers and encourage users to use them.

Finding SAR-005: Open SSH (Low)

Description:	The SSH service is exposed on port 22. While not inherently a vulnerability, it increases the attack surface. Ensure strong password policies and consider limiting access to trusted networks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`PORT 22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.11`

Remediation

Ensure strong SSH password policies are in place. Consider using key-based authentication and limiting access to trusted networks.

Finding SAR-006: Unresolvable Subdomain (Info)

Description:	The subdomain www.pay.sarral.io is not resolving to an IP address. This could indicate a misconfiguration or an abandoned subdomain.
Risk:	Likelihood: Info Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The errors section in the WebScraperRecon output contains NameResolutionError for www.pay.sarral.io.`

Remediation

Investigate the DNS configuration for www.pay.sarral.io. If the subdomain is no longer in use, remove the DNS record to prevent potential confusion or future exploitation.

Finding SAR-007: Contact Information Exposure (Info)

Description:	The website exposes email addresses (Info@sarral.io, info@sarral.io) and phone numbers (303035 100) in its content. While this is standard practice, it can be used by attackers for phishing or 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 emails and phones sections in the WebScraperRecon output contain email addresses and phone numbers for sarral.io and www.sarral.io.`

Remediation

Consider using a contact form instead of directly exposing email addresses. Implement measures to prevent abuse of contact information, such as rate limiting and CAPTCHAs.