SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-082
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	3	4	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Configure the web server to send the following security headers: Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection.
SAR-002: Outdated Software	Medium	Upgrade Nginx to the latest stable version to patch any known security vulnerabilities.
SAR-003: Outdated Apache Version	Medium	Upgrade to the latest stable version of Apache to patch any known vulnerabilities. Monitor security advisories for Apache and apply patches promptly.
SAR-004: Exposed Phone Numbers	Low	Review the content of sophie.sarral.io and remove any unnecessary phone numbers. Ensure that any phone numbers that are displayed are done so intentionally and with appropriate context.
SAR-005: Exposed Social Media Profiles and Emails	Low	Review the website content and remove any unnecessary social media links or email addresses. Consider using a contact form instead of directly exposing email addresses.
SAR-006: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server.
SAR-007: Lack of Web Application Firewall	Low	Implement a Web Application Firewall (WAF) to protect against common web attacks. Configure the WAF to block malicious traffic and monitor for suspicious activity.
SAR-008: Unresponsive Subdomain	Info	Investigate the DNS configuration for www.pay.sarral.io to ensure it is properly configured. If the subdomain is no longer in use, consider removing the DNS record.
SAR-009: SSH Version Information Disclosure	Info	Consider disabling SSH version banner disclosure to reduce information leakage. This can be done by modifying the SSH server configuration.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The web server is not sending recommended security headers such as HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. These headers help protect against various attacks, including clickjacking, cross-site scripting (XSS), and MIME sniffing.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`The security_headers section in the WebScraperRecon output shows null values for hsts, x_frame_options, x_content_type_options, referrer_policy, permissions_policy and x_xss_protection for sarral.io and www.sarral.io.`

Remediation

Configure the web server to send the following security headers: Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and 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: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104
Evidence:	`The headers section in the WebScraperRecon output for sophie.sarral.io shows 'Server: nginx/1.18.0 (Ubuntu)'.`

Remediation

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

Finding SAR-003: Outdated Apache Version (Medium)

Description:	The server is running Apache version 2.4.58. This version may contain known vulnerabilities that could be exploited. Regularly updating software components is crucial for maintaining security.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09-Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`Apache[2.4.58]`

Remediation

Upgrade to the latest stable version of Apache to patch any known vulnerabilities. Monitor security advisories for Apache and apply patches promptly.

Finding SAR-004: Exposed Phone Numbers (Low)

Description:	The web scraper found a large number of phone numbers on the sophie.sarral.io subdomain. While not inherently critical, this information could be used for social engineering or other malicious purposes.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`The phones section 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 phone numbers. Ensure that any phone numbers that are displayed are done so intentionally and with appropriate context.

Finding SAR-005: Exposed Social Media Profiles and Emails (Low)

Description:	The web scraper found social media profiles and email addresses on the sarral.io and www.sarral.io domains. This information could be used for social engineering or phishing attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`The social_profiles and emails sections in the WebScraperRecon output for sarral.io and www.sarral.io contain lists of social media profiles and email addresses.`

Remediation

Review the website content and remove any unnecessary social media links or email addresses. Consider using a contact form instead of directly exposing email addresses.

Finding SAR-006: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on pay.sarral.io, sophie.sarral.io, sarral.io and www.sarral.io. This method can be used to potentially expose sensitive information, such as cookies, when combined with cross-site scripting (XSS) vulnerabilities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The http_methods section in the WebScraperRecon output for pay.sarral.io, sophie.sarral.io, sarral.io and www.sarral.io includes TRACE.`

Remediation

Disable the TRACE HTTP method on the web server.

Finding SAR-007: Lack of Web Application Firewall (Low)

Description:	No Web Application Firewall (WAF) was detected. A WAF can provide an additional layer of security by filtering malicious traffic and preventing common web attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06-Security Misconfiguration CWE: CWE-693
Evidence:	`No WAF detected by the generic detection`

Remediation

Implement a Web Application Firewall (WAF) to protect against common web attacks. Configure the WAF to block malicious traffic and monitor for suspicious activity.

Finding SAR-008: Unresponsive Subdomain (Info)

Description:	The subdomain www.pay.sarral.io failed to resolve during the scan. This could indicate a misconfiguration or an abandoned subdomain.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The errors section in the WebScraperRecon output for www.pay.sarral.io shows NameResolutionError.`

Remediation

Investigate the DNS configuration for www.pay.sarral.io to ensure it is properly configured. If the subdomain is no longer in use, consider removing the DNS record.

Finding SAR-009: SSH Version Information Disclosure (Info)

Description:	The SSH server version is disclosed as OpenSSH 9.6p1 Ubuntu 3ubuntu13.11. While not directly a vulnerability, this information can be used by attackers to identify potential exploits specific to this version.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06-Security Misconfiguration CWE: CWE-200
Evidence:	`OpenSSH 9.6p1 Ubuntu 3ubuntu13.11`

Remediation

Consider disabling SSH version banner disclosure to reduce information leakage. This can be done by modifying the SSH server configuration.
