SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-078
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	5	1
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 a strict CSP, set X-Frame-Options to 'sameorigin' or 'deny', enable X-Content-Type-Options, configure Ref...
SAR-002: Outdated Software	Medium	Upgrade Nginx to the latest stable version to patch any known vulnerabilities.
SAR-003: Outdated Apache Version	Medium	Upgrade to the latest stable version of Apache to patch known vulnerabilities. Regularly check for security updates and apply them promptly.
SAR-004: No Web Application Firewall Detected	Medium	Implement a Web Application Firewall (WAF) to protect the web application from common attacks. Configure the WAF with appropriate rules and regularly update the rules to address new threats.
SAR-005: Information Exposure - Phone Numbers	Low	Review the content of sophie.sarral.io and remove any unnecessary phone numbers. Ensure that any phone numbers that are present are not sensitive and are intended for public consumption.
SAR-006: Domain parked or not properly configured	Low	Verify the DNS configuration for www.pay.sarral.io and ensure that it is properly configured to point to a valid server. If the subdomain is not intended to be used, remove the DNS record to prevent c...
SAR-007: Information Exposure - Email Addresses	Low	Implement measures to protect the exposed email addresses from spam and phishing attacks, such as using a CAPTCHA on contact forms and obfuscating email addresses on the website.
SAR-008: HTTP TRACE Method Enabled	Low	Disable the HTTP TRACE method on the web server to prevent XST attacks.
SAR-009: OpenSSH Version Disclosure	Low	Consider disabling version disclosure in the SSH server configuration or upgrading to the latest stable version. Ensure the SSH server is configured securely, following best practices.
SAR-010: Deprecated Browser Support	Info	Consider removing support for extremely outdated browsers like IE9 to reduce the attack surface and simplify development efforts. If support is necessary, ensure that proper security measures are in p...

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The target 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 man-in-the-middle attacks, cross-site scripting (XSS), and clickjacking.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`Security headers are null in the WebScraperRecon output for sarral.io, www.sarral.io and pay.sarral.io.`

Remediation

Implement 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, configure Referrer-Policy, and set X-XSS-Protection to '1; mode=block'.

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 can be exploited by attackers.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104
Evidence:	`The WebScraperRecon output for sophie.sarral.io shows that it is running Nginx version 1.18.0.`

Remediation

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

Finding SAR-003: Outdated Apache Version (Medium)

Description:	The web server is running Apache version 2.4.58. Running outdated software can expose the system to known vulnerabilities. While this specific version may not have readily exploitable vulnerabilities, maintaining up-to-date software is a crucial security practice.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021-Vulnerable and Outdated Components CWE: CWE-1035
Evidence:	`Apache httpd 2.4.58`

Remediation

Upgrade to the latest stable version of Apache to patch known vulnerabilities. Regularly check for security updates and apply them promptly.

Finding SAR-004: No Web Application Firewall Detected (Medium)

Description:	The scan indicates that no Web Application Firewall (WAF) was detected. A WAF provides a layer of security to protect against common web application attacks such as SQL injection and cross-site scripting. Without a WAF, the application is more vulnerable to these types of attacks.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A04:2021-Insecure Design CWE: CWE-200
Evidence:	`No WAF detected by the generic detection`

Remediation

Implement a Web Application Firewall (WAF) to protect the web application from common attacks. Configure the WAF with appropriate rules and regularly update the rules to address new threats.

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

Description:	The sophie.sarral.io subdomain exposes a large number of phone numbers. While these may not be directly exploitable, they can 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 WebScraperRecon output for sophie.sarral.io contains a large number of phone numbers.`

Remediation

Review the content of sophie.sarral.io and remove any unnecessary phone numbers. Ensure that any phone numbers that are present are not sensitive and are intended for public consumption.

Finding SAR-006: Domain parked or not properly configured (Low)

Description:	The subdomain www.pay.sarral.io does not resolve properly and returns name resolution errors. This could indicate a misconfiguration or a parked domain.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`The WebScraperRecon output for www.pay.sarral.io contains name resolution errors.`

Remediation

Verify the DNS configuration for www.pay.sarral.io and ensure that it is properly configured to point to a valid server. If the subdomain is not intended to be used, remove the DNS record to prevent confusion.

Finding SAR-007: Information Exposure - Email Addresses (Low)

Description:	The main domain (sarral.io and www.sarral.io) exposes email addresses (Info@sarral.io, info@sarral.io). While these may not be directly exploitable, they can be used for spamming 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 WebScraperRecon output for sarral.io and www.sarral.io contains email addresses.`

Remediation

Implement measures to protect the exposed email addresses from spam and phishing attacks, such as using a CAPTCHA on contact forms and obfuscating email addresses on the website.

Finding SAR-008: HTTP TRACE Method Enabled (Low)

Description:	The HTTP TRACE method is enabled on pay.sarral.io and sophie.sarral.io. The TRACE method can be used to conduct cross-site tracing (XST) attacks, potentially exposing sensitive information.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The WebScraperRecon output for pay.sarral.io and sophie.sarral.io shows that the TRACE method is enabled.`

Remediation

Disable the HTTP TRACE method on the web server to prevent XST attacks.

Finding SAR-009: OpenSSH Version Disclosure (Low)

Description:	The SSH server version is disclosed as OpenSSH 9.6p1 Ubuntu 3ubuntu13.11. While not directly exploitable, disclosing the version allows attackers to target specific vulnerabilities known to exist in that version. This information can be used for fingerprinting and targeted attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021-Vulnerable and Outdated Components CWE: CWE-200
Evidence:	`OpenSSH 9.6p1 Ubuntu 3ubuntu13.11`

Remediation

Consider disabling version disclosure in the SSH server configuration or upgrading to the latest stable version. Ensure the SSH server is configured securely, following best practices.

Finding SAR-010: Deprecated Browser Support (Info)

Description:	The website includes a warning message for users with Internet Explorer 9 or older, suggesting they upgrade their browser. While not a direct vulnerability, supporting deprecated browsers can increase the attack surface due to their known security flaws.
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 WebScraperRecon output for sarral.io and www.sarral.io contains the outdated browser warning message.`

Remediation

Consider removing support for extremely outdated browsers like IE9 to reduce the attack surface and simplify development efforts. If support is necessary, ensure that proper security measures are in place to mitigate the risks associated with these browsers.