SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 29, 2025
Project: SAR-065
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 November 29, 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	2	4	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers on the web server. Specifically, configure HSTS to enforce HTTPS, CSP to restrict allowed sources for content, and X-Frame-Options to prevent clickjacking. Set X...
SAR-002: Outdated Nginx Version	Medium	Upgrade Nginx to the latest stable version to patch any known vulnerabilities. Regularly update the web server software to maintain security.
SAR-003: Exposed Phone Numbers	Low	Review the content of 'sophie.sarral.io' and remove any unnecessary or sensitive phone numbers. Ensure that any phone numbers displayed are intended for public use.
SAR-004: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server. This can typically be done in the server configuration file.
SAR-005: Non-Functional Subdomain	Low	Investigate the DNS configuration for 'www.pay.sarral.io'. Either correct the DNS records to point to a valid server or remove the subdomain if it is no longer in use.
SAR-006: 404 Response on Subdomain	Low	Investigate the server configuration for 'pay.sarral.io'. Either correct the configuration to serve the intended content or remove the subdomain if it is no longer in use.
SAR-007: WHOIS Privacy Enabled	Info	No direct remediation is needed. This is an informational finding. Consider the implications of using a privacy service for domain registration.
SAR-008: reCAPTCHA Presence	Info	No remediation is needed. This is an informational finding. Ensure that the reCAPTCHA implementation is correctly configured and regularly updated.

Copyright © Sarral Security

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The target domain 'sarral.io' and 'www.sarral.io' are missing critical security headers such as HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. This increases the risk of various attacks, including man-in-the-middle attacks, cross-site scripting (XSS), and clickjacking.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-16
Evidence:	`Security headers are null for sarral.io and www.sarral.io`

Remediation

Implement the missing security headers on the web server. Specifically, configure HSTS to enforce HTTPS, CSP to restrict allowed sources for content, and X-Frame-Options to prevent clickjacking. Set X-Content-Type-Options to 'nosniff' to prevent MIME sniffing, and configure a strict Referrer-Policy and Permissions-Policy.

Copyright © Sarral Security

Finding SAR-002: Outdated Nginx Version (Medium)

Description:	The subdomain 'sophie.sarral.io' is running an outdated version of Nginx (1.18.0). Older versions of Nginx may contain known vulnerabilities that could be exploited by attackers.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06-Vulnerable and Outdated Components CWE: CWE-1035
Evidence:	`Server: nginx/1.18.0 (Ubuntu) on sophie.sarral.io`

Remediation

Upgrade Nginx to the latest stable version to patch any known vulnerabilities. Regularly update the web server software to maintain security.

Copyright © Sarral Security

Finding SAR-003: Exposed Phone Numbers (Low)

Description:	The subdomain 'sophie.sarral.io' exposes a large number of phone numbers within its content. While the risk is low, 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-Broken Access Control CWE: CWE-200
Evidence:	`Multiple phone numbers found on sophie.sarral.io`

Remediation

Review the content of 'sophie.sarral.io' and remove any unnecessary or sensitive phone numbers. Ensure that any phone numbers displayed are intended for public use.

Copyright © Sarral Security

Finding SAR-004: TRACE Method Enabled (Low)

Description:	The HTTP TRACE method is enabled on 'sarral.io', 'www.sarral.io' and 'sophie.sarral.io'. TRACE can be used in cross-site tracing attacks to steal cookies. While modern browsers mitigate this risk, disabling TRACE is still recommended.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`HTTP Methods: TRACE`

Remediation

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

Copyright © Sarral Security

Finding SAR-005: Non-Functional Subdomain (Low)

Description:	The subdomain 'www.pay.sarral.io' does not resolve, resulting in a NameResolutionError. This could indicate a misconfiguration or an abandoned subdomain.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`HTTPSConnectionPool(host='www.pay.sarral.io', port=443): Max retries exceeded with url: / (Caused by NameResolutionError("<urllib3.connection.HTTPSConnection object at 0x7f061e61d590>: Failed to resolve 'www.pay.sarral.io' ([Errno -2] Name or service not known)"))`

Remediation

Investigate the DNS configuration for 'www.pay.sarral.io'. Either correct the DNS records to point to a valid server or remove the subdomain if it is no longer in use.

Copyright © Sarral Security

Finding SAR-006: 404 Response on Subdomain (Low)

Description:	The subdomain 'pay.sarral.io' returns a 404 Not Found error. This could indicate a misconfiguration or an abandoned subdomain.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`status_code: 404 on pay.sarral.io`

Remediation

Investigate the server configuration for 'pay.sarral.io'. Either correct the configuration to serve the intended content or remove the subdomain if it is no longer in use.

Copyright © Sarral Security

Finding SAR-007: WHOIS Privacy Enabled (Info)

Description:	The WHOIS record shows that the domain registrant information is hidden using a privacy service ('Domains By Proxy, LLC'). While this protects the registrant's personal information, it can hinder transparency and make it difficult to identify the domain owner.
Risk:	Likelihood: Info Impact: Info
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`Registrant Organization: Domains By Proxy, LLC in WHOIS record`

Remediation

No direct remediation is needed. This is an informational finding. Consider the implications of using a privacy service for domain registration.

Copyright © Sarral Security

Finding SAR-008: reCAPTCHA Presence (Info)

Description:	The presence of reCAPTCHA on the contact form indicates an attempt to prevent automated abuse and spam submissions. This is a positive security measure.
Risk:	Likelihood: Info Impact: Info
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-693
Evidence:	`<div class="g-recaptcha" data-sitekey="6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee"></div>`

Remediation

No remediation is needed. This is an informational finding. Ensure that the reCAPTCHA implementation is correctly configured and regularly updated.

Copyright © Sarral Security