SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 29, 2025
Project: SAR-068
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 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.

Vulnerability Summary & Report Card

0	0	1	3	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers on the web server. For example, configure HSTS to enforce HTTPS, CSP to restrict allowed sources of content, and X-Frame-Options to prevent clickjacking.
SAR-002: Unresolvable Subdomain	Low	Verify and correct the DNS records for 'www.pay.sarral.io' to ensure proper resolution.
SAR-003: Exposed reCAPTCHA Site Key	Low	Ensure that the reCAPTCHA site key is properly protected and not directly exposed in client-side code. Consider using server-side validation to prevent abuse.
SAR-004: HTTP TRACE Method Enabled	Low	Disable the HTTP TRACE method on the web server.
SAR-005: Personally Identifiable Information (PII) Exposure	Info	Review the content of 'sophie.sarral.io' and remove any unnecessary exposure of phone numbers.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The subdomains 'sophie.sarral.io', 'sarral.io' and 'www.sarral.io' are missing several security headers, including HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. These headers are crucial for mitigating various attacks such as Cross-Site Scripting (XSS), Clickjacking, and Man-in-the-Middle (MitM) attacks.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-693
Evidence:	`The security_headers sections for 'sophie.sarral.io', 'sarral.io' and 'www.sarral.io' show null or missing values for these headers.`

Remediation

Implement the missing security headers on the web server. For example, configure HSTS to enforce HTTPS, CSP to restrict allowed sources of content, and X-Frame-Options to prevent clickjacking.

Finding SAR-002: Unresolvable Subdomain (Low)

Description:	The subdomain 'www.pay.sarral.io' fails to resolve, indicating a potential DNS misconfiguration. This could lead to denial-of-service or prevent legitimate users from accessing the intended service.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09-Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`The errors section for 'www.pay.sarral.io' shows NameResolutionError.`

Remediation

Verify and correct the DNS records for 'www.pay.sarral.io' to ensure proper resolution.

Finding SAR-003: Exposed reCAPTCHA Site Key (Low)

Description:	The reCAPTCHA site key '6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee' is exposed in the HTML source code of 'sarral.io'. While not a direct vulnerability, it can be used by attackers for malicious purposes such as automated abuse of forms.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`The comments section of 'www.sarral.io' and 'sarral.io' contains the reCAPTCHA site key.`

Remediation

Ensure that the reCAPTCHA site key is properly protected and not directly exposed in client-side code. Consider using server-side validation to prevent abuse.

Finding SAR-004: HTTP TRACE Method Enabled (Low)

Description:	The HTTP TRACE method is enabled on 'pay.sarral.io', 'sophie.sarral.io', 'www.sarral.io' and 'sarral.io'. This method can be used to expose sensitive information, such as cookies, and can be leveraged in cross-site tracing (XST) attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`The http_methods section for 'pay.sarral.io', 'sophie.sarral.io', 'www.sarral.io' and 'sarral.io' includes TRACE.`

Remediation

Disable the HTTP TRACE method on the web server.

Finding SAR-005: Personally Identifiable Information (PII) Exposure (Info)

Description:	The web scraper identified phone numbers on 'sophie.sarral.io'. This may lead to potential privacy violations.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A03-Injection CWE: CWE-200
Evidence:	`The phones section of 'sophie.sarral.io' contains multiple phone numbers.`

Remediation

Review the content of 'sophie.sarral.io' and remove any unnecessary exposure of phone numbers.