SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 29, 2025
Project: SAR-062
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	2	6
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers with appropriate values. For example, enable HSTS to enforce HTTPS, set X-Frame-Options to prevent clickjacking, and configure X-Content-Type-Options to prevent ...
SAR-002: Exposed Phone Numbers	Low	Review the website's content and remove any unnecessary phone numbers. If phone numbers are required, consider obfuscating them or using a contact form instead.
SAR-003: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the server.
SAR-004: WHOIS Information Disclosure	Info	Consider using a WHOIS privacy service to mask personal information. Review the exposed information and assess the risk. Ensure compliance with data privacy regulations.
SAR-005: DNS Information Disclosure	Info	Implement DNS security best practices, such as limiting zone transfers and using DNSSEC. Regularly review DNS records to ensure accuracy and minimize exposure of sensitive information. Consider using ...
SAR-006: Subdomain Enumeration	Info	Review the purpose and security of each subdomain. Ensure all subdomains are properly secured and monitored. Remove any unnecessary or outdated subdomains.
SAR-007: Domain Enumeration	Info	Review the discovered domains and ensure that all are intended to be publicly accessible. Consider limiting information exposure where possible.
SAR-008: Subdomain Enumeration	Info	Review discovered subdomains for sensitive information or misconfigurations. Consider restricting access to internal subdomains.
SAR-009: TODO Comments	Info	Review the website's content and remove any TODO comments.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The application is missing several security headers, including HSTS, 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, clickjacking, and cross-site scripting.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16: Improper Neutralization of Input That Causes or Allows Generation of Code
Evidence:	`www.sarral.io, sarral.io, pay.sarral.io, sophie.sarral.io are missing security headers.`

Remediation

Implement the missing security headers with appropriate values. For example, enable HSTS to enforce HTTPS, set X-Frame-Options to prevent clickjacking, and configure X-Content-Type-Options to prevent MIME sniffing.

Finding SAR-002: Exposed Phone Numbers (Low)

Description:	The web scraper found several phone numbers embedded in the HTML source code. While not directly exploitable, this information could be used for social engineering or other malicious purposes.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`sophie.sarral.io contains multiple phone numbers.`

Remediation

Review the website's content and remove any unnecessary phone numbers. If phone numbers are required, consider obfuscating them or using a contact form instead.

Finding SAR-003: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on the server. This method can be used to conduct cross-site tracing (XST) attacks, which can lead to the disclosure of sensitive information, such as cookies.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`TRACE method is enabled on www.sarral.io, sarral.io, and pay.sarral.io.`

Remediation

Disable the TRACE HTTP method on the server.

Finding SAR-004: WHOIS Information Disclosure (Info)

Description:	WHOIS records contain publicly available information about the domain registrant, administrator, and technical contacts. While this information is intended to be public, it can be used for reconnaissance purposes by attackers. The level of detail exposed can vary depending on the registrar and privacy settings.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Whois
References:	OWASP: OWASP-API3:2023 - Excessive Data Exposure CWE: CWE-200
Evidence:	`Registrant Name: REDACTED Registrant Organization: Domains By Proxy, LLC Registrant Street: REDACTED Registrant City: REDACTED Registrant State/Province: Arizona Registrant Postal Code: REDACTED Registrant Country: US Registrant Phone: REDACTED Registrant Email: REDACTED`

Remediation

Consider using a WHOIS privacy service to mask personal information. Review the exposed information and assess the risk. Ensure compliance with data privacy regulations.

Finding SAR-005: DNS Information Disclosure (Info)

Description:	The DNS lookup reveals the IP address associated with the domain sarral.io. While this is standard DNS functionality, it provides attackers with basic information about the target's infrastructure. This information can be used for further reconnaissance and potential attacks.
Risk:	Likelihood: High Impact: Low
System:	sarral.io
Tools Used:	NSLookup
References:	OWASP: N/A CWE: CWE-200
Evidence:	`Name: sarral.io Address: 159.89.216.111`

Remediation

Implement DNS security best practices, such as limiting zone transfers and using DNSSEC. Regularly review DNS records to ensure accuracy and minimize exposure of sensitive information. Consider using a CDN or proxy to mask the origin server's IP address.

Finding SAR-006: Subdomain Enumeration (Info)

Description:	Subdomain enumeration reveals potential attack surface. While not directly a vulnerability, it provides attackers with more targets to probe for weaknesses. The identified subdomains include sophie.sarral.io, projectdiscovery.io, www.pay.sarral.io, www.sarral.io, and pay.sarral.io.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Subfinder
References:	OWASP: OWASP-NA CWE: CWE-200
Evidence:	`Discovered subdomains: sophie.sarral.io, projectdiscovery.io, www.pay.sarral.io, www.sarral.io, pay.sarral.io`

Remediation

Review the purpose and security of each subdomain. Ensure all subdomains are properly secured and monitored. Remove any unnecessary or outdated subdomains.

Finding SAR-007: Domain Enumeration (Info)

Description:	The following domain names associated with sarral.io were discovered: sophie.sarral.io, sarral.io, www.pay.sarral.io, www.sarral.io, pay.sarral.io. This information can be used by attackers for reconnaissance purposes.
Risk:	Likelihood: High Impact: Info
System:	sarral.io
Tools Used:	Amass Passive
References:	OWASP: OWASP-WSTG-INFO-05 CWE: CWE-200
Evidence:	`Discovered domains: sophie.sarral.io, sarral.io, www.pay.sarral.io, www.sarral.io, pay.sarral.io`

Remediation

Review the discovered domains and ensure that all are intended to be publicly accessible. Consider limiting information exposure where possible.

Finding SAR-008: Subdomain Enumeration (Info)

Description:	The following subdomains were discovered: sophie.sarral.io, sarral.io, www.pay.sarral.io, www.sarral.io, pay.sarral.io. Subdomain enumeration can reveal potential attack surfaces.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	Assetfinder
References:	OWASP: OWASP-WSTG-INFO-009 CWE: CWE-200
Evidence:	`sophie.sarral.io, sarral.io, www.pay.sarral.io, www.sarral.io, pay.sarral.io`

Remediation

Review discovered subdomains for sensitive information or misconfigurations. Consider restricting access to internal subdomains.

Finding SAR-009: TODO Comments (Info)

Description:	The web scraper found TODO comments in the HTML source code. These comments may indicate unfinished or incomplete features, which could potentially expose vulnerabilities or provide attackers with insights into the application's development process.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-546: Potential Dead Code
Evidence:	`pay.sarral.io contains TODO comments.`

Remediation

Review the website's content and remove any TODO comments.