SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 03, 2025
Project: SAR-108
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 03, 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	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Information Exposure	Medium	Consider using a contact form instead of directly exposing email addresses. Implement measures to protect against phishing and social engineering attacks.
SAR-002: Information Exposure	Low	Remove all TODO comments from production code before deployment.
SAR-003: Information Exposure	Low	Educate employees about the risks of social engineering and encourage them to limit the information they share publicly.
SAR-004: Application Endpoint Exposure	Low	Ensure that all application endpoints are properly configured and secured. Implement custom error pages to avoid exposing sensitive information.
SAR-005: Deprecated Technology	Info	Ensure the website is fully compatible with modern browsers and that all dependencies are up to date.
SAR-006: Name Resolution Error	Info	Verify DNS configuration for these subdomains. Remove DNS records if the subdomains are no longer in use.

Technical Findings

Finding SAR-001: Information Exposure (Medium)

Description:	The web scraper identified emails (Info@sarral.io, info@sarral.io) and a phone number (303035 100) on the sarral.io domain. This information can be used for phishing attacks or social engineering.
Risk:	Likelihood: Medium 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:	`Emails: Info@sarral.io, info@sarral.io Phones: 303035 100`

Remediation

Consider using a contact form instead of directly exposing email addresses. Implement measures to protect against phishing and social engineering attacks.

Finding SAR-002: Information Exposure (Low)

Description:	The web scraper identified TODO comments in the source code of pay.sarral.io. These comments may reveal internal development practices or unfinished features, which could be leveraged by attackers.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A03:2021 - Injection CWE: CWE-532 - Insertion of Sensitive Information into Log File
Evidence:	`"TODO: replace with variable/translation for this", "TODO: replace this with stylesheet from this repo", "TODO: replace with variable/translation for this", "TODO: replace with variable/translation for this"`

Remediation

Remove all TODO comments from production code before deployment.

Finding SAR-003: Information Exposure (Low)

Description:	The web scraper identified LinkedIn profiles of employees on the sarral.io domain. This information can be used for social engineering attacks.
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:	`https://www.linkedin.com/company/sarral,`
	`https://www.linkedin.com/in/bob-candelmo-b4a27bb/,`
	`https://www.linkedin.com/in/kal-sambhangi-datadigitalandrisk/,`
	`https://www.linkedin.com/in/mike-p-roth/,`
	`https://www.linkedin.com/in/pavansomepalli/,`
	`https://www.linkedin.com/in/rfink02/,`
	`https://www.linkedin.com/in/roopesh-kondrella-6118a8b/`

Remediation

Educate employees about the risks of social engineering and encourage them to limit the information they share publicly.

Finding SAR-004: Application Endpoint Exposure (Low)

Description:	The pay.sarral.io subdomain returns a 404 Not Found error. This could indicate an exposed application endpoint that is not properly configured or secured.
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:	`https://pay.sarral.io/ returns 404`

Remediation

Ensure that all application endpoints are properly configured and secured. Implement custom error pages to avoid exposing sensitive information.

Finding SAR-005: Deprecated Technology (Info)

Description:	The website displays an outdated browser warning for Internet Explorer 9 and below. While this is good practice, it also indicates that the website may not be fully optimized or tested for modern browsers, potentially leading to compatibility issues or security vulnerabilities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2017 - Security Misconfiguration CWE: CWE-1104 - Use of Unmaintained Third-Party Components
Evidence:	`[if lte IE 9]> <p class="browserupgrade"> You are using an <strong>outdated</strong> browser. Please <a href="https://browsehappy.com/">upgrade your browser</a> to improve your experience and security. </p> <![endif]`

Remediation

Ensure the website is fully compatible with modern browsers and that all dependencies are up to date.

Finding SAR-006: Name Resolution Error (Info)

Description:	The web scraper was unable to resolve www.pay.sarral.io and www.sophie.sarral.io. This could indicate DNS misconfiguration or that these subdomains are no longer active.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: N/A
Evidence:	`[probe] https://www.pay.sarral.io -> HTTPSConnectionPool(host='www.pay.sarral.io', port=443): Max retries exceeded with url: / (Caused by NameResolutionError("<urllib3.connection.HTTPSConnection object at 0x7f1fb63bdd10>: Failed to resolve 'www.pay.sarral.io' ([Errno -2] Name or service not known)"))`

Remediation

Verify DNS configuration for these subdomains. Remove DNS records if the subdomains are no longer in use.