SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-092
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	6	6	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers on the web server configuration. Specifically, configure HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection...
SAR-002: Outdated Apache Web Server	Medium	Upgrade to the latest stable version of Apache web server.
SAR-003: Open FTP, RTSP and PPTP Services	Medium	Disable any unnecessary services to reduce the attack surface. If these services are required, ensure they are properly configured and secured, using strong authentication and encryption where possibl...
SAR-004: Missing Security Headers	Medium	Implement the missing security headers. For example, configure HSTS to enforce HTTPS, CSP to restrict the sources of content, and X-Frame-Options to prevent clickjacking.
SAR-005: Name Resolution Error	Medium	Verify the DNS configuration for www.pay.sarral.io and ensure that it is correctly pointing to the appropriate server. Check DNS records and server availability.
SAR-006: Connection Refused	Medium	Verify the service is running on sophie.sarral.io and that the firewall is not blocking connections. Check server availability and application logs.
SAR-007: Internal Phone Number Exposure	Low	Remove the phone numbers from the publicly accessible website. Review the content and remove any sensitive information.
SAR-008: Outdated Browser Notice	Low	Update the website's codebase to use modern technologies and libraries. Remove the outdated browser notice.
SAR-009: TRACE method enabled	Low	Disable the TRACE HTTP method on the web server.
SAR-010: reCaptcha Site Key Exposed	Low	Ensure the reCaptcha site key is properly protected and not easily accessible in the HTML source code. Consider implementing server-side validation to prevent abuse.

SAR-011: Open SSH Service	Low	Ensure SSH is properly configured with strong authentication, consider using key-based authentication, and restrict access to trusted networks.
SAR-012: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server. This can typically be done by modifying the server's configuration file.
SAR-013: Domain uses Privacy Protection Service	Info	No remediation is necessary. This is informational.
SAR-014: Subdomain does not resolve	Info	Check DNS configuration for www.pay.sarral.io. Remove the subdomain if it is no longer in use.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The main domain (sarral.io and www.sarral.io) and pay.sarral.io are missing several security headers, including HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. This makes the website vulnerable to various attacks, such as man-in-the-middle attacks, clickjacking, and cross-site scripting.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`Security headers are null for hsts, x_frame_options, x_content_type_options, referrer_policy, permissions_policy and x_xss_protection.`

Remediation

Implement the missing security headers on the web server configuration. Specifically, configure HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection headers.

Finding SAR-002: Outdated Apache Web Server (Medium)

Description:	The server is running Apache version 2.4.58. While not immediately vulnerable, running the latest version ensures that all known security patches are applied. Older versions may contain exploitable vulnerabilities.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	WhatWeb
References:	OWASP: A09-Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`Apache[2.4.58]`

Remediation

Upgrade to the latest stable version of Apache web server.

Finding SAR-003: Open FTP, RTSP and PPTP Services (Medium)

Description:	The scan identified open ports for FTP (21), RTSP (554) and PPTP (1723). These services may not be necessary and could present potential attack vectors if not properly secured or if they contain vulnerabilities. PPTP is considered insecure.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A01-Broken Access Control CWE: CWE-200
Evidence:	`21/tcp open ftp? 554/tcp open rtsp? 1723/tcp open pptp?`

Remediation

Disable any unnecessary services to reduce the attack surface. If these services are required, ensure they are properly configured and secured, using strong authentication and encryption where possible. Consider alternatives to PPTP.

Finding SAR-004: 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 cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks. Their absence increases the application's vulnerability to these types of exploits.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A07:2021 - Identification and Authentication Failures CWE: CWE-16: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Evidence:	`www.sarral.io, sophie.sarral.io, and pay.sarral.io are missing several security headers.`

Remediation

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

Finding SAR-005: Name Resolution Error (Medium)

Description:	The subdomain www.pay.sarral.io is failing to resolve, indicating a potential DNS configuration issue. This can lead to denial of service for users trying to access the subdomain.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-20: Improper Input Validation
Evidence:	`www.pay.sarral.io fails to resolve.`

Remediation

Verify the DNS configuration for www.pay.sarral.io and ensure that it is correctly pointing to the appropriate server. Check DNS records and server availability.

Finding SAR-006: Connection Refused (Medium)

Description:	The subdomain sophie.sarral.io is refusing connections, indicating a potential service outage or misconfiguration. This can lead to denial of service for users trying to access the subdomain.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-20: Improper Input Validation
Evidence:	`sophie.sarral.io is refusing connections.`

Remediation

Verify the service is running on sophie.sarral.io and that the firewall is not blocking connections. Check server availability and application logs.

Finding SAR-007: Internal Phone Number Exposure (Low)

Description:	The subdomain sophie.sarral.io exposes multiple internal phone numbers. This information could 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
Evidence:	`Multiple phone numbers are listed in the phones array for sophie.sarral.io.`

Remediation

Remove the phone numbers from the publicly accessible website. Review the content and remove any sensitive information.

Finding SAR-008: Outdated Browser Notice (Low)

Description:	The website includes a notice suggesting users upgrade their browser if they are using Internet Explorer 9 or earlier. This indicates the website may be using outdated technologies or libraries that could contain vulnerabilities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-937
Evidence:	`The comment section contains the string '[if lte IE 9]>'.`

Remediation

Update the website's codebase to use modern technologies and libraries. Remove the outdated browser notice.

Finding SAR-009: TRACE method enabled (Low)

Description:	The TRACE HTTP method is enabled on sarral.io, www.sarral.io and pay.sarral.io. This method can be used in cross-site tracing attacks to steal cookies.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The http_methods array contains TRACE.`

Remediation

Disable the TRACE HTTP method on the web server.

Finding SAR-010: reCaptcha Site Key Exposed (Low)

Description:	The reCaptcha site key is exposed in the HTML source code of the contact-us page. While not directly exploitable, it can be used by attackers to exhaust reCaptcha credits or perform other malicious activities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`<div class="g-recaptcha" data-sitekey="6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee"></div>`

Remediation

Ensure the reCaptcha site key is properly protected and not easily accessible in the HTML source code. Consider implementing server-side validation to prevent abuse.

Finding SAR-011: Open SSH Service (Low)

Description:	The scan identified an open SSH port (22) running OpenSSH 9.6p1. While SSH is generally secure, exposing it to the internet increases the risk of brute-force attacks and exploitation of potential vulnerabilities. Ensure SSH is properly configured with strong authentication and consider using key-based authentication.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)`

Remediation

Ensure SSH is properly configured with strong authentication, consider using key-based authentication, and restrict access to trusted networks.

Finding SAR-012: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on the server. This method can be used by attackers to steal cookies or other sensitive information via cross-site tracing (XST) attacks, especially when combined with cross-site scripting (XSS) vulnerabilities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`The TRACE method is enabled on www.sarral.io and sophie.sarral.io.`

Remediation

Disable the TRACE HTTP method on the web server. This can typically be done by modifying the server's configuration file.

Finding SAR-013: Domain uses Privacy Protection Service (Info)

Description:	The domain uses Domains By Proxy, LLC to hide registrant information. This is a common practice, but it can hinder identifying the true owner of the domain.
Risk:	Likelihood: Info Impact: Info
System:	sarral.io
Tools Used:	Whois
References:	OWASP: N/A CWE: N/A
Evidence:	`Registrant Organization: Domains By Proxy, LLC`

Remediation

No remediation is necessary. This is informational.

Finding SAR-014: Subdomain does not resolve (Info)

Description:	The subdomain www.pay.sarral.io does not resolve to an IP address. This could indicate a misconfiguration or an abandoned subdomain.
Risk:	Likelihood: Info Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: N/A
Evidence:	`The errors array contains 'Failed to resolve 'www.pay.sarral.io''.`

Remediation

Check DNS configuration for www.pay.sarral.io. Remove the subdomain if it is no longer in use.