SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 02, 2025
Project: SAR-097
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 02, 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	1	5	6	5
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Exposed Administrative Interfaces	High	Rename or relocate administrative directories to non-predictable names. Implement strong authentication and authorization mechanisms for all administrative interfaces. Ensure that administrative inter...
SAR-002: Missing Security Headers	Medium	Implement the following security headers: HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection.
SAR-003: Outdated Software	Medium	Upgrade Nginx to the latest stable version to patch any known vulnerabilities.
SAR-004: Outdated Apache Web Server	Medium	Upgrade the Apache web server to the latest stable version. Monitor security advisories for Apache and apply patches promptly.
SAR-005: Missing HTTP Strict Transport Security (HSTS) Header	Medium	Implement HSTS on the server with a reasonable max-age and includeSubDomains directive.
SAR-006: Sensitive Information Exposure via Fuzzing	Medium	Implement proper access controls to restrict access to sensitive files and directories. Remove unnecessary backup files and version control directories from the web server. Ensure that administrative ...
SAR-007: Information Disclosure - Phone Numbers	Low	Review the content of sophie.sarral.io and remove any sensitive information, including phone numbers, that are not intended for public disclosure.
SAR-008: Email Address Exposure	Low	Consider using an email obfuscation technique or a contact form to reduce the exposure of email addresses.
SAR-009: Open FTP, RTSP, and PPTP Ports	Low	Review the necessity of FTP, RTSP, and PPTP services. If not required, disable them and close the corresponding ports. If required, ensure they are properly secured and patched.
SAR-010: Publicly Accessible Email Addresses	Low	Consider obfuscating email addresses or using a contact form to reduce exposure to bots and malicious actors.

SAR-011: Web Server and Technology Disclosure	Low	Remove version information from server headers and keep software up to date.
SAR-012: TRACE method enabled	Low	Disable the TRACE method on the web server.
SAR-013: Subdomain Enumeration	Info	Review and document all subdomains. Ensure all subdomains are properly secured and monitored. Remove unused subdomains.
SAR-014: Unresponsive Subdomain	Info	Investigate the purpose of www.pay.sarral.io. If no longer needed, remove the DNS record. If required, correct the DNS configuration.
SAR-015: Contact Form reCaptcha	Info	Ensure reCaptcha is properly configured and monitored for abuse. Consider implementing additional anti-spam measures.
SAR-016: reCAPTCHA Implementation	Info	Ensure reCAPTCHA is properly configured and regularly updated to prevent bypasses. Monitor for suspicious activity.
SAR-017: Exposed Social Media Profiles	Info	Review the exposed social media profiles and ensure that the information shared does not create an unnecessary risk.

Technical Findings

Finding SAR-001: Exposed Administrative Interfaces (High)

Description:	The web server exposes potential administrative interfaces through predictable directory names. If these interfaces are not properly secured, attackers could gain unauthorized access to administrative functionalities, potentially leading to complete system compromise.
Risk:	Likelihood: Low Impact: High
System:	sarral.io
Tools Used:	FFUF
References:	OWASP: A01-Broken Access Control CWE: CWE-284
Evidence:	`admin, Admin, ADM, ADMIN, admin.cgi, admin.pl, admin.php, admin_, admin_area, admin_banner, admin_c, admin_index, admin_interface, admin_login, admin_logon, admin1, admin2, admin3, admin4_account, admin4_colon, admin-console, admin-admin, admincp, admin-interface, admincontrol, adminhelp, administer, administr8, administrat, administracion, administratie, administrador, administration, administrator, Administration, administratoraccounts, administrators, administrivia, adminlogin, adminlogon, adminpanel, adminpro, admins, adminsessions, AdminService, adminsql, admintools, AdminTools`

Remediation

Rename or relocate administrative directories to non-predictable names. Implement strong authentication and authorization mechanisms for all administrative interfaces. Ensure that administrative interfaces are not accessible from the public internet.

Finding SAR-002: Missing Security Headers (Medium)

Description:	The subdomain pay.sarral.io is missing several security headers, including HSTS, 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, clickjacking, and cross-site scripting.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`WebScraperRecon shows null values for security headers in pay.sarral.io.`

Remediation

Implement the following security headers: HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection.

Finding SAR-003: Outdated Software (Medium)

Description:	The subdomain sophie.sarral.io is running an outdated version of Nginx (1.18.0). This version may contain known vulnerabilities that could be exploited by attackers.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104
Evidence:	`WebScraperRecon identifies Nginx version 1.18.0 on sophie.sarral.io.`

Remediation

Upgrade Nginx to the latest stable version to patch any known vulnerabilities.

Finding SAR-004: Outdated Apache Web Server (Medium)

Description:	The Apache web server is running version 2.4.58. While not immediately vulnerable, running an outdated version of web server software can expose the system to known vulnerabilities that have been patched in newer releases. Regularly updating the web server software is crucial for maintaining security.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WhatWeb
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1035 - Use of a Potentially Vulnerable Component
Evidence:	`Apache[2.4.58]`

Remediation

Upgrade the Apache web server to the latest stable version. Monitor security advisories for Apache and apply patches promptly.

Finding SAR-005: Missing HTTP Strict Transport Security (HSTS) Header (Medium)

Description:	The HSTS header is missing on pay.sarral.io. This allows man-in-the-middle attacks to downgrade the connection to HTTP, potentially exposing sensitive information.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-614 - Sensitive Cookie in HTTP Cookie Without 'Secure' Attribute
Evidence:	`security_headers: { "hsts": null`

Remediation

Implement HSTS on the server with a reasonable max-age and includeSubDomains directive.

Finding SAR-006: Sensitive Information Exposure via Fuzzing (Medium)

Description:	The web server exposes various files and directories that could contain sensitive information. These include backup files, configuration files, version control directories (like .svn and .git), and common administrative paths. Accessing these resources may reveal sensitive data such as database credentials, API keys, internal paths, or source code.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	FFUF
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`.listing, .htpasswd, .htaccess, .bash_history, .bashrc, .mysql_history, .listings, .config, .perf, .profile, .passwd, .cvs, .sh_history, .cache, .cvsignore, .history, .ssh, .rhosts, .subversion, .git/HEAD, .hta, .forward, .svn/entries, .svn, .web`

Remediation

Implement proper access controls to restrict access to sensitive files and directories. Remove unnecessary backup files and version control directories from the web server. Ensure that administrative interfaces are properly secured and not publicly accessible. Review server configuration to prevent information leakage.

Finding SAR-007: Information Disclosure - Phone Numbers (Low)

Description:	The subdomain sophie.sarral.io exposes multiple phone numbers, which 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
Evidence:	`WebScraperRecon identified multiple phone numbers on sophie.sarral.io.`

Remediation

Review the content of sophie.sarral.io and remove any sensitive information, including phone numbers, that are not intended for public disclosure.

Finding SAR-008: Email Address Exposure (Low)

Description:	Email addresses (Info@sarral.io, info@sarral.io) are exposed on the sarral.io website, which could be targeted for spam or phishing attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: CWE-200
Evidence:	`WebScraperRecon identified email addresses on sarral.io.`

Remediation

Consider using an email obfuscation technique or a contact form to reduce the exposure of email addresses.

Finding SAR-009: Open FTP, RTSP, and PPTP Ports (Low)

Description:	The scan identified open ports for FTP (21), RTSP (554), and PPTP (1723). These services may not be necessary and can increase the attack surface. Leaving unused ports open can provide potential entry points for attackers.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`21/tcp open ftp? 554/tcp open rtsp? 1723/tcp open pptp?`

Remediation

Review the necessity of FTP, RTSP, and PPTP services. If not required, disable them and close the corresponding ports. If required, ensure they are properly secured and patched.

Finding SAR-010: Publicly Accessible Email Addresses (Low)

Description:	Email addresses (Info@sarral.io, info@sarral.io) are exposed on www.sarral.io. This can lead to spam and potential phishing attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`emails: [ "Info@sarral.io", "info@sarral.io" ]`

Remediation

Consider obfuscating email addresses or using a contact form to reduce exposure to bots and malicious actors.

Finding SAR-011: Web Server and Technology Disclosure (Low)

Description:	The web server (Nginx 1.18.0) and technologies (React) used by sophie.sarral.io are disclosed in the headers and content. This information can be used by attackers to target known vulnerabilities in these specific versions.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`Server: nginx/1.18.0 (Ubuntu)`

Remediation

Remove version information from server headers and keep software up to date.

Finding SAR-012: TRACE method enabled (Low)

Description:	The HTTP TRACE method is enabled on pay.sarral.io and sophie.sarral.io. This method can be used to potentially expose sensitive information, such as cookies, when combined with other vulnerabilities like XSS.
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:	`"http_methods": [ "", "TRACE" ]`

Remediation

Disable the TRACE method on the web server.

Finding SAR-013: Subdomain Enumeration (Info)

Description:	Multiple subdomains were identified, which could expand the attack surface. These include www.pay.sarral.io, pay.sarral.io, www.sarral.io, and sophie.sarral.io. Discovery of subdomains allows attackers to target specific systems or services.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Subfinder (Passive), Amass Passive, Assetfinder
References:	OWASP: OWASP-OTG-INFO-002 CWE: CWE-200
Evidence:	`Subfinder (Passive), Amass Passive, and Assetfinder identified multiple subdomains.`

Remediation

Review and document all subdomains. Ensure all subdomains are properly secured and monitored. Remove unused subdomains.

Finding SAR-014: Unresponsive Subdomain (Info)

Description:	The subdomain www.pay.sarral.io is not resolving, indicating a potential misconfiguration or abandoned service. This could lead to confusion or be exploited by attackers registering a similar domain.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: OWASP-OTG-INFO-009 CWE: CWE-200
Evidence:	`WebScraperRecon reports NameResolutionError for www.pay.sarral.io.`

Remediation

Investigate the purpose of www.pay.sarral.io. If no longer needed, remove the DNS record. If required, correct the DNS configuration.

Finding SAR-015: Contact Form reCaptcha (Info)

Description:	The contact form on sarral.io uses reCaptcha, which helps prevent automated spam submissions. However, the presence of reCaptcha also indicates a potential target for bypassing or exploiting the captcha mechanism.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: N/A
Evidence:	`WebScraperRecon identified reCaptcha implementation on sarral.io.`

Remediation

Ensure reCaptcha is properly configured and monitored for abuse. Consider implementing additional anti-spam measures.

Finding SAR-016: reCAPTCHA Implementation (Info)

Description:	The presence of reCAPTCHA on www.sarral.io/contact-us indicates an attempt to prevent automated abuse. However, improper configuration or vulnerabilities in the implementation could lead to bypasses or other issues.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-693: Protection Mechanism Failure
Evidence:	`<div class="g-recaptcha" data-sitekey="6LfwfTgrAAAAAIVUfz-z7wSuXUOx0l5_Csfqsaee"></div>`

Remediation

Ensure reCAPTCHA is properly configured and regularly updated to prevent bypasses. Monitor for suspicious activity.

Finding SAR-017: Exposed Social Media Profiles (Info)

Description:	Social media profiles are exposed on www.sarral.io. This information can be used for social engineering attacks.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`https://www.linkedin.com/company/sarral`

Remediation

Review the exposed social media profiles and ensure that the information shared does not create an unnecessary risk.