SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-093
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	7	3	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Configure the web server to send the missing security headers. For example, add the following to the Apache configuration: Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; pr...
SAR-002: Unresponsive Subdomain	Medium	Investigate the DNS configuration and server status for www.pay.sarral.io to ensure it is properly configured and responsive. If the subdomain is no longer needed, remove the DNS record.
SAR-003: Outdated Apache Version	Medium	Upgrade Apache to the latest stable version to patch any known vulnerabilities. Monitor security advisories for Apache and apply patches promptly.
SAR-004: Potentially Unsecured Services	Medium	Investigate the necessity of running FTP, RTSP, and PPTP services. If not required, disable them. If required, ensure they are configured securely with strong authentication, encryption, and access co...
SAR-005: Lack of Web Application Firewall	Medium	Implement a Web Application Firewall (WAF) to protect against common web application attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Configure the WAF...
SAR-006: Missing Security Headers	Medium	Implement the missing security headers with appropriate configurations. For example, enable HSTS to enforce HTTPS, configure CSP to restrict the sources of content, and set X-Frame-Options to prevent ...
SAR-007: Outdated Nginx Version	Medium	Upgrade Nginx to the latest stable version to patch known vulnerabilities and improve security.
SAR-008: Domain Privacy Not Fully Effective	Low	Ensure WHOIS privacy settings are maximized and consider using a registrar that offers more comprehensive privacy options.
SAR-009: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server. This can typically be done by configuring the server to not accept TRACE requests.

SAR-010: Outdated Browser Warning	Low	Consider removing support for extremely outdated browsers or provide a more prominent and persistent upgrade recommendation.
SAR-011: Subdomain Enumeration	Info	Regularly review and monitor subdomains to ensure they are authorized and properly secured. Remove any unused or forgotten subdomains.
SAR-012: Publicly Accessible Email Addresses	Info	Consider obfuscating or hiding email addresses to reduce the risk of spam and phishing.

Technical Findings

Finding SAR-001: Missing Security Headers (Medium)

Description:	The web server is not sending 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.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16
Evidence:	`www.sarral.io, sarral.io, and sophie.sarral.io are missing security headers`

Remediation

Configure the web server to send the missing security headers. For example, add the following to the Apache configuration: Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload", Header set X-Frame-Options "SAMEORIGIN", Header set X-Content-Type-Options "nosniff", Header set Referrer-Policy "strict-origin-when-cross-origin", Header set X-XSS-Protection "1; mode=block", and configure CSP appropriately.

Finding SAR-002: Unresponsive Subdomain (Medium)

Description:	The subdomain www.pay.sarral.io is not resolving correctly, indicating a potential misconfiguration or service outage. This could lead to denial of service or other availability issues.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-200
Evidence:	`NameResolutionError for www.pay.sarral.io`

Remediation

Investigate the DNS configuration and server status for www.pay.sarral.io to ensure it is properly configured and responsive. If the subdomain is no longer needed, remove the DNS record.

Finding SAR-003: Outdated Apache Version (Medium)

Description:	The server is running Apache version 2.4.58. While not immediately vulnerable, older versions may contain known security vulnerabilities that have been patched in more recent 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 Apache to the latest stable version to patch any known vulnerabilities. Monitor security advisories for Apache and apply patches promptly.

Finding SAR-004: Potentially Unsecured Services (Medium)

Description:	The scan identified open ports for FTP (21), RTSP (554), and PPTP (1723). These services, if enabled, may be vulnerable to various attacks, especially if using default configurations or weak authentication mechanisms. PPTP is considered obsolete and highly insecure.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-266 - Incorrect Privilege Assignment
Evidence:	`21/tcp open ftp? 554/tcp open rtsp? 1723/tcp open pptp?`

Remediation

Investigate the necessity of running FTP, RTSP, and PPTP services. If not required, disable them. If required, ensure they are configured securely with strong authentication, encryption, and access controls. Consider replacing PPTP with a more secure VPN solution.

Finding SAR-005: Lack of Web Application Firewall (Medium)

Description:	The scan did not detect a Web Application Firewall (WAF) in front of the web server. A WAF provides an additional layer of security by filtering malicious traffic and protecting against common web application attacks.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	WafW00f
References:	OWASP: A04:2021 - Insecure Design CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`No WAF detected by the generic detection`

Remediation

Implement a Web Application Firewall (WAF) to protect against common web application attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Configure the WAF with appropriate rules and regularly update them to address new threats.

Finding SAR-006: Missing Security Headers (Medium)

Description:	The application 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 common web attacks such as cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	DNS Resolver
References:	OWASP: A07:2021 - Identification and Authentication Failures CWE: CWE-16
Evidence:	`pay.sarral.io, sophie.sarral.io and www.sarral.io are missing security headers.`

Remediation

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

Finding SAR-007: Outdated Nginx Version (Medium)

Description:	The server is running an outdated version of Nginx (1.18.0). Older versions may contain known vulnerabilities that could be exploited.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1188
Evidence:	`sophie.sarral.io is running Nginx 1.18.0.`

Remediation

Upgrade Nginx to the latest stable version to patch known vulnerabilities and improve security.

Finding SAR-008: Domain Privacy Not Fully Effective (Low)

Description:	While the domain uses a privacy service (Domains By Proxy, LLC), the registrar (GoDaddy) and other domain details are still exposed in the WHOIS record. This information can be used for social engineering or other reconnaissance activities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Whois
References:	OWASP: N/A CWE: CWE-200
Evidence:	`WHOIS record reveals registrar and other domain details despite using a privacy service.`

Remediation

Ensure WHOIS privacy settings are maximized and consider using a registrar that offers more comprehensive privacy options.

Finding SAR-009: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on the server. This method can be used to expose sensitive information, such as cookies, when combined with cross-site scripting (XSS) attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`The TRACE method is enabled on pay.sarral.io and www.sarral.io.`

Remediation

Disable the TRACE HTTP method on the web server. This can typically be done by configuring the server to not accept TRACE requests.

Finding SAR-010: Outdated Browser Warning (Low)

Description:	The website displays a warning message suggesting users upgrade their browser if they are using Internet Explorer 9 or older. Supporting outdated browsers can introduce security vulnerabilities.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-937
Evidence:	`www.sarral.io displays a browser upgrade warning for IE9 and older.`

Remediation

Consider removing support for extremely outdated browsers or provide a more prominent and persistent upgrade recommendation.

Finding SAR-011: Subdomain Enumeration (Info)

Description:	Multiple tools identified several subdomains for the target domain. While not a direct vulnerability, subdomain enumeration can expand the attack surface and provide potential entry points for attackers.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Subfinder (Passive), Amass Passive, Assetfinder
References:	OWASP: N/A CWE: CWE-200
Evidence:	`Identified subdomains: www.sarral.io, www.pay.sarral.io, sophie.sarral.io, pay.sarral.io`

Remediation

Regularly review and monitor subdomains to ensure they are authorized and properly secured. Remove any unused or forgotten subdomains.

Finding SAR-012: Publicly Accessible Email Addresses (Info)

Description:	Email addresses (Info@sarral.io, info@sarral.io) are publicly exposed on the website. This can lead to spam and potential phishing attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`Email addresses found on www.sarral.io.`

Remediation

Consider obfuscating or hiding email addresses to reduce the risk of spam and phishing.