SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 02, 2025
Project: SAR-106
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	0	3	6	3
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing HTTP Strict Transport Security (HSTS) Header	Medium	Configure the web server to include the HSTS header in its responses. The header should include a max-age directive to specify the duration for which the browser should remember to only access the sit...
SAR-002: Missing Security Headers	Medium	Configure the web server to include these security headers in its responses. Set X-Frame-Options to 'DENY' or 'SAMEORIGIN' to prevent clickjacking. Set X-Content-Type-Options to 'nosniff' to prevent M...
SAR-003: Outdated Software Component	Medium	Upgrade Apache httpd to the latest stable version. Monitor security advisories for any identified vulnerabilities in the current version.
SAR-004: Information Disclosure - Email Addresses	Low	Consider using a contact form instead of directly exposing email addresses on the website. Implement measures to prevent email harvesting, such as CAPTCHAs or rate limiting.
SAR-005: Information Disclosure - Phone Numbers	Low	Review the necessity of displaying all phone numbers on the website. Consider using a contact form instead of directly exposing phone numbers. Implement measures to prevent phone number harvesting.
SAR-006: Outdated Browser Warning	Low	Ensure that the website is regularly updated to use modern web technologies and that support for outdated browsers is phased out. Encourage users to upgrade their browsers to the latest versions for i...
SAR-007: 404 Not Found Error	Low	Investigate the cause of the 404 error on pay.sarral.io. Ensure that the subdomain is properly configured and that all links are valid. Implement custom error pages to provide a better user experience...

SAR-008: Name Resolution Errors	Low	Verify the DNS records for www.pay.sarral.io and www.sophie.sarral.io to ensure they are correctly configured and pointing to the appropriate IP addresses. Ensure that the DNS servers are properly con...
SAR-009: No Web Application Firewall Detected	Low	Implement a web application firewall (WAF) to protect against common web application attacks. Configure the WAF with appropriate rules and policies to filter malicious traffic.
SAR-010: Information Disclosure - Social Media Profiles	Info	Review the necessity of linking to employee profiles on the website. Educate employees about the risks of social engineering and how to protect their personal information online.
SAR-011: Domain Privacy	Info	No remediation is necessary. This is a privacy measure.
SAR-012: Information Disclosure: Software Version	Info	Configure the web server to suppress the display of software versions in HTTP headers and server responses. Consider using a reverse proxy to further obfuscate the backend server information.

Technical Findings

Finding SAR-001: Missing HTTP Strict Transport Security (HSTS) Header (Medium)

Description:	The HTTP Strict Transport Security (HSTS) header is missing on pay.sarral.io. HSTS is a web security policy mechanism that helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows a web server to inform web browsers that it should only be accessed using HTTPS, instead of using HTTP. This can help prevent man-in-the-middle attacks.
Risk:	Likelihood: High Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-614 - Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
Evidence:	`Security headers for pay.sarral.io show hsts: null`

Remediation

Configure the web server to include the HSTS header in its responses. The header should include a max-age directive to specify the duration for which the browser should remember to only access the site over HTTPS. Consider including the includeSubDomains directive to apply the policy to all subdomains, and the preload directive to include the site in the HSTS preload list.

Finding SAR-002: Missing Security Headers (Medium)

Description:	The subdomains pay.sarral.io and sophie.sarral.io are missing several security headers, including X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protection. These headers provide protection against various client-side attacks, such as clickjacking, MIME sniffing attacks, and cross-site scripting (XSS).
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-16: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
Evidence:	`Security headers for pay.sarral.io and sophie.sarral.io show null values for multiple security headers.`

Remediation

Configure the web server to include these security headers in its responses. Set X-Frame-Options to 'DENY' or 'SAMEORIGIN' to prevent clickjacking. Set X-Content-Type-Options to 'nosniff' to prevent MIME sniffing attacks. Implement a Referrer-Policy to control how much information the browser includes with navigations away from the document. Use Permissions-Policy to allow or deny the use of browser features in the web application. Set X-XSS-Protection to '1; mode=block' to enable XSS filtering.

Finding SAR-003: Outdated Software Component (Medium)

Description:	The server is running Apache httpd 2.4.58. While not immediately vulnerable, outdated software may contain known vulnerabilities that could be exploited. Regular updates are crucial for maintaining security.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A09-Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`Apache httpd 2.4.58`

Remediation

Upgrade Apache httpd to the latest stable version. Monitor security advisories for any identified vulnerabilities in the current version.

Finding SAR-004: Information Disclosure - Email Addresses (Low)

Description:	Email addresses (Info@sarral.io, info@sarral.io) were found on the main domain sarral.io. This information can be used for phishing attacks or spam campaigns.
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:	`Email addresses found in the HTML source code of sarral.io.`

Remediation

Consider using a contact form instead of directly exposing email addresses on the website. Implement measures to prevent email harvesting, such as CAPTCHAs or rate limiting.

Finding SAR-005: Information Disclosure - Phone Numbers (Low)

Description:	Multiple phone numbers were found on sophie.sarral.io. This information can be used for unsolicited calls or social engineering attacks.
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:	`Phone numbers found in the HTML source code of sophie.sarral.io.`

Remediation

Review the necessity of displaying all phone numbers on the website. Consider using a contact form instead of directly exposing phone numbers. Implement measures to prevent phone number harvesting.

Finding SAR-006: Outdated Browser Warning (Low)

Description:	The website displays a warning message for users with outdated browsers (IE9 or earlier). While this is a good practice, it indicates that the website may still support or be compatible with older, potentially vulnerable browsers.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021-Vulnerable and Outdated Components CWE: CWE-937: Improperly Formatted Error Messages
Evidence:	`HTML comments containing conditional statements for IE9 and earlier.`

Remediation

Ensure that the website is regularly updated to use modern web technologies and that support for outdated browsers is phased out. Encourage users to upgrade their browsers to the latest versions for improved security and performance.

Finding SAR-007: 404 Not Found Error (Low)

Description:	The subdomain pay.sarral.io returns a 404 Not Found error. This could indicate a misconfiguration or a broken link, potentially leading to a negative user experience.
Risk:	Likelihood: High 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:	`HTTP probe of pay.sarral.io returns a 404 status code.`

Remediation

Investigate the cause of the 404 error on pay.sarral.io. Ensure that the subdomain is properly configured and that all links are valid. Implement custom error pages to provide a better user experience.

Finding SAR-008: Name Resolution Errors (Low)

Description:	The subdomains www.pay.sarral.io and www.sophie.sarral.io are not resolving, resulting in name resolution errors. This indicates a DNS configuration issue.
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:	`WebScraperRecon errors indicate "Failed to resolve 'www.pay.sarral.io'" and "Failed to resolve 'www.sophie.sarral.io'".`

Remediation

Verify the DNS records for www.pay.sarral.io and www.sophie.sarral.io to ensure they are correctly configured and pointing to the appropriate IP addresses. Ensure that the DNS servers are properly configured and responsive.

Finding SAR-009: No Web Application Firewall Detected (Low)

Description:	A web application firewall (WAF) was not detected. WAFs provide an additional layer of security by filtering malicious traffic and protecting against common web application attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WafW00f
References:	OWASP: A06-Vulnerable and Outdated Components CWE: CWE-200
Evidence:	`No WAF detected by the generic detection`

Remediation

Implement a web application firewall (WAF) to protect against common web application attacks. Configure the WAF with appropriate rules and policies to filter malicious traffic.

Finding SAR-010: Information Disclosure - Social Media Profiles (Info)

Description:	LinkedIn profiles of employees were found on sarral.io. 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:	`LinkedIn profiles found in the HTML source code of sarral.io.`

Remediation

Review the necessity of linking to employee profiles on the website. Educate employees about the risks of social engineering and how to protect their personal information online.

Finding SAR-011: Domain Privacy (Info)

Description:	The WHOIS record shows that the domain sarral.io is registered through GoDaddy and uses Domains By Proxy, LLC. This service obscures the registrant's contact information, making it more difficult to identify the owner of the domain.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	Whois
References:	OWASP: N/A CWE: N/A
Evidence:	`WHOIS record shows Registrant Organization: Domains By Proxy, LLC`

Remediation

No remediation is necessary. This is a privacy measure.

Finding SAR-012: Information Disclosure: Software Version (Info)

Description:	The server is exposing the version of Apache and Ubuntu Linux. While not a direct vulnerability, this information can be used by attackers to target specific vulnerabilities associated with these versions.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WhatWeb
References:	OWASP: A05-Security Misconfiguration CWE: CWE-200
Evidence:	`HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)]`

Remediation

Configure the web server to suppress the display of software versions in HTTP headers and server responses. Consider using a reverse proxy to further obfuscate the backend server information.
