SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 02, 2025
Project: SAR-102
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	7	9	5
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Exposed Administrative Interfaces	High	Ensure that all administrative interfaces are protected by strong authentication mechanisms, such as multi-factor authentication. Regularly audit access logs to detect and prevent unauthorized access ...
SAR-002: DNS Resolution Error	Medium	Verify and correct the DNS records for the affected subdomain to ensure proper resolution.
SAR-003: Missing HSTS Header	Medium	Implement the HSTS header on the pay.sarral.io subdomain to enforce HTTPS connections.
SAR-004: Potential Vulnerability in Contact Form	Medium	Review and secure the send_mail.php script to prevent abuse or injection attacks. Implement proper input validation and sanitization.
SAR-005: 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 access the site via...
SAR-006: Exposure of API Endpoints	Medium	Implement proper authentication and authorization mechanisms for all API endpoints. Regularly audit and test API security to prevent vulnerabilities.
SAR-007: Outdated Apache Version	Medium	Upgrade to the latest stable version of Apache. Regularly apply security patches to prevent exploitation of known vulnerabilities.
SAR-008: Sensitive Information Disclosure	Medium	Restrict access to sensitive directories and files by configuring appropriate permissions and access controls. Ensure that backup files are stored securely and are not accessible to unauthorized users...
SAR-009: Information Disclosure - Server Version	Low	Disable the server version display in the HTTP headers.
SAR-010: Information Disclosure - Phone Numbers	Low	Review and remove any unnecessary phone numbers from the publicly accessible website.

SAR-011: Information Disclosure - Email Addresses	Low	Implement measures to protect email addresses from being harvested, such as using obfuscation techniques or a contact form.
SAR-012: Unnecessary HTTP methods enabled	Low	Disable the HTTP TRACE method on the server.
SAR-013: Exposure of Internal Phone Numbers	Low	Review the content of sophie.sarral.io and remove any phone numbers that are not intended for public exposure. Implement measures to prevent the unintentional exposure of sensitive information in the ...
SAR-014: Exposure of Email Addresses	Low	Consider obfuscating email addresses on the website or using a contact form to reduce exposure to automated bots. Implement robust spam filtering and phishing detection mechanisms.
SAR-015: TRACE method enabled	Low	Disable the TRACE method on the web server.
SAR-016: No WAF Detected	Low	Implement a Web Application Firewall (WAF) to protect against common web application attacks. Configure the WAF to block malicious traffic and monitor for suspicious activity.
SAR-017: User Enumeration	Low	Disable or restrict access to user directories. Implement measures to prevent user enumeration, such as requiring valid credentials to access user profiles or directories.
SAR-018: Information Disclosure - Social Profiles	Info	Review the linked GitHub repositories to ensure no sensitive information is exposed.
SAR-019: Information Disclosure - LinkedIn Profiles	Info	Review the necessity of exposing employee LinkedIn profiles on the website.
SAR-020: Outdated Browser Warning	Info	Remove the outdated browser warning or update it to reflect current browser versions.
SAR-021: Social Media Profile Exposure	Info	Ensure that all linked social media profiles and GitHub repositories are properly secured and do not expose any sensitive information.
SAR-022: OpenSSH Version Information Disclosure	Info	Consider disabling version information disclosure in the SSH server configuration or keeping the server updated to the latest stable release.

Technical Findings

Finding SAR-001: Exposed Administrative Interfaces (High)

Description:	The web server enumeration revealed several potential administrative interfaces (admin, ADMIN, Admin, administracion, administer, admincp, administrat, administratie, administr8, administrador, administration, administrator, administratoraccounts, administrivia, administrators, adminlogon, adminlogin, adminpro, AdminService, adminpanel, admins, adminsessions, adminsql, AdminTools, admintools, ADMON, admon). If these interfaces are not properly secured, an attacker could gain unauthorized access to administrative functions, potentially leading to complete system compromise.
Risk:	Likelihood: Low Impact: High
System:	sarral.io
Tools Used:	FFUF
References:	OWASP: A05:2021 - Broken Access Control CWE: CWE-264
Evidence:	`admin, ADMIN, Admin, administracion, administer, admincp`

Remediation

Ensure that all administrative interfaces are protected by strong authentication mechanisms, such as multi-factor authentication. Regularly audit access logs to detect and prevent unauthorized access attempts. Implement role-based access control to limit the privileges of administrative users.

Finding SAR-002: DNS Resolution Error (Medium)

Description:	The subdomain www.pay.sarral.io fails to resolve, indicating a potential DNS misconfiguration. This can lead to denial of service for users attempting to access this subdomain.
Risk:	Likelihood: High Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: CWE-200
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 0x7f397bb75810>: Failed to resolve 'www.pay.sarral.io' ([Errno -2] Name or service not known)"))`

Remediation

Verify and correct the DNS records for the affected subdomain to ensure proper resolution.

Finding SAR-003: Missing HSTS Header (Medium)

Description:	The pay.sarral.io subdomain is missing the HTTP Strict Transport Security (HSTS) header. This allows man-in-the-middle attackers to downgrade connections to HTTP.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-614
Evidence:	`"hsts": null`

Remediation

Implement the HSTS header on the pay.sarral.io subdomain to enforce HTTPS connections.

Finding SAR-004: Potential Vulnerability in Contact Form (Medium)

Description:	The contact page uses reCAPTCHA and makes an AJAX call to send_mail.php. This script may be vulnerable to abuse or injection attacks if not properly secured.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A03:2021 - Injection CWE: CWE-79
Evidence:	`<script> $("#contactForm").on("submit", function (e) { e.preventDefault(); $.ajax({ url: "send_mail.php", method: "POST", data: $(this).serialize()`

Remediation

Review and secure the send_mail.php script to prevent abuse or injection attacks. Implement proper input validation and sanitization.

Finding SAR-005: 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 protects against man-in-the-middle attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
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 access the site via HTTPS.

Finding SAR-006: Exposure of API Endpoints (Medium)

Description:	The website www.sarral.io exposes API endpoints (/api.js, /api.js?render=6LfwfTgrAAAAAF8FCXh_3WsE_uYRB_9I9f6Qx_9R). These endpoints could potentially be targeted for unauthorized access or abuse if not properly secured.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`The Alive Web Hosts tool identified API endpoints on www.sarral.io.`

Remediation

Implement proper authentication and authorization mechanisms for all API endpoints. Regularly audit and test API security to prevent vulnerabilities.

Finding SAR-007: Outdated Apache Version (Medium)

Description:	The web server is running Apache version 2.4.58. While not immediately vulnerable, running the latest version is crucial for patching security flaws and maintaining system security. Older versions may contain known vulnerabilities that could be exploited.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1035 - Use of a Potentially Vulnerable Component
Evidence:	`Apache httpd 2.4.58`

Remediation

Upgrade to the latest stable version of Apache. Regularly apply security patches to prevent exploitation of known vulnerabilities.

Finding SAR-008: Sensitive Information Disclosure (Medium)

Description:	The web server exposes several directories and files that could contain sensitive information. These include configuration files (.config, .rhosts, .subversion, .cache, .hta, .listings), backup directories (_baks, _db_backups, _backup, _archive, autobackup), version control system directories (.git/HEAD, .svn, .cvs, .cvsignore, .svn/entries), temporary directories (_temp, _tmp, _tempalbums), and various other potentially sensitive locations (_vti_bin, _vti_log, _vti_rpc, _vti_txt, _vti_script, _vti_map, _vti_pvt, _vti_inf, _vti_cnf). Access to these resources could allow an attacker to gain unauthorized information about the system, its configuration, or its users.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	FFUF
References:	OWASP: A03:2021 - Injection CWE: CWE-200
Evidence:	`.config, .rhosts, .subversion, .cache, .hta, .listings, _baks, _db_backups, .git/HEAD, .svn, .cvs`

Remediation

Restrict access to sensitive directories and files by configuring appropriate permissions and access controls. Ensure that backup files are stored securely and are not accessible to unauthorized users. Remove any unnecessary files or directories from the web server.

Finding SAR-009: Information Disclosure - Server Version (Low)

Description:	The sophie.sarral.io subdomain exposes the server version (nginx/1.18.0 (Ubuntu)) in the HTTP headers. This information can be used by attackers to identify known vulnerabilities in the specific server version.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A03:2021 - Injection CWE: CWE-200
Evidence:	`"Server": "nginx/1.18.0 (Ubuntu)"`

Remediation

Disable the server version display in the HTTP headers.

Finding SAR-010: Information Disclosure - Phone Numbers (Low)

Description:	The sophie.sarral.io subdomain contains numerous phone numbers, which may lead to potential privacy concerns or 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 found in the HTML content of sophie.sarral.io`

Remediation

Review and remove any unnecessary phone numbers from the publicly accessible website.

Finding SAR-011: Information Disclosure - Email Addresses (Low)

Description:	The www.sarral.io domain exposes email addresses (Info@sarral.io, info@sarral.io), which can be targeted for spam or phishing attacks.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`Email addresses found in the HTML content of www.sarral.io`

Remediation

Implement measures to protect email addresses from being harvested, such as using obfuscation techniques or a contact form.

Finding SAR-012: Unnecessary HTTP methods enabled (Low)

Description:	The HTTP TRACE method is enabled on pay.sarral.io and sophie.sarral.io. This method can be used to steal cookies or other sensitive information.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200
Evidence:	`"http_methods": [ "", "TRACE" ]`

Remediation

Disable the HTTP TRACE method on the server.

Finding SAR-013: Exposure of Internal Phone Numbers (Low)

Description:	The subdomain sophie.sarral.io exposes a large number of phone numbers within its HTML content. While the context and validity of these numbers are unknown, their exposure could potentially be leveraged for social engineering attacks or other malicious purposes.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`The Alive Web Hosts tool identified numerous phone numbers on sophie.sarral.io.`

Remediation

Review the content of sophie.sarral.io and remove any phone numbers that are not intended for public exposure. Implement measures to prevent the unintentional exposure of sensitive information in the future.

Finding SAR-014: Exposure of Email Addresses (Low)

Description:	The website www.sarral.io exposes email addresses (Info@sarral.io, info@sarral.io) within its HTML content. This could lead to increased spam or phishing attempts targeting these addresses.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`The Alive Web Hosts tool identified email addresses on www.sarral.io.`

Remediation

Consider obfuscating email addresses on the website or using a contact form to reduce exposure to automated bots. Implement robust spam filtering and phishing detection mechanisms.

Finding SAR-015: TRACE method enabled (Low)

Description:	The HTTP TRACE method is enabled on pay.sarral.io and sophie.sarral.io. The TRACE method is used to debug web server connections. Attackers can use this method to steal cookies or other sensitive information.
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 Alive Web Hosts tool identified that the TRACE method is enabled on pay.sarral.io and sophie.sarral.io.`

Remediation

Disable the TRACE method on the web server.

Finding SAR-016: No WAF Detected (Low)

Description:	A Web Application Firewall (WAF) was not detected. While not a direct vulnerability, the absence of a WAF increases the attack surface and potential impact of web application vulnerabilities. A WAF provides an additional layer of security by filtering malicious traffic and preventing common web attacks.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WafW00f
References:	OWASP: A04:2021 - Insecure Design 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 to block malicious traffic and monitor for suspicious activity.

Finding SAR-017: User Enumeration (Low)

Description:	The web server enumeration revealed several user directories (~administrator, ~admin, ~adm, ~amanda, ~guest, ~apache, ~ftp, ~http, ~httpd, ~bin, ~log, ~logs, ~mail, ~operator, ~nobody, ~lp, ~root, ~sysadmin, ~sys, ~user, ~sysadm, ~test, ~www, ~webmaster, ~tmp). This information could be used by an attacker to enumerate valid user accounts on the system, which could then be targeted in brute-force or phishing attacks.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	FFUF
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200
Evidence:	`~administrator, ~admin, ~adm, ~amanda, ~guest, ~apache`

Remediation

Disable or restrict access to user directories. Implement measures to prevent user enumeration, such as requiring valid credentials to access user profiles or directories.

Finding SAR-018: Information Disclosure - Social Profiles (Info)

Description:	The sophie.sarral.io subdomain contains links to GitHub repositories, which may expose internal code or dependencies.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: CWE-200
Evidence:	`Links to GitHub repositories found in the HTML content of sophie.sarral.io`

Remediation

Review the linked GitHub repositories to ensure no sensitive information is exposed.

Finding SAR-019: Information Disclosure - LinkedIn Profiles (Info)

Description:	The www.sarral.io domain exposes LinkedIn profiles of employees, which can be used for social engineering attacks.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: CWE-200
Evidence:	`Links to LinkedIn profiles found in the HTML content of www.sarral.io`

Remediation

Review the necessity of exposing employee LinkedIn profiles on the website.

Finding SAR-020: Outdated Browser Warning (Info)

Description:	The www.sarral.io domain displays an outdated browser upgrade message for Internet Explorer 9, which may indicate a lack of maintenance or awareness of modern web standards.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: N/A CWE: N/A
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

Remove the outdated browser warning or update it to reflect current browser versions.

Finding SAR-021: Social Media Profile Exposure (Info)

Description:	The subdomain sophie.sarral.io exposes links to various social media profiles and GitHub repositories within its HTML content. While not inherently a vulnerability, this information could be used for reconnaissance purposes.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`The Alive Web Hosts tool identified social media links on sophie.sarral.io.`

Remediation

Ensure that all linked social media profiles and GitHub repositories are properly secured and do not expose any sensitive information.

Finding SAR-022: OpenSSH Version Information Disclosure (Info)

Description:	The SSH server is running OpenSSH 9.6p1. While this version is relatively recent, disclosing the version number allows attackers to target specific vulnerabilities associated with that version. This information can be used to fingerprint the system and identify potential weaknesses.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`OpenSSH 9.6p1 Ubuntu 3ubuntu13.11`

Remediation

Consider disabling version information disclosure in the SSH server configuration or keeping the server updated to the latest stable release.