SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 02, 2025
Project: SAR-096
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	2	6	7	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: OpenSSH Multiple Vulnerabilities	High	Upgrade OpenSSH to the latest stable version and apply all available security patches.
SAR-002: Apache HTTP Server Multiple Vulnerabilities	High	Upgrade Apache HTTP Server to the latest stable version and apply all available security patches.
SAR-003: Missing Security Headers	Medium	Implement the missing security headers on the web server. For HSTS, configure the server to send the Strict-Transport-Security header with a max-age directive. For X-Frame-Options, set the header to D...
SAR-004: Cleartext Protocol Exposure	Medium	Disable or remove FTP, RTSP, and PPTP services if they are not required. If these services are necessary, implement secure alternatives such as SFTP, RTSPS, or VPNs to encrypt data in transit. Ensure ...
SAR-005: Outdated Software Component	Medium	Upgrade OpenSSH to the latest stable version to address any known vulnerabilities and ensure the system is protected against potential attacks. Regularly monitor for security updates and apply them pr...
SAR-006: Outdated Software	Medium	Upgrade Nginx to the latest stable version to patch any known vulnerabilities.
SAR-007: Missing Security Headers	Medium	Implement the missing security headers on the server configuration.
SAR-008: Slowloris Denial of Service Vulnerability	Medium	Implement mitigation techniques such as setting connection limits, using a reverse proxy with timeouts, or employing a web application firewall (WAF).
SAR-009: Information Exposure through Comments	Low	Remove or sanitize all comments before deploying the application to production. Ensure that no sensitive information or internal development notes are included in the deployed code.
SAR-010: Phone Number and Social Media Exposure	Low	Review the necessity of exposing all listed phone numbers and social media links. Consider removing or obfuscating any sensitive information that is not required for public access.

SAR-011: reCaptcha Implementation	Low	Ensure that the reCaptcha response is properly validated on the server-side before processing any form data. Implement appropriate error handling and logging to detect and prevent abuse.
SAR-012: Web Server Version Information Disclosure	Low	Configure the web server to suppress the display of the server version in HTTP responses. This can be achieved by modifying the ServerTokens and ServerSignature directives in the Apache configuration ...
SAR-013: Information Disclosure	Low	Review the website content and remove any unnecessary exposure of email addresses and social media profiles. Consider using a contact form instead of directly displaying email addresses.
SAR-014: TRACE Method Enabled	Low	Disable the TRACE method on the web server configuration.
SAR-015: Potential Sensitive Directory Disclosure	Low	Ensure that sensitive directories are not publicly accessible and implement proper access controls.
SAR-016: Email Address Exposure	Info	Implement measures to protect against email harvesting, such as using CAPTCHAs or email obfuscation techniques. Monitor for any suspicious activity targeting these email addresses.
SAR-017: Outdated Browser Warning for IE9	Info	Evaluate the necessity of supporting outdated browsers like IE9. If support is required, ensure that the website is properly secured against vulnerabilities specific to these browsers. Consider deprec...

Technical Findings

Finding SAR-001: OpenSSH Multiple Vulnerabilities (High)

Description:	The OpenSSH version 9.6p1 running on the target is vulnerable to multiple exploits. These vulnerabilities could allow an attacker to gain unauthorized access to the system.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	Nmap Vulnerability Scan
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1189
Evidence:	`Nmap identified multiple CVEs associated with the OpenSSH version, including CVE-2024-6387.`

Remediation

Upgrade OpenSSH to the latest stable version and apply all available security patches.

Finding SAR-002: Apache HTTP Server Multiple Vulnerabilities (High)

Description:	The Apache HTTP Server version 2.4.58 is vulnerable to multiple exploits. These vulnerabilities could allow an attacker to perform various malicious activities, including remote code execution or information disclosure.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	Nmap Vulnerability Scan
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-937
Evidence:	`Nmap identified multiple CVEs associated with the Apache version, including CVE-2024-38476 and CVE-2024-38474.`

Remediation

Upgrade Apache HTTP Server to the latest stable version and apply all available security patches.

Finding SAR-003: 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. The absence of these headers can make the website vulnerable to various attacks, such as man-in-the-middle attacks (HSTS), clickjacking (X-Frame-Options), and MIME-sniffing attacks (X-Content-Type-Options).
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16: Improper Neutralization of Input During Initialization
Evidence:	`The security_headers section for pay.sarral.io shows null values 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. For HSTS, configure the server to send the Strict-Transport-Security header with a max-age directive. For X-Frame-Options, set the header to DENY or SAMEORIGIN. For X-Content-Type-Options, set the header to nosniff. Implement a Referrer-Policy and Permissions-Policy to control the information shared in the Referer header and the browser features available to the website, respectively. Set X-XSS-Protection to 1; mode=block.

Finding SAR-004: Cleartext Protocol Exposure (Medium)

Description:	The scan identified FTP, RTSP, and PPTP services running on the target. These protocols transmit data in cleartext, making them vulnerable to eavesdropping and data interception. An attacker could potentially capture sensitive information, such as usernames, passwords, and other confidential data, by passively monitoring network traffic.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A02:2021 - Cryptographic Failures CWE: CWE-319 - Cleartext Transmission of Sensitive Information
Evidence:	`Nmap scan identified open ports 21 (FTP), 554 (RTSP), and 1723 (PPTP).`

Remediation

Disable or remove FTP, RTSP, and PPTP services if they are not required. If these services are necessary, implement secure alternatives such as SFTP, RTSPS, or VPNs to encrypt data in transit. Ensure proper authentication and authorization mechanisms are in place to prevent unauthorized access.

Finding SAR-005: Outdated Software Component (Medium)

Description:	The scan identified OpenSSH version 9.6p1 running on the target. While not immediately vulnerable, running an outdated version of OpenSSH may expose the system to known vulnerabilities that have been patched in newer releases. Attackers could potentially exploit these vulnerabilities to gain unauthorized access to the system.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104 - Use of Unmaintained Third-Party Components
Evidence:	`Nmap scan identified OpenSSH 9.6p1.`

Remediation

Upgrade OpenSSH to the latest stable version to address any known vulnerabilities and ensure the system is protected against potential attacks. Regularly monitor for security updates and apply them promptly.

Finding SAR-006: Outdated Software (Medium)

Description:	The server 'sophie.sarral.io' is running an outdated version of Nginx (1.18.0). Older versions of software may contain known vulnerabilities that could be exploited by attackers.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104 - Use of Unmaintained Third-Party Components
Evidence:	`Server: nginx/1.18.0 (Ubuntu)`

Remediation

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

Finding SAR-007: Missing Security Headers (Medium)

Description:	The subdomains 'pay.sarral.io' and 'sophie.sarral.io' are missing several security headers, including HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. These headers help protect against various attacks, such as man-in-the-middle attacks, clickjacking, and cross-site scripting.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Alive Web Hosts
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16 - Configuration
Evidence:	`{'hsts': null, 'csp': null, 'x_frame_options': null, 'x_content_type_options': null, 'referrer_policy': null, 'permissions_policy': null, 'x_xss_protection': null}`

Remediation

Implement the missing security headers on the server configuration.

Finding SAR-008: Slowloris Denial of Service Vulnerability (Medium)

Description:	The target web server is likely vulnerable to Slowloris, a denial-of-service attack that works by holding connections open as long as possible, starving the server's resources.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Nmap Vulnerability Scan
References:	OWASP: A08:2021 - Software and Data Integrity Failures CWE: CWE-400
Evidence:	`Nmap's http-slowloris-check script identified the server as 'LIKELY VULNERABLE' to Slowloris DOS attack (CVE-2007-6750).`

Remediation

Implement mitigation techniques such as setting connection limits, using a reverse proxy with timeouts, or employing a web application firewall (WAF).

Finding SAR-009: Information Exposure through Comments (Low)

Description:	The subdomain pay.sarral.io contains comments such as "TODO: replace with variable/translation for this" and "TODO: replace this with stylesheet from this repo". These comments can reveal internal development practices and potential areas of future changes, which could be useful to an attacker.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A03:2021 - Injection CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`The comments section for pay.sarral.io contains TODO comments.`

Remediation

Remove or sanitize all comments before deploying the application to production. Ensure that no sensitive information or internal development notes are included in the deployed code.

Finding SAR-010: Phone Number and Social Media Exposure (Low)

Description:	The subdomain sophie.sarral.io exposes a large number of phone numbers and social media links. While not inherently a vulnerability, this information can be used for social engineering attacks or reconnaissance.
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:	`The phones and social_profiles sections for sophie.sarral.io contain numerous entries.`

Remediation

Review the necessity of exposing all listed phone numbers and social media links. Consider removing or obfuscating any sensitive information that is not required for public access.

Finding SAR-011: reCaptcha Implementation (Low)

Description:	The domain sarral.io includes reCaptcha implementation. The presence of a hidden input field with id="g-recaptcha-response" and a div with class="g-recaptcha" and data-sitekey attribute suggests the use of reCaptcha for form protection. However, the use of AJAX to submit the form and the presence of a send_mail.php script indicates a potential vulnerability if the reCaptcha response is not properly validated on the server-side.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A03:2021 - Injection CWE: CWE-602: Client-Side Enforcement of Server-Side Security
Evidence:	`The comments section for sarral.io contains reCaptcha related code.`

Remediation

Ensure that the reCaptcha response is properly validated on the server-side before processing any form data. Implement appropriate error handling and logging to detect and prevent abuse.

Finding SAR-012: Web Server Version Information Disclosure (Low)

Description:	The scan revealed that the target is running Apache httpd 2.4.58. Disclosing the web server version can provide attackers with valuable information to identify known vulnerabilities and launch targeted attacks. While not a direct vulnerability, it increases the attack surface.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A03:2021 - Injection CWE: CWE-200 - Information Exposure
Evidence:	`Nmap scan identified Apache httpd 2.4.58.`

Remediation

Configure the web server to suppress the display of the server version in HTTP responses. This can be achieved by modifying the ServerTokens and ServerSignature directives in the Apache configuration file.

Finding SAR-013: Information Disclosure (Low)

Description:	The main domain 'www.sarral.io' exposes several email addresses and social media profiles. This information can be used by attackers for social engineering or reconnaissance 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:	`Emails: ['Info@sarral.io', 'info@sarral.io'] Social Profiles: ['http://github.com/davist11/jQuery-One-Page-Nav', 'https://www.linkedin.com/company/sarral', ...]`

Remediation

Review the website content and remove any unnecessary exposure of email addresses and social media profiles. Consider using a contact form instead of directly displaying email addresses.

Finding SAR-014: TRACE Method Enabled (Low)

Description:	The HTTP TRACE method is enabled on 'pay.sarral.io' and 'sophie.sarral.io'. This method can be used by attackers 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:	`http_methods: ['', 'TRACE']`

Remediation

Disable the TRACE method on the web server configuration.

Finding SAR-015: Potential Sensitive Directory Disclosure (Low)

Description:	The FFUF scan identified several potentially sensitive directory names, such as 'Documents and Settings', 'Program Files', and 'reports list'. While these directories may not directly expose sensitive information, their existence could aid an attacker in further reconnaissance.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	FFUF
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-548
Evidence:	`FFUF scan output showing 301 redirects for 'Documents and Settings', 'Program Files', and 'reports list'.`

Remediation

Ensure that sensitive directories are not publicly accessible and implement proper access controls.

Finding SAR-016: Email Address Exposure (Info)

Description:	The domain sarral.io exposes email addresses (Info@sarral.io, info@sarral.io). While not inherently a vulnerability, this information can be used for phishing or spam campaigns.
Risk:	Likelihood: Low Impact: Info
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:	`The emails section for sarral.io contains email addresses.`

Remediation

Implement measures to protect against email harvesting, such as using CAPTCHAs or email obfuscation techniques. Monitor for any suspicious activity targeting these email addresses.

Finding SAR-017: Outdated Browser Warning for IE9 (Info)

Description:	The domain sarral.io includes a warning message for users with Internet Explorer 9 or older, suggesting they upgrade their browser. While this is a good practice, it also indicates that the website may still be supporting outdated and potentially vulnerable browsers.
Risk:	Likelihood: Low Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-937: Improperly Omitting Optimization Attributes
Evidence:	`The comments section for sarral.io contains the conditional comment for IE9.`

Remediation

Evaluate the necessity of supporting outdated browsers like IE9. If support is required, ensure that the website is properly secured against vulnerabilities specific to these browsers. Consider deprecating support for IE9 and older versions.
