SARRAL SECURITY

sophie.sarral.io

Security Assessment Findings Report

Business Confidential

Date: December 02, 2025
Project: SAR-105
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@sophie.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 sophie.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	5	6	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Missing Security Headers	Medium	Implement the missing security headers in the web server configuration. For example, configure HSTS to enforce HTTPS, CSP to restrict the sources of content, and X-Frame-Options to prevent clickjackin...
SAR-002: Outdated Software	Medium	Upgrade Nginx and React to the latest stable versions to patch any known vulnerabilities.
SAR-003: Outdated Nginx Version	Medium	Upgrade Nginx to the latest stable version to patch any known security vulnerabilities. Regularly check for updates and apply them promptly.
SAR-004: Exposed MySQL Service	Medium	Ensure that the MySQL service is properly secured with strong authentication and access controls. Consider restricting access to the MySQL service to only authorized IP addresses or internal networks.
SAR-005: Outdated MySQL Version	Medium	Upgrade MySQL to the latest stable version to patch any known security vulnerabilities. Regularly check for updates and apply them promptly.
SAR-006: Sensitive Information Disclosure - Phone Numbers	Low	Review the website content and remove any unnecessary phone numbers. Implement measures to protect the phone numbers from being scraped, such as using CAPTCHAs or rate limiting.
SAR-007: Sensitive Information Disclosure - Social Media Profiles	Low	Review the website content and remove any unnecessary social media profiles. Implement measures to protect the social media profiles from being scraped, such as using CAPTCHAs or rate limiting.
SAR-008: TRACE method enabled	Low	Disable the TRACE HTTP method on the web server.
SAR-009: HTTPS Connection Refused	Low	Investigate the HTTPS service configuration and ensure that it is properly configured and running. Check firewall rules to ensure that traffic to port 443 is allowed.

SAR-010: HTTPS Connection Refused	Low	Investigate the HTTPS service configuration and ensure that it is properly configured and running. Check firewall rules to ensure that traffic to port 443 is allowed.
SAR-011: HTTPS Connection Refused	Low	Investigate the HTTPS service configuration and ensure that it is properly configured and running. Check firewall rules to ensure that traffic to port 443 is allowed.
SAR-012: Domain Name Resolution Error	Info	Verify the DNS configuration for 'www.sophie.sarral.io' and ensure that it is properly configured. If the subdomain is not intended to be active, remove the DNS record.

Technical Findings

Finding SAR-001: 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 various attacks, such as cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks.
Risk:	Likelihood: Medium Impact: Medium
System:	sophie.sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-16: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Evidence:	`Security headers are null: hsts, csp, x_frame_options, x_content_type_options, referrer_policy, permissions_policy, x_xss_protection`

Remediation

Implement the missing security headers in the web server configuration. For example, configure HSTS to enforce HTTPS, CSP to restrict the sources of content, and X-Frame-Options to prevent clickjacking.

Finding SAR-002: Outdated Software (Medium)

Description:	The server is running an outdated version of Nginx (1.18.0) and React. Outdated software may contain known vulnerabilities that can be exploited by attackers.
Risk:	Likelihood: Medium Impact: Medium
System:	sophie.sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1104: Use of Unmaintained Third Party Component
Evidence:	`Server: nginx/1.18.0 (Ubuntu), Technologies: Nginx, React`

Remediation

Upgrade Nginx and React to the latest stable versions to patch any known vulnerabilities.

Finding SAR-003: 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 by attackers. Regular updates are crucial for maintaining security.
Risk:	Likelihood: Medium Impact: Medium
System:	sophie.sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1035 - Use of a Potentially Dangerous Function
Evidence:	`nginx 1.18.0 (Ubuntu)`

Remediation

Upgrade Nginx to the latest stable version to patch any known security vulnerabilities. Regularly check for updates and apply them promptly.

Finding SAR-004: Exposed MySQL Service (Medium)

Description:	The MySQL service is exposed on port 3306. This could allow unauthorized access to the database if not properly secured with strong authentication and access controls.
Risk:	Likelihood: Medium Impact: Medium
System:	sophie.sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`3306/tcp open mysql MySQL 8.0.44-0ubuntu0.22.04.1`

Remediation

Ensure that the MySQL service is properly secured with strong authentication and access controls. Consider restricting access to the MySQL service to only authorized IP addresses or internal networks.

Finding SAR-005: Outdated MySQL Version (Medium)

Description:	The server is running an outdated version of MySQL (8.0.44). Older versions may contain known vulnerabilities that could be exploited by attackers. Regular updates are crucial for maintaining security.
Risk:	Likelihood: Medium Impact: Medium
System:	sophie.sarral.io
Tools Used:	Nmap Top 1000
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-1035 - Use of a Potentially Dangerous Function
Evidence:	`MySQL 8.0.44-0ubuntu0.22.04.1`

Remediation

Upgrade MySQL to the latest stable version to patch any known security vulnerabilities. Regularly check for updates and apply them promptly.

Finding SAR-006: Sensitive Information Disclosure - Phone Numbers (Low)

Description:	The web scraper identified multiple phone numbers on the website. While not a direct vulnerability, this information could be used for social engineering or other malicious purposes.
Risk:	Likelihood: Low Impact: Low
System:	sophie.sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`Multiple phone numbers found in WebScraperRecon output.`

Remediation

Review the website content and remove any unnecessary phone numbers. Implement measures to protect the phone numbers from being scraped, such as using CAPTCHAs or rate limiting.

Finding SAR-007: Sensitive Information Disclosure - Social Media Profiles (Low)

Description:	The web scraper identified social media profiles on the website. While not a direct vulnerability, this information could be used for social engineering or other malicious purposes.
Risk:	Likelihood: Low Impact: Low
System:	sophie.sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A01:2021 - Broken Access Control CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`Multiple social media profiles found in WebScraperRecon output.`

Remediation

Review the website content and remove any unnecessary social media profiles. Implement measures to protect the social media profiles from being scraped, such as using CAPTCHAs or rate limiting.

Finding SAR-008: 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:	sophie.sarral.io
Tools Used:	WebScraperRecon
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 HTTP method on the web server.

Finding SAR-009: HTTPS Connection Refused (Low)

Description:	The tool failed to establish a connection to the HTTPS service on port 443. This could indicate a misconfiguration, service outage, or firewall issue.
Risk:	Likelihood: Low Impact: Info
System:	sophie.sarral.io
Tools Used:	WhatWeb
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`ERROR Opening: https://sophie.sarral.io - Connection refused`

Remediation

Investigate the HTTPS service configuration and ensure that it is properly configured and running. Check firewall rules to ensure that traffic to port 443 is allowed.

Finding SAR-010: HTTPS Connection Refused (Low)

Description:	The tool failed to establish a connection to the HTTPS service on port 443. This could indicate a misconfiguration, service outage, or firewall issue.
Risk:	Likelihood: Low Impact: Info
System:	sophie.sarral.io
Tools Used:	SSLScan
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`ERROR: Could not open a connection to host sophie.sarral.io (20.124.91.118) on port 443 (connect: Connection refused).`

Remediation

Investigate the HTTPS service configuration and ensure that it is properly configured and running. Check firewall rules to ensure that traffic to port 443 is allowed.

Finding SAR-011: HTTPS Connection Refused (Low)

Description:	The tool failed to establish a connection to the HTTPS service on port 443. This could indicate a misconfiguration, service outage, or firewall issue.
Risk:	Likelihood: Low Impact: Info
System:	sophie.sarral.io
Tools Used:	WafW00f
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='sophie.sarral.io', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7fc644a7c590>: Failed to establish a new connection: [Errno 111] Connection refused'))`

Remediation

Investigate the HTTPS service configuration and ensure that it is properly configured and running. Check firewall rules to ensure that traffic to port 443 is allowed.

Finding SAR-012: Domain Name Resolution Error (Info)

Description:	The web scraper failed to resolve the domain 'www.sophie.sarral.io'. This could indicate a DNS misconfiguration or an inactive subdomain.
Risk:	Likelihood: Low Impact: Info
System:	sophie.sarral.io
Tools Used:	WebScraperRecon
References:	OWASP: A05:2021 - Security Misconfiguration CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Evidence:	`NameResolutionError("<urllib3.connection.HTTPSConnection object at 0x7fbc13548ec0>: Failed to resolve 'www.sophie.sarral.io' ([Errno -2] Name or service not known)")`

Remediation

Verify the DNS configuration for 'www.sophie.sarral.io' and ensure that it is properly configured. If the subdomain is not intended to be active, remove the DNS record.
