SECURITY ASSESSMENT REPORT

Target: sophie.sarral.io
Date: November 25, 2025
Scan ID: 27

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **sophie.sarral.io** on 2025-11-25. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	2
High	1
Medium	5
Low	1
Info	0

2. Detailed Findings

1. PPTP Vulnerability

Severity: CRITICAL

Tool: Nmap Top 1000

Description:

PPTP (port 1723) is open. PPTP is a deprecated and highly insecure VPN protocol with known vulnerabilities. It should not be used.

Remediation:

Disable the PPTP service immediately. Migrate to a more secure VPN protocol such as OpenVPN, WireGuard, or IPsec.

2. Service Unavailability

Severity: CRITICAL

Tool: WafW00f

Description:

The target server (sophie.sarral.io) is refusing connections, preventing access to the website and any potential web application. This could be due to a server outage, firewall blocking the scanner, or misconfiguration.

Remediation:

Investigate the server's status, network connectivity, and firewall rules. Ensure the server is running and accessible from the internet. Check for any misconfigurations in the web server or network settings. Verify that the firewall is not blocking legitimate traffic from the scanner's IP address.

3. Exposed MySQL Service

Severity: HIGH

Tool: Nmap Top 1000

Description:

MySQL (port 3306) is open and accessible. If not properly secured with strong authentication and access controls, it could be vulnerable to unauthorized access and data breaches.

Remediation:

Ensure MySQL is configured with strong authentication (e.g., strong passwords, key-based authentication). Restrict access to MySQL to only authorized IP addresses or networks. Consider using a firewall to block external access to port 3306.

4. Potentially Unsecured FTP Service

Severity: MEDIUM **Tool:** Nmap Top 1000

Description:

FTP (port 21) is open, but the service version is unknown. If a standard, unencrypted FTP service is running, it transmits credentials in plaintext, making it vulnerable to eavesdropping and credential theft.

Remediation:

Determine the FTP service running. If it's a standard FTP, disable it and use a secure alternative like SFTP (over SSH) or FTPS (FTP over SSL/TLS). If required, configure FTP with TLS encryption and strong authentication.

5. Outdated OpenSSH Version

Severity: MEDIUM **Tool:** Nmap Top 1000

Description:

The system is running OpenSSH 8.9p1, which may contain known vulnerabilities. While not ancient, it's prudent to keep SSH up to date.

Remediation:

Upgrade OpenSSH to the latest stable version available for the Ubuntu distribution. Regularly apply security patches to the operating system.

6. Outdated Nginx Version

Severity: MEDIUM

Tool: Nmap Top 1000

Description:

The system is running nginx 1.18.0. While not critically old, newer versions contain security fixes and performance improvements.

Remediation:

Upgrade nginx to the latest stable version available for the Ubuntu distribution. Regularly apply security patches to the operating system.

7. Potentially Unsecured RTSP Service

Severity: MEDIUM

Tool: Nmap Top 1000

Description:

RTSP (port 554) is open, but the service version is unknown. RTSP can be vulnerable if not properly secured, potentially allowing unauthorized access to media streams.

Remediation:

Determine the RTSP service running. Secure the RTSP service with authentication and encryption (if supported). If not needed, disable the service.

8. Outdated MySQL Version

Severity: MEDIUM

Tool: Nmap Top 1000

Description:

The system is running MySQL 8.0.44. While not ancient, newer versions contain security fixes and performance improvements.

Remediation:

Upgrade MySQL to the latest stable version available for the Ubuntu distribution. Regularly apply security patches to the operating system.

9. Closed HTTPS Port

Severity: LOW

Tool: Nmap Top 1000

Description:

Port 443 (HTTPS) is closed. This means secure communication is not possible on this port. If secure communication is intended, this is a misconfiguration.

Remediation:

Investigate why HTTPS is not enabled. If secure communication is required, configure a web server to listen on port 443 with a valid SSL/TLS certificate.

3. Appendix: Raw Tool Output

The following section contains raw output from the security tools used during the assessment.

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 13:23 EST Nmap scan report for
sophie.sarral.io (20.124.91.118) Host is up (0.23s latency). Not shown: 992 filtered tcp
ports (no-response) PORT STATE SERVICE VERSION 21/tcp open ftp? 22/tcp open ssh OpenSSH
8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0) 80/tcp open http nginx 1.18.0
(Ubuntu) 443/tcp closed https 554/tcp open rtsp? 1723/tcp open pptp? 3000/tcp closed ppp
3306/tcp open mysql MySQL 8.0.44-0ubuntu0.22.04.1 Service Info: OS: Linux; CPE:
cpe:/o:linux:linux_kernel Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in
186.73 seconds
```

Tool: WhatWeb

```
/usr/bin/whatweb:257:in `require_relative': cannot load such file --
/usr/bin/lib/messages (LoadError) from /usr/bin/whatweb:257:in `'
```

Tool: WafW00f

```
______ / \ ( W00f! ) \ ____/ ,, __ 404 Hack Not Found |`-.__ / / __ __ /" _/ /_/ \ \ / /
*===* / \ \_/ / 405 Not Allowed / )__// \ / /| / /---` 403 Forbidden \\/` \ | / _ \ `\
/_\\_ 502 Bad Gateway / / \ \ 500 Internal Error `_____``-` /_/ \_\\ ~ WAFW00F : v2.3.1
~ The Web Application Firewall Fingerprinting Toolkit [*] Checking
https://sophie.sarral.io ERROR:wafw00f:Something went wrong
HTTPSConnectionPool(host='sophie.sarral.io', port=443): Max retries exceeded with url:
/ (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111]
Connection refused')) ERROR:wafw00f:Site sophie.sarral.io appears to be down
```