SECURITY ASSESSMENT REPORT

Target: sophie.sarral.io
Date: November 24, 2025
Scan ID: 8

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **sophie.sarral.io** on 2025-11-24. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

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

2. Detailed Findings

1. Open MySQL Port (3306)

Severity: HIGH **Tool:** Active Recon

Description:

MySQL port 3306 is open and accessible. If not properly secured with strong authentication and access controls, it could allow unauthorized access to the database.

Remediation:

Implement strong authentication for MySQL, restrict access to the MySQL port to only authorized IP addresses, and ensure that the MySQL server is configured securely. Consider using a firewall to block external access to port 3306.

2. Outdated Nginx Version

Severity: MEDIUM **Tool:** Active Recon

Description:

The server is running Nginx version 1.18.0, which is an older version. Older versions may contain known vulnerabilities that could be exploited by attackers.

Remediation:

Upgrade Nginx to the latest stable version to patch any known vulnerabilities. Regularly update the server's operating system and software packages.

3. Missing HTTPS on Port 443

Severity: MEDIUM **Tool:** Active Recon

Description:

Port 443 is closed, indicating that HTTPS is not enabled. This means that communication between the server and users is not encrypted, making it vulnerable to eavesdropping and man-in-the-middle attacks.

Remediation:

Enable HTTPS on the server by installing an SSL/TLS certificate and configuring the web server to listen on port 443. Redirect all HTTP traffic to HTTPS.

4. HTTPX Tool Error

Severity: LOW **Tool:** Passive Recon

Description:

The HTTPX tool encountered an error during the live service check, specifically indicating an unrecognized option '-s'. This suggests a potential misconfiguration of the tool, an outdated version, or an incorrect command-line syntax.

Remediation:

Review the HTTPX command-line options and ensure they are correct. Update HTTPX to the latest version. Verify the tool's configuration and dependencies. If the '-s' option was intended, determine its correct replacement or remove it if unnecessary.

5. Missing DNSSEC

Severity: LOW **Tool:** Active Recon

Description:

DNSSEC is not enabled for the domain. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks.

Remediation:

Implement DNSSEC to digitally sign DNS records and ensure their authenticity. This will help prevent attackers from redirecting traffic to malicious servers.

6. DNS Resolution Failure

Severity: INFO **Tool:** Passive Recon

Description:

The DNS resolution process failed to resolve the subdomain sophie.sarral.io to an IP address. This could indicate a DNS configuration issue, a problem with the DNS servers being used, or that the subdomain is not properly configured in DNS.

Remediation:

Verify the DNS configuration for the sarral.io domain and ensure that the sophie subdomain has a valid DNS record (A, CNAME, etc.). Check the DNS server's health and availability. Investigate potential DNS propagation delays.

3. Appendix: Raw Tool Output

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

Tool: Passive Recon

```
{"unique_subdomains_count": 1, "subdomains": ["sophie.sarral.io"], "resolved_hosts":
[], "live_services": [], "_raw_logs": "[05:13:38 AM] [+] Starting passive enumeration
for: sophie.sarral.io\n[05:13:38 AM] [+] Using temporary output directory:
/tmp/tmpiztvgx9j\n[05:13:38 AM] [+] Running Subfinder...\n[05:14:09 AM] [+] Running
Findomain...\n[05:14:17 AM] [+] Running Assetfinder...\n[05:14:19 AM] [+] Running Amass
Passive...\n[05:17:56 AM] [+] Merging results...\n[05:17:56 AM] [+] Found 1 unique
subdomains.\n[05:17:56 AM] [+] Checking DNS resolution with dnsx...\n[05:27:56 AM] [+]
DNSX resolved 0 hosts.\n[05:27:56 AM] [+] Checking HTTP/HTTPS services with
httpx...\n[05:27:56 AM] [!] HTTPX Error Output: Usage: httpx [OPTIONS] URL\n\nError: No
such option: -s\n[05:27:56 AM] [+] HTTPX found 0 live services.\n[05:27:56 AM] [+] Recon
complete.\n{\"unique_subdomains_count\": 1, \"subdomains\": [\"sophie.sarral.io\"],
\"resolved_hosts\": [], \"live_services\": []}\n"}
```

Tool: Active Recon

```
{"nmap_fast": "Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 05:28 EST\nNmap
scan report for sophie.sarral.io (20.124.91.118)\nHost is up (0.30s latency).\nNot
shown: 95 filtered tcp ports (no-response)\nPORT STATE SERVICE\n22/tcp open ssh\n80/tcp
open http\n443/tcp closed https\n3000/tcp closed ppp\n3306/tcp open mysql\n\nNmap done:
1 IP address (1 host up) scanned in 7.20 seconds", "whatweb": "\u001b[1m\u001b[31mERROR
Opening: https://sophie.sarral.io - Connection refused - connect(2) for
\"20.124.91.118\" port
443\u001b[0m\n\u001b[1m\u001b[34mhttp://sophie.sarral.io\u001b[0m [200 OK]
\u001b[1mCountry\u001b[0m[\u001b[0m\u001b[22mUNITED
STATES\u001b[0m][\u001b[1m\u001b[31mUS\u001b[0m], \u001b[1mHTML5\u001b[0m,
\u001b[1mHTTPServer\u001b[0m[\u001b[1m\u001b[31mUbuntu
Linux\u001b[0m][\u001b[1m\u001b[36mnginx/1.18.0 (Ubuntu)\u001b[0m],
\u001b[1mIP\u001b[0m[\u001b[0m\u001b[22m20.124.91.118\u001b[0m],
\u001b[1mMeta-Author\u001b[0m[\u001b[0m\u001b[22mSarral\u001b[0m],
\u001b[1mScript\u001b[0m[\u001b[0m\u001b[22mmodule\u001b[0m],
\u001b[1mTitle\u001b[0m[\u001b[1m\u001b[33mSOPHIE - Sarral\u001b[0m],
\u001b[1mX-UA-Compatible\u001b[0m[\u001b[0m\u001b[22mIE=edge\u001b[0m],
\u001b[1mnginx\u001b[0m[\u001b[1m\u001b[32m1.18.0\u001b[0m]", "dnsrecon":
"2025-11-24T05:28:15.554319-0500 INFO Starting enumeration for domain:
sophie.sarral.io\n2025-11-24T05:28:15.556281-0500 INFO std: Performing General
Enumeration against: sophie.sarral.io...\n2025-11-24T05:28:15.781314-0500 ERROR No
answer for DNSSEC query for sophie.sarral.io\n2025-11-24T05:28:16.072513-0500 INFO \t A
sophie.sarral.io 20.124.91.118\n2025-11-24T05:28:16.592628-0500 INFO Enumerating SRV
Records\n2025-11-24T05:28:17.603259-0500 ERROR No SRV Records Found for
sophie.sarral.io\n2025-11-24T05:28:17.603581-0500 INFO Completed enumeration for
domain: sophie.sarral.io", "_raw_logs": "[05:28:01 AM] [+] Starting Active Recon on
sophie.sarral.io...\n[05:28:01 AM] [+] Nmap: Scanning top 1000 ports...\n[05:28:08 AM]
[+] Nmap scan completed.\n[05:28:08 AM] [+] WhatWeb: Identifying technologies using
/home/kali/whatweb/whatweb...\n[05:28:14 AM] [+] WhatWeb completed.\n[05:28:14 AM] [+]
DNSRecon: Enumerating DNS records...\n[05:28:17 AM] [+] DNSRecon completed.\n[05:28:17
AM] [+] Active Recon phase finished.\n{\"nmap_fast\": \"Starting Nmap 7.95 (
https://nmap.org ) at 2025-11-24 05:28 EST\\nNmap scan report for sophie.sarral.io
(20.124.91.118)\\nHost is up (0.30s latency).\\nNot shown: 95 filtered tcp ports
(no-response)\\nPORT STATE SERVICE\\n22/tcp open ssh\\n80/tcp open http\\n443/tcp
```

```
closed https\\n3000/tcp closed ppp\\n3306/tcp open mysql\\n\\nNmap done: 1 IP address
(1 host up) scanned in 7.20 seconds\", \"whatweb\": \"\\u001b[1m\\u001b[31mERROR
Opening: https://sophie.sarral.io - Connection refused - connect(2) for
\\\"20.124.91.118\\\" port
443\\u001b[0m\\n\\u001b[1m\\u001b[34mhttp://sophie.sarral.io\\u001b[0m [200 OK]
\\u001b[1mCountry\\u001b[0m[\\u001b[0m\\u001b[22mUNITED
STATES\\u001b[0m][\\u001b[1m\\u001b[31mUS\\u001b[0m], \\u001b[1mHTML5\\u001b[0m,
\\u001b[1mHTTPServer\\u001b[0m[\\u001b[1m\\u001b[31mUbuntu
Linux\\u001b[0m][\\u001b[1m\\u001b[36mnginx/1.18.0 (Ubuntu)\\u001b[0m],
\\u001b[1mIP\\u001b[0m[\\u001b[0m\\u001b[22m20.124.91.118\\u001b[0m],
\\u001b[1mMeta-Author\\u001b[0m[\\u001b[0m\\u001b[22mSarral\\u001b[0m],
\\u001b[1mScript\\u001b[0m[\\u001b[0m\\u001b[22mmodule\\u001b[0m],
\\u001b[1mTitle\\u001b[0m[\\u001b[1m\\u001b[33mSOPHIE - Sarral\\u001b[0m],
\\u001b[1mX-UA-Compatible\\u001b[0m[\\u001b[0m\\u001b[22mIE=edge\\u001b[0m],
\\u001b[1mnginx\\u001b[0m[\\u001b[1m\\u001b[32m1.18.0\\u001b[0m]\", \"dnsrecon\":
\"2025-11-24T05:28:15.554319-0500 INFO Starting enumeration for domain:
sophie.sarral.io\\n2025-11-24T05:28:15.556281-0500 INFO std: Performing General
Enumeration against: sophie.sarral.io...\\n2025-11-24T05:28:15.781314-0500 ERROR No
answer for DNSSEC query for sophie.sarral.io\\n2025-11-24T05:28:16.072513-0500 INFO \\t
A sophie.sarral.io 20.124.91.118\\n2025-11-24T05:28:16.592628-0500 INFO Enumerating SRV
Records\\n2025-11-24T05:28:17.603259-0500 ERROR No SRV Records Found for
sophie.sarral.io\\n2025-11-24T05:28:17.603581-0500 INFO Completed enumeration for
domain: sophie.sarral.io\"}\n"}
```