SECURITY ASSESSMENT REPORT

Target: sophie.sarral.io
Date: November 24, 2025
Scan ID: 6

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	3

2. Detailed Findings

1. Open MySQL Port

Severity: HIGH **Tool:** Active Recon

Description:

The MySQL port (3306) is open to the public. This is a significant security risk, as it allows potential attackers to attempt to connect to the database and potentially gain unauthorized access to sensitive data.

Remediation:

Restrict access to the MySQL port to only authorized IP addresses or networks. Implement strong authentication for MySQL users. Keep MySQL software updated to the latest version. Consider using a firewall to block external access to the port.

---

2. Open SSH Port

Severity: MEDIUM **Tool:** Active Recon

Description:

The SSH port (22) is open, which could be a target for brute-force attacks or exploitation of SSH vulnerabilities if not properly secured.

Remediation:

Ensure SSH is configured with strong passwords or key-based authentication. Consider restricting SSH access to specific IP addresses or networks. Keep SSH software updated to the latest version.

---

3. Open HTTP Port without HTTPS

Severity: MEDIUM **Tool:** Active Recon

Description:

The HTTP port (80) is open, but the HTTPS port (443) is closed. This means that all traffic to the website is unencrypted, making it vulnerable to eavesdropping and man-in-the-middle attacks.

Remediation:

Enable HTTPS by installing an SSL/TLS certificate and configuring the web server to redirect HTTP traffic to HTTPS. Ensure the certificate is valid and properly configured.

4. HTTPX Command Error

Severity: LOW **Tool:** Passive Recon

Description:

The httpx command failed with an error indicating an invalid option ('-s'). This suggests a problem with the configuration or usage of the httpx tool in the scanning process.

Remediation:

Review the httpx command syntax and configuration to ensure it is correct. Update httpx to the latest version and verify that all required dependencies are installed. Investigate the scanning tool's configuration to ensure it's passing the correct parameters to httpx.

5. WhatWeb Failure

Severity: LOW **Tool:** Active Recon

Description:

The WhatWeb scan failed due to a missing library. This prevents the identification of technologies used on the target, which could be useful for identifying potential vulnerabilities.

Remediation:

Investigate and resolve the WhatWeb error by installing the missing library or reinstalling WhatWeb. Ensure all dependencies are met.

6. Subdomain without DNS Resolution

Severity: INFO **Tool:** Passive Recon

Description:

The subdomain 'sophie.sarral.io' was identified, but DNS resolution failed. This could indicate a misconfiguration in the DNS records, a non-existent host, or a temporary DNS issue.

Remediation:

Verify the DNS records for 'sophie.sarral.io' to ensure they are correctly configured and point to a valid IP address. Check for any DNS propagation delays or temporary DNS server issues.

---

7. Lack of Live Services

Severity: INFO **Tool:** Passive Recon

Description:

No live HTTP/HTTPS services were detected on the identified subdomain. This could indicate that the subdomain is not hosting any web applications, or that the services are not accessible due to firewall restrictions or other network issues.

Remediation:

Verify that the subdomain is intended to host web services. If so, check the firewall rules and network configuration to ensure that HTTP/HTTPS traffic is allowed. Investigate the application server logs for any errors or issues that might be preventing the services from running.

---

8. Missing SRV Records

Severity: INFO **Tool:** Active Recon

Description:

No SRV records were found for the domain. While not inherently a vulnerability, the absence of SRV records might indicate misconfiguration or lack of certain services.

Remediation:

Verify if SRV records are expected for the domain. If so, configure them correctly with the appropriate values.

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": "[03:53:45 AM] [+] Starting passive enumeration
for: sophie.sarral.io\n[03:53:45 AM] [+] Using temporary output directory:
/tmp/tmpap6ltbgb\n[03:53:45 AM] [+] Running Subfinder...\n[03:54:17 AM] [+] Running
Findomain...\n[03:54:20 AM] [+] Running Assetfinder...\n[03:54:22 AM] [+] Running Amass
Passive...\n[03:57:53 AM] [+] Merging results...\n[03:57:53 AM] [+] Found 1 unique
subdomains.\n[03:57:53 AM] [+] Checking DNS resolution with dnsx...\n[04:07:53 AM] [+]
DNSX resolved 0 hosts.\n[04:07:53 AM] [+] Checking HTTP/HTTPS services with
httpx...\n[04:07:54 AM] [!] HTTPX Error Output: Usage: httpx [OPTIONS] URL\n\nError: No
such option: -s\n[04:07:54 AM] [+] HTTPX found 0 live services.\n[04:07:54 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 04:07 EST\nNmap
scan report for sophie.sarral.io (20.124.91.118)\nHost is up (0.33s 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 8.93 seconds", "whatweb": "/usr/bin/whatweb:257:in
`require_relative': cannot load such file -- /usr/bin/lib/messages (LoadError)\n\tfrom
/usr/bin/whatweb:257:in `'", "dnsrecon": "2025-11-24T04:08:09.203686-0500 INFO Starting
enumeration for domain: sophie.sarral.io\n2025-11-24T04:08:09.205439-0500 INFO std:
Performing General Enumeration against:
sophie.sarral.io...\n2025-11-24T04:08:09.662873-0500 ERROR No answer for DNSSEC query
for sophie.sarral.io\n2025-11-24T04:08:10.136093-0500 INFO \t A sophie.sarral.io
20.124.91.118\n2025-11-24T04:08:11.735997-0500 INFO Enumerating SRV
Records\n2025-11-24T04:08:13.868488-0500 ERROR No SRV Records Found for
sophie.sarral.io\n2025-11-24T04:08:13.868832-0500 INFO Completed enumeration for
domain: sophie.sarral.io", "_raw_logs": "[04:07:58 AM] [+] Starting Active Recon on
sophie.sarral.io...\n[04:07:58 AM] [+] Nmap: Scanning top 1000 ports...\n[04:08:07 AM]
[+] Nmap scan completed.\n[04:08:07 AM] [+] WhatWeb: Identifying
technologies...\n[04:08:08 AM] [+] WhatWeb completed.\n[04:08:08 AM] [+] DNSRecon:
Enumerating DNS records...\n[04:08:13 AM] [+] DNSRecon completed.\n[04:08:13 AM] [+]
Active Recon phase finished.\n{\"nmap_fast\": \"Starting Nmap 7.95 ( https://nmap.org )
at 2025-11-24 04:07 EST\\nNmap scan report for sophie.sarral.io (20.124.91.118)\\nHost
is up (0.33s 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 8.93
seconds\", \"whatweb\": \"/usr/bin/whatweb:257:in `require_relative': cannot load such
file -- /usr/bin/lib/messages (LoadError)\\n\\tfrom /usr/bin/whatweb:257:in `'\",
\"dnsrecon\": \"2025-11-24T04:08:09.203686-0500 INFO Starting enumeration for domain:
sophie.sarral.io\\n2025-11-24T04:08:09.205439-0500 INFO std: Performing General
Enumeration against: sophie.sarral.io...\\n2025-11-24T04:08:09.662873-0500 ERROR No
answer for DNSSEC query for sophie.sarral.io\\n2025-11-24T04:08:10.136093-0500 INFO \\t
A sophie.sarral.io 20.124.91.118\\n2025-11-24T04:08:11.735997-0500 INFO Enumerating SRV
Records\\n2025-11-24T04:08:13.868488-0500 ERROR No SRV Records Found for
sophie.sarral.io\\n2025-11-24T04:08:13.868832-0500 INFO Completed enumeration for
domain: sophie.sarral.io\"}\n"}
```