SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 35

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **sarral.io** on 2025-11-26. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	1
Medium	5
Low	8
Info	9

2. Detailed Findings

1. Exposed Payment Processing Subdomain (pay.sarral.io)

Severity: HIGH **Tool:** Subfinder

Description:

The 'pay.sarral.io' subdomain suggests payment processing functionality. If not properly secured, it could be vulnerable to various attacks, including cross-site scripting (XSS), SQL injection, and man-in-the-middle (MITM) attacks, potentially leading to the theft of sensitive financial information.

Remediation:

Conduct a thorough security audit and penetration test of the 'pay.sarral.io' subdomain. Implement strong input validation and output encoding to prevent XSS and SQL injection. Enforce HTTPS with a valid SSL/TLS certificate to prevent MITM attacks. Implement multi-factor authentication (MFA) for administrative access. Ensure compliance with relevant payment card industry (PCI) standards.

---

2. Lack of DNSSEC

Severity: MEDIUM **Tool:** NSLookup

Description:

The domain sarral.io does not appear to be using DNSSEC. DNSSEC provides authentication of DNS data, preventing attackers from manipulating DNS records to redirect users to malicious sites. Without DNSSEC, the domain is vulnerable to DNS spoofing and cache poisoning attacks.

Remediation:

Implement DNSSEC for the sarral.io domain. This involves generating cryptographic keys, signing the DNS records, and publishing the public key in the parent zone.

---

3. Potential Subdomain Takeover (sarral.io)

Severity: MEDIUM **Tool:** Subfinder

Description:

The identified subdomains, particularly those under 'sarral.io', could be vulnerable to subdomain takeover if they are pointing to inactive or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage accounts, GitHub Pages). An attacker could claim these subdomains and host malicious content, potentially leading to phishing attacks or reputational damage.

Remediation:

Regularly audit DNS records and associated cloud services for all subdomains. Ensure that subdomains pointing to cloud services are properly configured and actively used. Remove DNS records for unused or decommissioned services. Implement subdomain takeover prevention measures offered by cloud providers.

---

4. Outdated Software/Services on Subdomains

Severity: MEDIUM **Tool:** Subfinder

Description:

Subdomains may be running outdated software or services, making them vulnerable to known exploits. This is especially true for less frequently used or maintained subdomains.

Remediation:

Implement a regular patching and vulnerability management program for all subdomains. Use automated tools to scan for vulnerabilities and apply patches promptly. Ensure that all software and services are kept up to date with the latest security updates.

---

5. Potential for Subdomain Takeover

Severity: MEDIUM **Tool:** Amass Passive

Description:

If any of the subdomains (pay.sarral.io, sophie.sarral.io, www.pay.sarral.io) are pointing to inactive or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage accounts, Heroku apps), they could be vulnerable to subdomain takeover attacks. An attacker could claim the inactive service and host malicious content or intercept sensitive data.

Remediation:

Verify that all subdomains are actively used and properly configured. Regularly audit DNS records and cloud service configurations to identify and remediate any potential subdomain takeover vulnerabilities. Implement preventative measures like DNS record monitoring and automated checks for orphaned cloud resources.

6. Outdated Apache HTTPD Version

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

Description:

The scan identifies Apache httpd 2.4.58. While not ancient, it's crucial to ensure this is the absolute latest patch level for the 2.4 branch. Older versions may contain known vulnerabilities that could be exploited.

Remediation:

Upgrade Apache HTTPD to the latest available version within the 2.4 branch or consider upgrading to a newer major version (2.5 if available and compatible) after thorough testing. Regularly apply security patches.

7. Lack of DNSSEC

Severity: LOW **Tool:** Whois

Description:

DNSSEC is not enabled for the domain. This makes the domain potentially vulnerable to DNS spoofing and cache poisoning attacks, although the risk is relatively low if other security measures are in place.

Remediation:

Implement DNSSEC to digitally sign DNS records, ensuring their authenticity and integrity. This will protect against DNS-based attacks.

8. Single A Record

Severity: LOW **Tool:** NSLookup

Description:

The domain sarral.io resolves to a single IP address (159.89.216.111). This creates a single point of failure. If the server at this IP address becomes unavailable, the website will be inaccessible.

Remediation:

Implement redundancy by adding multiple A records pointing to different servers. Consider using a load balancer to distribute traffic across these servers.

---

9. Information Disclosure via Subdomain Enumeration

Severity: LOW **Tool:** Subfinder

Description:

The enumeration of subdomains itself can provide attackers with valuable information about the organization's infrastructure and services. This information can be used to target specific systems or individuals.

Remediation:

While complete prevention is difficult, minimize the exposure of internal subdomains. Implement access controls to restrict access to sensitive resources. Regularly review and update DNS records to remove unnecessary entries. Consider using a wildcard SSL certificate to cover all subdomains.

---

10. Lack of HTTPS on Subdomains

Severity: LOW **Tool:** Amass Passive

Description:

The scan doesn't explicitly state whether HTTPS is enabled on each subdomain. If any subdomains are serving content over HTTP instead of HTTPS, they are vulnerable to man-in-the-middle attacks, where attackers can intercept and modify traffic.

Remediation:

Ensure that HTTPS is enabled and properly configured on all subdomains. Enforce HTTPS redirection to prevent users from accessing the site over HTTP. Implement HSTS (HTTP Strict Transport Security) to instruct browsers to always use HTTPS.

11. Information Disclosure via Subdomain Enumeration

Severity: LOW **Tool:** Amass Passive

Description:

The discovery of subdomains like 'pay.sarral.io' and 'sophie.sarral.io' provides attackers with information about the organization's infrastructure and services. This information can be used to target specific systems or individuals.

Remediation:

While subdomain enumeration is difficult to prevent entirely, minimize the exposure of sensitive subdomain names. Implement strong access controls and authentication mechanisms to protect sensitive data and systems. Consider using wildcard certificates to simplify certificate management and reduce the risk of certificate-related vulnerabilities.

12. Target Unreachable/Non-Existent

Severity: LOW **Tool:** Assetfinder

Description:

The target domain might be unreachable due to network issues, DNS resolution problems, or the domain simply not existing. This prevents any vulnerability assessment.

Remediation:

Confirm the target domain is valid and resolves to a valid IP address. Use tools like `ping` or `nslookup` to verify reachability and DNS resolution. If the domain is invalid, correct the target and rerun the scan.

13. Default Apache Configuration

Severity: LOW **Tool:** Nmap Top 1000

Description:

The scan indicates a standard Ubuntu Apache installation. Default configurations often include example files, directory listings, and other features that can expose sensitive information or provide attack vectors.

Remediation:

Review the Apache configuration files (e.g., apache2.conf, httpd.conf, virtual host configurations) and disable or remove any unnecessary modules, example files, and directory listings. Implement proper access controls and hardening measures.

---

14. MySQL Port Closed but Present

Severity: LOW **Tool:** Nmap Top 1000

Description:

The scan shows port 3306 (MySQL) as closed. While closed is better than open, the presence of the port suggests MySQL is installed on the server. If MySQL is not actively used, it should be uninstalled to reduce the attack surface. If it is used, ensure it is properly secured and only accessible from authorized locations.

Remediation:

If MySQL is not required, uninstall it. If it is required, ensure it is properly configured with strong passwords, restricted access (e.g., bind to localhost or specific IP addresses), and the latest security patches. Consider using a firewall to restrict access to port 3306.

---

15. WHOIS Privacy Protection

Severity: INFO **Tool:** Whois

Description:

The registrant information is hidden behind a privacy service (Domains By Proxy, LLC). While this is not inherently a vulnerability, it can hinder identifying the true owner of the domain, potentially complicating investigations in case of malicious activity.

Remediation:

Consider the context of the domain's use. If transparency is required, the privacy protection should be removed. Otherwise, ensure internal records clearly identify the domain owner and responsible parties.

16. Reliance on GoDaddy's Name Servers

Severity: INFO **Tool:** Whois

Description:

The domain relies on GoDaddy's name servers (ns63.domaincontrol.com, ns64.domaincontrol.com). While GoDaddy is a reputable provider, using a single provider creates a single point of failure. If GoDaddy's DNS infrastructure is compromised, the domain's availability could be affected.

Remediation:

Consider using a geographically diverse set of name servers from different providers to improve resilience and availability. This reduces the impact of outages affecting a single provider.

17. Domain Status: Client Prohibited Actions

Severity: INFO **Tool:** Whois

Description:

The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited status codes. These are security measures implemented by the registrar to prevent unauthorized changes to the domain. While not a vulnerability, it's important to be aware of these restrictions.

Remediation:

These statuses are generally beneficial. Ensure that the authorized personnel are aware of these restrictions and the process for removing them if legitimate changes are required.

18. Non-Authoritative Answer

Severity: INFO **Tool:** NSLookup

Description:

The response is a non-authoritative answer, meaning the DNS server (10.77.145.30) is not the authoritative server for sarral.io. This is normal behavior for most DNS queries, but it's important to be aware of when investigating DNS-related issues.

Remediation:

No mitigation is required. This is informational.

---

19. Exposed Subdomains Increase Attack Surface

Severity: INFO **Tool:** Amass Passive

Description:

The discovery of subdomains (pay.sarral.io, sophie.sarral.io, www.pay.sarral.io, www.sarral.io) expands the potential attack surface. Each subdomain represents a separate entry point that could be targeted by attackers.

Remediation:

Conduct thorough security assessments of each subdomain, including vulnerability scanning, penetration testing, and configuration reviews. Ensure all subdomains are properly secured and monitored.

---

20. Potential Scan Configuration Issue

Severity: INFO **Tool:** Assetfinder

Description:

Assetfinder returned no domains, suggesting a possible misconfiguration or network connectivity problem preventing the tool from identifying subdomains. This could lead to a false sense of security if vulnerabilities exist but are not being discovered.

Remediation:

Verify the target domain is correct, ensure Assetfinder is properly configured with API keys (if required), and check network connectivity to the target. Rerun the scan after confirming these aspects.

21. OpenSSH Version Disclosure

Severity: INFO **Tool:** Nmap Top 1000

Description:

The scan reveals the specific version of OpenSSH (9.6p1). While not inherently a vulnerability, disclosing the version makes the server a more attractive target for attackers looking for version-specific exploits. It also allows attackers to quickly determine if the server is vulnerable to any known exploits for that specific version.

Remediation:

Consider disabling version disclosure in the SSH configuration file (sshd_config) by setting `Protocol 2` and removing or commenting out the `VersionAddendum` directive. Keep OpenSSH updated to the latest version.

22. Lack of Identifiable WAF

Severity: INFO **Tool:** WafW00f

Description:

The WafW00f scan did not identify a specific WAF. While this doesn't guarantee the absence of a WAF, it suggests that standard fingerprinting techniques are ineffective, potentially indicating a custom or obfuscated WAF configuration. This could make it more difficult to assess the security posture of the web application.

Remediation:

Conduct further investigation to determine if a WAF is present, including manual testing and analysis of server responses to malicious requests. Review server configurations and security policies to understand the implemented security measures. Consider using more advanced WAF detection techniques.

23. No URLs Discovered - Potential Scan Configuration Issue

Severity: INFO **Tool:** HTTPx

Description:

The HTTPx scan returned an empty result, indicating that no URLs were discovered for the specified target(s). This could be due to incorrect target specification, network connectivity problems, or misconfiguration of the HTTPx tool itself. It does not directly indicate a vulnerability in the target, but rather a problem with the scanning process.

Remediation:

1. Verify the target URL(s) are correct and accessible. 2. Check network connectivity between the scanning machine and the target. 3. Review the HTTPx command-line arguments and configuration file for any errors. 4. Ensure the target is not blocking the scanning machine's IP address. 5. Try a simple ping or curl command to the target to confirm basic connectivity.

3. Appendix: Raw Tool Output

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

Tool: Whois

```
Domain Name: sarral.io Registry Domain ID: REDACTED Registrar WHOIS Server:
whois.godaddy.com Registrar URL: http://www.godaddy.com/domains/search.aspx?ci=8990
Updated Date: 2025-10-27T23:25:06Z Creation Date: 2023-09-12T23:24:25Z Registry Expiry
Date: 2026-09-12T23:24:25Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar
Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain
Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Registry
Registrant ID: REDACTED Registrant Name: REDACTED Registrant Organization: Domains By
Proxy, LLC Registrant Street: REDACTED Registrant City: REDACTED Registrant
State/Province: Arizona Registrant Postal Code: REDACTED Registrant Country: US
Registrant Phone: REDACTED Registrant Phone Ext: REDACTED Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED Registrant Email: REDACTED Registry Admin ID: REDACTED
Admin Name: REDACTED Admin Organization: REDACTED Admin Street: REDACTED Admin City:
REDACTED Admin State/Province: REDACTED Admin Postal Code: REDACTED Admin Country:
REDACTED Admin Phone: REDACTED Admin Phone Ext: REDACTED Admin Fax: REDACTED Admin Fax
Ext: REDACTED Admin Email: REDACTED Registry Tech ID: REDACTED Tech Name: REDACTED Tech
Organization: REDACTED Tech Street: REDACTED Tech City: REDACTED Tech State/Province:
REDACTED Tech Postal Code: REDACTED Tech Country: REDACTED Tech Phone: REDACTED Tech
Phone Ext: REDACTED Tech Fax: REDACTED Tech Fax Ext: REDACTED Tech Email: REDACTED Name
Server: ns63.domaincontrol.com Name Server: ns64.domaincontrol.com DNSSEC: unsigned URL
of the ICANN Whois Inaccuracy Complaint Form: https://icann.org/wicf/ >>> Last update of
WHOIS database: 2025-11-26T08:40:33Z <<< For more information on Whois status codes,
please visit https://icann.org/epp Terms of Use: Access to WHOIS information is provided
to assist persons in determining the contents of a domain name registration record in
the registry database. The data in this record is provided by Identity Digital or the
Registry Operator for informational purposes only, and accuracy is not guaranteed. This
service is intended only for query-based access. You agree that you will use this data
only for lawful purposes and that, under no circumstances will you use this data to (a)
allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile
of mass unsolicited, commercial advertising or solicitations to entities other than the
data recipient's own existing customers; or (b) enable high volume, automated,
electronic processes that send queries or data to the systems of Registry Operator, a
Registrar, or Identity Digital except as reasonably necessary to register domain names
or modify existing registrations. When using the Whois service, please consider the
following: The Whois service is not a replacement for standard EPP commands to the SRS
service. Whois is not considered authoritative for registered domain objects. The Whois
service may be scheduled for downtime during production or OT&E; maintenance periods.
Queries to the Whois services are throttled. If too many queries are received from a
single IP address within a specified time, the service will begin to reject further
queries for a period of time to prevent disruption of Whois service access. Abuse of the
Whois system through data mining is mitigated by detecting and limiting bulk query
access from single sources. Where applicable, the presence of a [Non-Public Data] tag
indicates that such data is not made publicly available due to applicable data privacy
laws or requirements. Should you wish to contact the registrant, please refer to the
Whois records available through the registrar URL listed above. Access to non-public
data may be provided, upon request, where it can be re asonably confirmed that the
requester holds a specific legitimate interest and a proper legal basis for accessing
the withheld data. Access to this data provided by Identity Digital can be requested by
submitting a request via the form found at
https://www.identity.digital/about/policies/whois-layered-access/. The Registrar of
```

```
Record identified in this output may have an RDDS service that can be queried for
additional information on how to contact the Registrant, Admin, or Tech contact of the
queried domain name. Identity Digital Inc. and Registry Operator reserve the right to
modify these terms at any time. By submitting this query, you agree to abide by this
policy.
```

Tool: NSLookup

```
Server: 10.77.145.30 Address: 10.77.145.30#53 Non-authoritative answer: Name: sarral.io
Address: 159.89.216.111
```

Tool: Subfinder

```
__ _____ __ _______ __/ /_ / __(_)___ ____/ /__ _____ / ___/ / / / __ \/ /_/ / __ \/ __
/ _ \/ ___/ (__ ) /_/ / /_/ / __/ / / / / /_/ / __/ / /____/\__,_/_.___/_/ /_/_/
/_/\__,_/\___/_/ projectdiscovery.io [INF] Loading provider config from
/home/kali/.config/subfinder/provider-config.yaml [INF] Enumerating subdomains for
sarral.io [INF] Found 4 subdomains for sarral.io in 11 seconds 556 milliseconds
pay.sarral.io www.pay.sarral.io www.sarral.io sophie.sarral.io
```

Tool: Amass Passive

```
sarral.io pay.sarral.io www.sarral.io sophie.sarral.io www.pay.sarral.io The
enumeration has finished Discoveries are being migrated into the local database
```

Tool: Assetfinder

```
```

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 03:41 EST Nmap scan report for
sarral.io (159.89.216.111) Host is up (0.085s latency). Not shown: 996 filtered tcp
ports (no-response) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 9.6p1 Ubuntu
3ubuntu13.11 (Ubuntu Linux; protocol 2.0) 80/tcp open http Apache httpd 2.4.58
((Ubuntu)) 443/tcp open ssl/http Apache httpd 2.4.58 3306/tcp closed mysql Service Info:
Host: sarral.io; 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 44.45 seconds
```

Tool: WhatWeb

```
zsh:1: no such file or directory: /usr/share/whatweb/whatweb
```

Tool: WafW00f

```
______ / \ ( Woof! ) \ ____/ ) ,, ) (_ .-. - _______ ( |__| ()``; |==|_______) .)|__| / (' /|\ ( |__| ( / ) / | \ . |__| \(_)_)) / | \ |__| ~ WAFW00F : v2.3.1 ~ The Web Application Firewall Fingerprinting Toolkit [*] Checking https://sarral.io [+] Generic Detection results: [-] No WAF detected by the generic detection [~] Number of requests: 7
```

Tool: HTTPx

```
Usage: httpx [OPTIONS] URL Error: No such option: -l
```