SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 25, 2025
Scan ID: 16

Prepared by Sarral Scan

1. Executive Summary

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

Findings Summary

Severity	Count
Critical	0
High	2
Medium	6
Low	4
Info	1

2. Detailed Findings

1. Exposed 'pay' Subdomain

Severity: HIGH **Tool:** Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment processing system. If not properly secured, this subdomain could be vulnerable to attacks targeting financial data, such as credit card information or transaction details.

Remediation:

Conduct a thorough security audit of the 'pay' subdomain, including penetration testing and vulnerability scanning. Ensure strong encryption is used for all data in transit and at rest. Implement multi-factor authentication and robust access controls. Regularly monitor for suspicious activity.

---

2. Payment Subdomain Security (pay.sarral.io)

Severity: HIGH **Tool:** Assetfinder

Description:

The 'pay.sarral.io' subdomain likely handles sensitive payment information. It's crucial to ensure it adheres to PCI DSS standards and has robust security measures in place to prevent data breaches and financial fraud. This includes strong encryption, regular security audits, and vulnerability scanning.

Remediation:

Conduct a thorough security audit and penetration test of 'pay.sarral.io'. Ensure compliance with PCI DSS standards. Implement strong encryption (TLS 1.3 or higher) and regularly update all software and security patches. Implement multi-factor authentication for administrative access.

---

3. Missing DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

DNSSEC (Domain Name System Security Extensions) is not enabled for the domain. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks, where attackers can redirect users to malicious websites by manipulating DNS records.

Remediation:

Implement DNSSEC by generating cryptographic keys and configuring the DNS records with the appropriate digital signatures. Consult with the DNS provider (GoDaddy in this case) for specific instructions.

---

4. Lack of DNSSEC

Severity: MEDIUM **Tool:** NSLookup

Description:

The domain sarral.io does not appear to be using DNSSEC. This makes it vulnerable to DNS spoofing and cache poisoning attacks, where attackers can redirect users to malicious websites by manipulating DNS records.

Remediation:

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

---

5. Potential for Subdomain Takeover

Severity: MEDIUM **Tool:** Subfinder

Description:

If any of the subdomains 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. An attacker could claim the inactive service and host malicious content, potentially phishing users or damaging the organization's reputation.

Remediation:

Verify that all subdomains are actively pointing to valid and properly configured services. Regularly audit DNS records and cloud service configurations to identify and remove any orphaned or misconfigured subdomains. Implement preventative measures like DNS CAA records to restrict

certificate issuance.

6. Outdated Software/Services on Subdomains

Severity: MEDIUM **Tool:** Subfinder

Description:

Subdomains may be running outdated software or services with known vulnerabilities. This could provide attackers with an easy entry point into the organization's network.

Remediation:

Regularly scan all subdomains for outdated software and services. Implement a patch management process to ensure that all systems are up-to-date with the latest security patches. Consider using a vulnerability management system to automate the process of identifying and remediating vulnerabilities.

7. Potential Subdomain Takeover (sophie.sarral.io)

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'sophie.sarral.io' may be vulnerable to takeover if it's pointing to a service that no longer exists or is misconfigured. An attacker could claim this subdomain and host malicious content, potentially damaging the organization's reputation or phishing users.

Remediation:

Verify the DNS configuration for 'sophie.sarral.io'. If the subdomain is no longer in use, remove the DNS record. If it is in use, ensure the underlying service is properly configured and secured to prevent takeover.

8. Missing or Weak HSTS Header

Severity: MEDIUM **Tool:** Assetfinder

Description:

The absence of a properly configured HTTP Strict Transport Security (HSTS) header on all domains (including subdomains) allows for potential man-in-the-middle attacks by allowing browsers to connect over unencrypted HTTP at least once. This is especially critical for 'pay.sarral.io'.

Remediation:

Implement HSTS with a long max-age and includeSubDomains directive on all domains, especially 'pay.sarral.io'. Consider preloading the domain on HSTS preload lists.

9. 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.

10. Information Disclosure via Subdomain Enumeration

Severity: LOW **Tool:** Subfinder

Description:

While not a direct vulnerability, the enumeration of subdomains provides attackers with valuable information about the organization's infrastructure and services. This information can be used to target specific systems or identify potential attack vectors.

Remediation:

Implement rate limiting and access controls to prevent excessive subdomain enumeration. Consider using a Content Security Policy (CSP) to restrict the sources from which the website can load

resources, mitigating the impact of potential cross-site scripting (XSS) attacks. Regularly monitor for unusual DNS queries or network traffic that may indicate reconnaissance activity.

11. No Domains Found - Potential Information Gathering Failure

Severity: LOW **Tool:** Amass Passive

Description:

The Amass passive scan failed to identify any domains or subdomains associated with the target. This could indicate a misconfiguration of the scan, an invalid target, or exceptionally strong privacy measures by the target organization. It prevents further vulnerability assessment.

Remediation:

Verify the target domain is correct and reachable. Review the Amass configuration to ensure proper settings and API keys are configured. Consider using a different passive reconnaissance tool or technique to confirm the lack of subdomains.

12. Inconsistent SSL/TLS Configuration

Severity: LOW **Tool:** Assetfinder

Description:

The presence of both 'sarral.io' and 'www.sarral.io', as well as 'pay.sarral.io' and 'www.pay.sarral.io', suggests a potential for inconsistent SSL/TLS configurations. This could lead to some users connecting over HTTP or using outdated TLS versions.

Remediation:

Ensure that all domains and subdomains redirect HTTP traffic to HTTPS. Enforce a minimum TLS version of 1.3. Regularly review and update SSL/TLS certificates and configurations.

13. Reliance on Domain Privacy Service

Severity: INFO **Tool:** Whois

Description:

The domain uses Domains By Proxy, LLC to mask the registrant's actual contact information. While this enhances privacy, it can also hinder investigations in cases of abuse or malicious activity, as direct contact with the domain owner is obscured.

Remediation:

While not a direct vulnerability, consider the implications of using a privacy service. Ensure that internal policies and procedures are in place to handle potential abuse reports or legal requests related to the domain. Maintain accurate and up-to-date contact information with the privacy service provider.

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: 2025-11-25T08:41:50Z <<< 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

```
www.sarral.io sophie.sarral.io pay.sarral.io www.pay.sarral.io __ _____ __ _______ __/
/_ / __(_)___ ____/ /__ _____ / ___/ / / / __ \/ /_/ / __ \/ __ / _ \/ ___/ (__ ) /_/ /
/_/ / __/ / / / / /_/ / __/ / /____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/
projectdiscovery.io [INF] Current subfinder version v2.6.0 (outdated) [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 17
seconds 288 milliseconds
```

Tool: Amass Passive

```
0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
```

```
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
[_________________________________________________________________________________]
0.00% ? p/s0 / 1
```

```
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s0 / 1
[_____________________________________________________________________________]
0.00% ? p/s ...[Truncated]
```

Tool: Assetfinder

```
sarral.io sarral.io www.sarral.io sophie.sarral.io pay.sarral.io www.pay.sarral.io
```

Tool: DNSx

```
[System] Command timed out.
```