SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 25, 2025
Scan ID: 23

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	4
Low	3
Info	3

2. Detailed Findings

1. Potential Payment Processing Security Issues on pay.sarral.io

Severity: HIGH **Tool:** Subfinder

Description:

The subdomain 'pay.sarral.io' likely handles payment processing. Without proper security measures, it could be vulnerable to attacks such as cross-site scripting (XSS), SQL injection, or man-in-the-middle attacks, potentially leading to financial data breaches.

Remediation:

Conduct a thorough security audit and penetration test of 'pay.sarral.io'. Implement robust input validation, output encoding, and secure coding practices. Ensure TLS/SSL is properly configured and enforced. Regularly update all software and libraries used in the payment processing system. Implement strong access controls and monitoring.

---

2. Insecure 'pay' Subdomain Configuration

Severity: HIGH **Tool:** Assetfinder

Description:

The 'pay.sarral.io' and 'www.pay.sarral.io' subdomains likely handle sensitive payment information. Without proper security measures, these subdomains could be vulnerable to various attacks, including cross-site scripting (XSS), SQL injection, and man-in-the-middle attacks. A compromised 'pay' subdomain could lead to data breaches and financial losses.

Remediation:

1. Conduct a thorough security audit of the 'pay.sarral.io' subdomain, including penetration testing and vulnerability scanning. 2. Implement strong input validation and output encoding to prevent XSS and SQL injection attacks. 3. Enforce HTTPS with a valid SSL/TLS certificate and HSTS to prevent man-in-the-middle attacks. 4. Implement multi-factor authentication (MFA) for administrative access to the 'pay' subdomain.

---

3. Missing DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

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

Remediation:

Implement DNSSEC by generating DNSSEC keys and configuring the domain's DNS records with the registrar (GoDaddy). This will cryptographically sign DNS data, ensuring its authenticity and integrity.

4. 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.

5. Exposure of Development/Staging Environment on sophie.sarral.io

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'sophie.sarral.io' might be a development or staging environment. If not properly secured, it could expose sensitive information, configuration details, or vulnerable code to attackers, potentially leading to a compromise of the production environment.

Remediation:

Restrict access to 'sophie.sarral.io' to authorized personnel only. Implement strong authentication and authorization mechanisms. Ensure that the environment does not contain any sensitive production data. Regularly scan for vulnerabilities and apply necessary patches. Consider using a separate network segment for development and staging environments.

6. Wildcard DNS and Potential Subdomain Takeover

Severity: MEDIUM **Tool:** Assetfinder

Description:

The presence of multiple subdomains, including 'sophie.sarral.io', suggests a potential wildcard DNS configuration. If 'sophie.sarral.io' or any other subdomain is not actively used and properly configured, it could be vulnerable to subdomain takeover. An attacker could claim the subdomain and host malicious content, potentially damaging the organization's reputation or launching phishing attacks.

Remediation:

1. Inventory all subdomains and their associated services. 2. Ensure all subdomains are actively managed and properly configured. 3. Implement monitoring for unauthorized subdomain creation or changes. 4. If a subdomain is no longer in use, either remove the DNS record or configure it to point to a neutral landing page with appropriate security measures.

7. 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.

8. Lack of HTTP Strict Transport Security (HSTS)

Severity: LOW **Tool:** Subfinder

Description:

The scan doesn't explicitly confirm HSTS is enabled on all subdomains. Without HSTS, users are vulnerable to man-in-the-middle attacks that downgrade HTTPS connections to HTTP, potentially exposing sensitive data.

Remediation:

Implement HSTS on all subdomains, including 'www.sarral.io', 'pay.sarral.io', 'sophie.sarral.io', and 'www.pay.sarral.io'. Configure the 'max-age' directive to a reasonable value (e.g., one year) and consider including the 'includeSubDomains' directive. Preload HSTS to ensure it is enabled from the first connection.

---

9. Lack of Security Headers

Severity: LOW **Tool:** Assetfinder

Description:

The scan output doesn't provide information about security headers. However, it's crucial to ensure that all domains, especially 'pay.sarral.io', have properly configured security headers such as Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), X-Frame-Options, and X-XSS-Protection. These headers can help mitigate various attacks and improve the overall security posture.

Remediation:

1. Analyze the HTTP response headers for all domains, especially 'pay.sarral.io'. 2. Implement and configure security headers such as CSP, HSTS, X-Frame-Options, and X-XSS-Protection. 3. Regularly review and update security header configurations to address emerging threats.

---

10. Privacy Protection Enabled

Severity: INFO **Tool:** Whois

Description:

The registrant information is hidden behind a privacy service (Domains By Proxy, LLC). While this protects the registrant's personal information, it can hinder investigations in cases of abuse or malicious activity originating from the domain.

Remediation:

While not strictly a vulnerability, consider the implications of privacy protection. Law enforcement or other legitimate parties can still request registrant information from the registrar if necessary. No immediate action is required unless transparency is desired.

---

11. Standard Domain Status Locks

Severity: INFO **Tool:** Whois

Description:

The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited status codes set. These are standard security measures to prevent unauthorized changes to the domain registration.

Remediation:

These status codes are a positive security measure and should remain enabled. No action is required.

---

12. 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.

---

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: 2025-11-25T11:45:35Z <<< 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

```
sophie.sarral.io pay.sarral.io www.pay.sarral.io www.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 6 seconds
15 milliseconds
```

Tool: Amass Passive

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

Tool: Assetfinder

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

Tool: DNSx

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