SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 25, 2025
Scan ID: 26

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	1
Medium	9
Low	2
Info	4

2. Detailed Findings

1. Unprotected Administrative Interfaces

Severity: HIGH **Tool:** Assetfinder

Description:

If sarral.io hosts any administrative interfaces (e.g., /admin, /login), they could be vulnerable to brute-force attacks, default credentials, or other authentication bypass techniques if not properly secured.

Remediation:

Implement strong authentication mechanisms, such as multi-factor authentication (MFA), for all administrative interfaces. Regularly audit and update credentials. Restrict access to administrative interfaces based on IP address or network segment. Implement rate limiting to prevent brute-force attacks.

---

2. Lack of DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

DNSSEC (Domain Name System Security Extensions) is not enabled for the domain. This makes the domain potentially 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 DNSSEC keys and configuring the domain's DNS records with the appropriate DS (Delegation Signer) records at the registrar (GoDaddy).

---

3. Missing SPF Record

Severity: MEDIUM **Tool:** NSLookup

Description:

The absence of an SPF (Sender Policy Framework) record allows attackers to more easily spoof emails from the sarral.io domain, increasing the risk of phishing and email-based attacks.

Remediation:

Create and publish an SPF record that specifies which mail servers are authorized to send emails on behalf of sarral.io. Regularly review and update the SPF record as needed.

4. Missing DKIM Record

Severity: MEDIUM **Tool:** NSLookup

Description:

The lack of a DKIM (DomainKeys Identified Mail) record makes it harder for email recipients to verify the authenticity of emails from sarral.io, increasing the risk of email tampering and phishing attacks.

Remediation:

Implement DKIM signing for outgoing emails and publish a DKIM record in DNS. Regularly rotate DKIM keys for enhanced security.

5. Missing DMARC Record

Severity: MEDIUM **Tool:** NSLookup

Description:

Without a DMARC (Domain-based Message Authentication, Reporting & Conformance) record, the domain owner has limited control over how email providers handle emails that fail SPF or DKIM checks, potentially leading to increased email spoofing and phishing success rates.

Remediation:

Implement a DMARC policy to instruct email providers on how to handle emails that fail authentication checks (SPF and DKIM). Start with a 'p=none' policy to monitor email traffic and gradually move to stricter policies like 'p=quarantine' or 'p=reject' as confidence increases.

6. Potential Payment Processing Vulnerabilities

Severity: MEDIUM **Tool:** Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' indicates a payment processing system. These subdomains are critical and require thorough security audits to prevent vulnerabilities such as SQL injection, cross-site scripting (XSS), or insecure direct object references (IDOR) that could lead to financial data breaches.

Remediation:

Conduct a comprehensive security audit and penetration test of the 'pay.sarral.io' and 'www.pay.sarral.io' subdomains. Implement robust input validation, output encoding, and access controls. Ensure compliance with PCI DSS standards if applicable.

---

7. Lack of Security Headers

Severity: MEDIUM **Tool:** Assetfinder

Description:

The domain sarral.io may be missing security headers such as Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), X-Frame-Options, and X-XSS-Protection. Absence of these headers can expose the website to various attacks like Cross-Site Scripting (XSS), clickjacking, and man-in-the-middle attacks.

Remediation:

Implement security headers on the web server. Configure CSP to restrict the sources of content the browser is allowed to load. Enable HSTS to enforce HTTPS connections. Set X-Frame-Options to prevent clickjacking. Enable X-XSS-Protection to filter out reflected XSS attacks.

---

8. Missing or Weak SSL/TLS Configuration

Severity: MEDIUM **Tool:** Assetfinder

Description:

The domain sarral.io might be using outdated SSL/TLS protocols or weak cipher suites, making it vulnerable to man-in-the-middle attacks and data interception. The certificate itself may be misconfigured or invalid.

Remediation:

Ensure the web server is configured to use the latest TLS protocol (TLS 1.3 or 1.2). Disable support for older protocols like SSLv3 and TLS 1.0/1.1. Use strong cipher suites. Regularly check the SSL/TLS certificate for validity and proper configuration using tools like SSL Labs' SSL Server Test.

---

9. Vulnerable Third-Party Libraries

Severity: MEDIUM **Tool:** Assetfinder

Description:

The website hosted on sarral.io may be using outdated or vulnerable third-party libraries (e.g., JavaScript libraries, frameworks). These libraries could contain known vulnerabilities that attackers can exploit.

Remediation:

Regularly scan the website for outdated or vulnerable third-party libraries using tools like Retire.js or Snyk. Update libraries to the latest versions or apply patches to address known vulnerabilities. Implement a Software Composition Analysis (SCA) process to manage third-party dependencies.

---

10. Lack of Input Validation

Severity: MEDIUM **Tool:** Assetfinder

Description:

The website hosted on sarral.io may not properly validate user input, leading to vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection.

Remediation:

Implement robust input validation on both the client-side and server-side. Sanitize and encode user input before displaying it on the website. Use parameterized queries or prepared statements to prevent SQL Injection. Implement a Web Application Firewall (WAF) to filter out malicious requests.

11. Reliance on Registrar's Name Servers

Severity: LOW **Tool:** Whois

Description:

The domain relies on the registrar's (GoDaddy) name servers (ns63.domaincontrol.com, ns64.domaincontrol.com). While convenient, this creates a single point of failure. If GoDaddy's DNS infrastructure experiences issues, the domain's availability could be affected.

Remediation:

Consider using a geographically diverse set of authoritative name servers, potentially including a third-party DNS provider, to improve redundancy and resilience. This reduces the risk of a single point of failure affecting the domain's availability.

12. Subdomain Takeover Risk

Severity: LOW **Tool:** Subfinder

Description:

If any of the subdomains, particularly 'sophie.sarral.io', are pointing to inactive or misconfigured cloud services (e.g., AWS S3 bucket, Azure Blob Storage, GitHub Pages), they could be vulnerable to subdomain takeover. An attacker could claim the subdomain and host malicious content or phish for credentials.

Remediation:

Verify that all subdomains are actively used and properly configured. Regularly audit DNS records and cloud service configurations to identify and remove dangling DNS records or misconfigured services. Implement preventative measures like DNS record monitoring and automated cleanup processes.

13. Privacy Protection Enabled

Severity: INFO **Tool:** Whois

Description:

The domain uses a privacy service (Domains By Proxy, LLC) to mask the registrant's personal information. While this protects privacy, it can hinder investigations in cases of abuse or illegal activity, making it harder to identify the true owner of the domain.

Remediation:

While not a direct vulnerability, consider the implications of privacy protection. Ensure that internal policies and procedures are in place to handle potential abuse reports or legal requests related to the domain. Law enforcement can still obtain the underlying information from the registrar if necessary.

---

14. Standard EPP Statuses

Severity: INFO **Tool:** Whois

Description:

The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited statuses set. These are standard security measures to prevent unauthorized changes to the domain registration. While not a vulnerability, it's important to be aware of these statuses and their implications.

Remediation:

These statuses are generally beneficial and should remain in place unless there is a specific reason to remove them. Ensure that authorized personnel understand how to manage these statuses if changes are required.

---

15. Non-Authoritative Answer

Severity: INFO **Tool:** NSLookup

Description:

The NSLookup returned a non-authoritative answer, meaning the DNS server queried (192.168.29.1) did not directly manage the sarral.io domain. This isn't inherently a vulnerability, but it indicates the response was cached. If the cache is poisoned, it could lead to incorrect IP resolution.

Remediation:

While not directly fixable by the domain owner, ensure the DNS resolvers used are secure and reputable. Regularly flush the DNS cache on your local machine if you suspect DNS poisoning.

16. Information Disclosure via Subdomain Enumeration

Severity: INFO **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 preventing subdomain enumeration entirely is difficult, consider implementing rate limiting on DNS queries and using a Content Security Policy (CSP) to restrict the sources from which resources can be loaded. Regularly review and update subdomain records to minimize the attack surface.

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: 2025-11-25T17:52:49Z <<< 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: 192.168.29.1 Address: 192.168.29.1#53 Non-authoritative answer: Name: sarral.io
Address: 159.89.216.111
```

Tool: Subfinder

```
__ _____ __ _______ __/ /_ / __(_)___ ____/ /__ _____ / ___/ / / / __ \/ /_/ / __ \/ __
/ _ \/ ___/ (__ ) /_/ / /_/ / __/ / / / / /_/ / __/ / /____/\__,_/_.___/_/ /_/_/
/_/\__,_/\___/_/ 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 308 milliseconds www.sarral.io sophie.sarral.io pay.sarral.io www.pay.sarral.io
```

Tool: Amass Passive

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

Tool: Assetfinder

```
sarral.io
```

Tool: DNSx

```
_ __ __ __| | _ __ ___ \ \/ / / _' || '_ \ / __| \ / | (_| || | | |\__ \ / \ \__,_||_|
|_||___//_/\_\ projectdiscovery.io [INF] Current dnsx version 1.1.4 (outdated) [System]
Command timed out.
```