SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 36

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	2
Medium	7
Low	4
Info	3

2. Detailed Findings

1. Exposed Payment Processing Subdomain

Severity: HIGH **Tool:** Subfinder

Description:

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

Remediation:

Implement robust security measures for the 'pay.sarral.io' subdomain, including: strong input validation and output encoding to prevent XSS and SQL injection; use of HTTPS with a valid SSL/TLS certificate to prevent MITM attacks; regular security audits and penetration testing; and adherence to PCI DSS standards if applicable.

2. Insecure 'pay' subdomain

Severity: HIGH **Tool:** Assetfinder

Description:

The 'pay.sarral.io' subdomain likely handles sensitive financial data. Without proper security measures (e.g., strong encryption, PCI DSS compliance), it could be vulnerable to data breaches, man-in-the-middle attacks, and other financial fraud.

Remediation:

Conduct a thorough security audit of the 'pay.sarral.io' subdomain, focusing on data encryption (HTTPS), authentication mechanisms, and compliance with relevant regulations (e.g., PCI DSS). Implement robust intrusion detection and prevention systems.

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 publishing the corresponding DNS records (DS and DNSKEY) with the domain's registrar. Consult with the DNS provider 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 Subdomain Takeover

Severity: MEDIUM **Tool:** Subfinder

Description:

Subdomains might be pointing to non-existent or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage accounts, GitHub Pages). If these services are not properly configured or have been abandoned, an attacker could claim the subdomain 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 secured. Remove DNS records for unused or abandoned services.

6. Potential Sensitive Data Exposure on 'pay' Subdomains

Severity: MEDIUM **Tool:** Amass Passive

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests the handling of payment-related data. If these subdomains are not properly secured, they could be vulnerable to attacks that expose sensitive financial information.

Remediation:

Prioritize security assessments of 'pay' subdomains. Ensure compliance with PCI DSS standards if applicable. Implement strong encryption, access controls, and input validation to protect payment data.

7. Potential subdomain takeover

Severity: MEDIUM **Tool:** Assetfinder

Description:

If the DNS records for any of these subdomains point to a service that is no longer in use (e.g., a defunct cloud provider instance), an attacker could claim the subdomain and host malicious content, potentially leading to phishing or other attacks.

Remediation:

Regularly audit DNS records to ensure they point to active and controlled resources. Implement subdomain verification mechanisms where possible. Monitor for unauthorized changes to DNS records.

8. Exposed 'sophie' subdomain

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'sophie.sarral.io' subdomain might be a development or staging environment. If it contains sensitive data or is not properly secured, it could expose internal information or provide an entry point for attackers to access the production environment.

Remediation:

Implement strict access controls for the 'sophie.sarral.io' subdomain. Ensure it does not contain any production data or credentials. Regularly scan for vulnerabilities and apply security patches. Consider using a separate network for development and staging environments.

9. Lack of HTTPS on all subdomains

Severity: MEDIUM **Tool:** Assetfinder

Description:

If any of these subdomains are not served over HTTPS, communication between users and the server is vulnerable to eavesdropping and man-in-the-middle attacks.

Remediation:

Ensure that all subdomains are configured to use HTTPS with a valid SSL/TLS certificate. Enforce HTTPS redirection to prevent users from accessing the site over HTTP.

10. Reliance on WHOIS Privacy

Severity: LOW **Tool:** Whois

Description:

While WHOIS privacy protects personal information, it can hinder incident response and attribution in case of malicious activity originating from the domain. It also makes it harder to verify the legitimacy of the domain owner.

Remediation:

Consider the trade-offs between privacy and transparency. Ensure that internal contact information is readily available for law enforcement or security researchers if needed. Implement strong authentication and authorization mechanisms to prevent unauthorized use of the domain.

11. 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.

12. Lack of HTTP Strict Transport Security (HSTS)

Severity: LOW

Tool: Subfinder

Description:

The scan doesn't explicitly confirm or deny HSTS. If HSTS is not enabled on all subdomains, particularly 'pay.sarral.io', users could be vulnerable to MITM attacks that downgrade connections to HTTP.

Remediation:

Enable HSTS on all subdomains, including 'pay.sarral.io', with a long max-age value and include subdomains. Ensure that the HSTS header is properly configured and that the domain is preloaded in browsers.

13. Lack of Information on Subdomain Purpose

Severity: LOW

Tool: Amass Passive

Description:

Without knowing the purpose of each subdomain (e.g., 'sophie.sarral.io'), it's difficult to assess the potential impact of a compromise. Unnecessary or forgotten subdomains can become easy targets.

Remediation:

Document the purpose and owner of each subdomain. Regularly review and decommission unused or outdated subdomains to reduce the attack surface.

14. GoDaddy Registrar

Severity: INFO **Tool:** Whois

Description:

The domain is registered with GoDaddy. While GoDaddy is a reputable registrar, it's important to be aware of potential security incidents that have affected registrars in the past. This is not a vulnerability in itself, but a factor to consider for overall risk assessment.

Remediation:

Stay informed about security best practices for domain registration and management. Enable two-factor authentication on the GoDaddy account. Regularly review domain settings and contact information.

15. Information Disclosure via Subdomain Enumeration

Severity: INFO **Tool:** Subfinder

Description:

The enumeration of subdomains reveals the organization's infrastructure and services. This information can be used by attackers to map the attack surface and identify potential vulnerabilities.

Remediation:

While subdomain enumeration is difficult to prevent entirely, minimize the exposure of sensitive information in subdomain names. Implement security measures to protect all identified subdomains, regardless of their perceived importance.

16. Exposed Subdomains Increase Attack Surface

Severity: INFO **Tool:** Amass Passive

Description:

The discovery of multiple subdomains expands the potential attack surface. Each subdomain represents a potential entry point for attackers to exploit vulnerabilities.

Remediation:

Conduct thorough vulnerability assessments and penetration testing on all identified subdomains. Implement a robust subdomain management strategy, including regular audits and monitoring.

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: 2025-11-26T08:45:00Z <<< 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 www.sarral.io [INF] Found 4 subdomains for sarral.io in 30 seconds 1
millisecond sophie.sarral.io pay.sarral.io www.pay.sarral.io
```

Tool: Amass Passive

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

Tool: Assetfinder

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