SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 33

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	5
Info	2

2. Detailed Findings

1. Misconfigured Payment Portal (pay.sarral.io, www.pay.sarral.io)

Severity: HIGH **Tool:** Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment portal. If this portal is not properly secured, it could be vulnerable to attacks such as SQL injection, cross-site scripting (XSS), or unauthorized access to sensitive financial data.

Remediation:

Conduct a thorough security audit and penetration test of the payment portal. Ensure that all payment processing is PCI DSS compliant and that strong authentication and authorization mechanisms are in place. Regularly update software and apply security patches.

---

2. Potential for Sensitive Data Exposure on 'pay' subdomain

Severity: HIGH **Tool:** Assetfinder

Description:

The 'pay' subdomain suggests financial transactions or payment processing. If not properly secured, it could be vulnerable to attacks that expose sensitive financial data, such as credit card numbers or bank account details. This subdomain requires immediate and thorough security assessment.

Remediation:

Conduct a comprehensive security audit and penetration test of the 'pay' subdomain. Ensure that all payment processing is PCI DSS compliant. Implement strong access controls and encryption to protect sensitive data. Regularly monitor for suspicious activity and implement intrusion detection systems.

---

3. Single Point of Failure: Reliance on GoDaddy's Name Servers

Severity: MEDIUM **Tool:** Whois

Description:

The domain relies solely on GoDaddy's name servers (ns63.domaincontrol.com and ns64.domaincontrol.com). If GoDaddy experiences a DNS outage, the domain will become unavailable.

Remediation:

Implement DNS redundancy by using a secondary DNS provider or a geographically diverse set of name servers from different providers.

4. Lack of DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

DNSSEC 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.

Remediation:

Enable DNSSEC to digitally sign DNS records and ensure their authenticity. This will protect against DNS-based attacks.

5. 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.

6. Potential Subdomain Takeover

Severity: MEDIUM **Tool:** Subfinder

Description:

If 'sophie.sarral.io' or other subdomains are pointing to non-existent or unused services (e.g., a cloud storage bucket that has been deleted), an attacker could claim the subdomain and host malicious content, potentially leading to phishing attacks or reputational damage.

Remediation:

Regularly audit DNS records and ensure that all subdomains point to active and properly configured services. Implement subdomain takeover prevention measures, such as verifying ownership of cloud resources associated with subdomains.

---

7. Payment Processing Subdomain Exposure

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'pay.sarral.io' is exposed. Without proper security measures, this could be a target for attackers attempting to intercept or manipulate payment information. A passive scan cannot determine if proper security measures are in place.

Remediation:

Conduct a thorough security audit of 'pay.sarral.io', including penetration testing and code review, to ensure PCI DSS compliance and protect sensitive payment data. Implement strong access controls and monitoring.

---

8. Subdomain Takeover Potential

Severity: MEDIUM **Tool:** Assetfinder

Description:

The identified subdomains (www.pay.sarral.io, pay.sarral.io, sophie.sarral.io) might be vulnerable to subdomain takeover if they are pointing to inactive or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage accounts, Heroku apps). An attacker could claim these subdomains and host

malicious content, potentially leading to phishing attacks or brand damage.

Remediation:

Verify that all subdomains are actively used and properly configured. If a subdomain is no longer needed, remove the DNS record. If a subdomain points to a cloud service, ensure the service is properly configured and secured to prevent unauthorized access and takeover. Regularly audit DNS records and cloud service configurations.

---

9. Information Disclosure via 'sophie' subdomain

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'sophie' subdomain could potentially expose internal information or resources if not properly secured. It might be a development or staging environment that contains sensitive data or configurations.

Remediation:

Investigate the purpose of the 'sophie' subdomain. If it's a development or staging environment, ensure it's isolated from the production environment and doesn't contain sensitive production data. Implement strong access controls and authentication mechanisms. Regularly review and update the security configuration.

---

10. Privacy Concerns due to Domains By Proxy

Severity: LOW **Tool:** Whois

Description:

The domain is registered through Domains By Proxy, which obscures the actual owner's contact information. This can hinder incident response and make it difficult to identify the responsible party in case of malicious activity.

Remediation:

Consider revealing the actual owner information, or implementing robust internal security policies and monitoring to compensate for the lack of direct contact information.

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. Information Disclosure via Subdomains

Severity: LOW **Tool:** Subfinder

Description:

Subdomains like 'sophie.sarral.io' might inadvertently expose sensitive information about internal systems, employees, or projects. This information could be used by attackers to gain a foothold in the network or launch targeted attacks.

Remediation:

Review the content and configuration of all subdomains to ensure that no sensitive information is publicly accessible. Implement strict access control policies and regularly monitor for data leaks.

13. Potential Weak Security on 'sophie.sarral.io'

Severity: LOW **Tool:** Amass Passive

Description:

The subdomain 'sophie.sarral.io' may be a personal or development subdomain with weaker security configurations than the main domain. This could provide an entry point for attackers to compromise the

network.

Remediation:

Investigate the purpose and security configuration of 'sophie.sarral.io'. Ensure it adheres to the same security standards as the main domain or, if no longer needed, decommission it. Implement strong authentication and authorization mechanisms.

14. Lack of HTTPS on all subdomains

Severity: LOW **Tool:** Assetfinder

Description:

It's not explicitly stated that all subdomains are using HTTPS. If any subdomain is serving content over HTTP, it exposes users to man-in-the-middle attacks and data interception.

Remediation:

Enforce HTTPS on all subdomains using TLS certificates. Implement HSTS (HTTP Strict Transport Security) to ensure browsers always connect to the domain over HTTPS. Regularly monitor certificate expiration dates and renew them promptly.

15. 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.

16. General Subdomain Enumeration Risk

Severity: INFO **Tool:** Amass Passive

Description:

Enumerating subdomains increases the attack surface. Each subdomain represents a potential entry point for attackers if not properly secured and maintained.

Remediation:

Regularly audit all subdomains for security vulnerabilities and outdated software. Implement a robust subdomain management process, including regular reviews and decommissioning of unused subdomains. Consider using DNSSEC to protect against DNS spoofing attacks.

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: 2025-11-26T08:30:44Z <<< 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] 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 pay.sarral.io [INF] Found 4 subdomains for
sarral.io in 1 second 652 milliseconds www.pay.sarral.io www.sarral.io sophie.sarral.io
```

Tool: Amass Passive

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

Tool: Assetfinder

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