SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 25, 2025
Scan ID: 18

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	3
Info	4

2. Detailed Findings

1. Unprotected Administrative Interfaces

Severity: HIGH **Tool:** Assetfinder

Description:

The domain might have publicly accessible administrative interfaces (e.g., /admin, /login) that are not adequately protected with strong authentication and authorization mechanisms. This could allow unauthorized access to sensitive data and system configurations.

Remediation:

Restrict access to administrative interfaces to authorized users only. Implement multi-factor authentication (MFA) for all administrative accounts. Regularly audit access logs for suspicious activity. Consider using a web application firewall (WAF) to protect against brute-force attacks and other common web application vulnerabilities.

2. Lack of Input Validation

Severity: HIGH **Tool:** Assetfinder

Description:

The website may not be properly validating user input, making it vulnerable to injection attacks such as SQL injection, Cross-Site Scripting (XSS), and command injection. This could allow attackers to execute arbitrary code or access sensitive data.

Remediation:

Implement robust input validation and sanitization techniques on all user-supplied data. Use parameterized queries or prepared statements to prevent SQL injection. Encode output to prevent XSS attacks. Avoid using dynamic code execution functions.

3. Unsigned DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

The domain sarral.io does not have DNSSEC enabled. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks, where attackers can redirect users to malicious websites.

Remediation:

Implement DNSSEC by generating DNSSEC keys and adding the appropriate records (DS, DNSKEY) to the domain's zone file at the registrar (GoDaddy).

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. Payment Processing Subdomain Security

Severity: MEDIUM

Tool: Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' subdomains indicates a payment processing system. These subdomains are critical and require thorough security audits to prevent financial data breaches. Vulnerabilities could include insecure configurations, outdated software, or lack of proper input validation.

Remediation:

Conduct a comprehensive security audit of the 'pay' subdomains, including penetration testing and code review. Ensure PCI DSS compliance if applicable. Implement strong input validation and output encoding to prevent injection attacks. Keep all software and libraries up to date.

6. Lack of Security Headers

Severity: MEDIUM **Tool:** Assetfinder

Description:

The domain 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 and configure security headers on the web server. Use tools like securityheaders.com to assess the current header configuration and identify missing or misconfigured headers. Prioritize HSTS, CSP, and X-Frame-Options.

7. Missing or Weak SSL/TLS Configuration

Severity: MEDIUM **Tool:** Assetfinder

Description:

The domain might be using outdated SSL/TLS protocols or weak cipher suites, making it vulnerable to eavesdropping and man-in-the-middle attacks. The certificate itself might be misconfigured or expiring soon.

Remediation:

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

8. Vulnerable Third-Party Libraries

Severity: MEDIUM **Tool:** Assetfinder

Description:

The website may be using outdated or vulnerable third-party libraries (e.g., JavaScript libraries, frameworks) that contain known security flaws. These vulnerabilities can be exploited to compromise the website and its users.

Remediation:

Regularly scan the website for vulnerable third-party libraries using tools like Snyk or OWASP Dependency-Check. Update all libraries to the latest versions to patch known vulnerabilities. Implement a software composition analysis (SCA) process to manage third-party dependencies.

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. Development/Testing Subdomain Exposure

Severity: LOW **Tool:** Subfinder

Description:

The 'sophie.sarral.io' subdomain might be a development or testing environment. If not properly secured, it could expose sensitive information such as API keys, database credentials, or internal application details. It could also be an entry point for attackers to gain unauthorized access to the production environment.

Remediation:

Review the purpose and security configuration of 'sophie.sarral.io'. If it's a development/testing environment, ensure it's isolated from the production network. Remove any sensitive data or credentials. Implement strong authentication and authorization controls. Consider removing the subdomain if it's no longer needed.

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. Reliance on Privacy Service (Domains By Proxy)

Severity: INFO **Tool:** Whois

Description:

The registrant information is hidden behind a privacy service (Domains By Proxy, LLC). While this protects personal information, it can also obscure the true owner of the domain, potentially hindering investigations in case of malicious activity. It is not inherently a vulnerability, but it can be a factor in security incidents.

Remediation:

While not a direct fix, consider the implications of using a privacy service and ensure that contact information is still accessible through appropriate channels if needed for legitimate purposes. Ensure the underlying contact information provided to the privacy service is accurate and up-to-date.

13. 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. While not a vulnerability, it's good to confirm these are intentionally set.

Remediation:

Review the domain status codes to ensure they align with the intended security posture. If any of these statuses are not desired, they can be modified through the registrar (GoDaddy).

14. 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.

15. Wildcard DNS and Potential Subdomain Takeover

Severity: INFO **Tool:** Subfinder

Description:

The existence of multiple subdomains, including 'www.pay.sarral.io', suggests the possibility of a wildcard DNS record. If a service is not properly configured for a specific subdomain, it could be vulnerable to subdomain takeover. An attacker could claim the subdomain and host malicious content.

Remediation:

Verify the DNS configuration for sarral.io. Ensure that all subdomains are properly configured and point to valid resources. Implement preventative measures against subdomain takeover, such as regularly monitoring DNS records and using a service like AWS Route 53's Alias records to prevent dangling DNS entries.

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: 2025-11-25T09:39:50Z <<< 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

```
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 3 seconds
516 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
```

Tool: DNSx

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