SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 39

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	1
Medium	9
Low	8
Info	5

2. Detailed Findings

1. Unsecured Payment Subdomain

Severity: HIGH

Tool: Assetfinder

Description:

The subdomain 'pay.sarral.io' likely handles sensitive payment information. If not properly secured with HTTPS, strong encryption, and regular security audits, it could be vulnerable to man-in-the-middle attacks, data breaches, and other exploits.

Remediation:

Ensure 'pay.sarral.io' is served over HTTPS with a valid SSL/TLS certificate. Implement strong encryption protocols (e.g., TLS 1.3). Conduct regular penetration testing and vulnerability assessments. Implement PCI DSS compliance if applicable.

2. 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.

3. Potential Payment Processing Vulnerabilities on pay.sarral.io

Severity: MEDIUM

Tool: Subfinder

Description:

The subdomain 'pay.sarral.io' suggests payment processing functionality. Without further investigation, it's impossible to determine specific vulnerabilities, but common issues include insecure data storage, lack of proper input validation, and vulnerabilities in third-party payment gateways. The presence of this subdomain necessitates a thorough security audit.

Remediation:

Conduct a comprehensive security assessment of 'pay.sarral.io', including penetration testing, code review, and vulnerability scanning. Ensure compliance with PCI DSS standards if applicable. Implement robust input validation and output encoding to prevent injection attacks. Regularly update all software and libraries used in the payment processing system.

4. Potential Payment Processing Security Risks

Severity: MEDIUM **Tool:** Amass Passive

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' indicates a payment processing system. Without further information, it's impossible to determine specific vulnerabilities, but payment systems are high-value targets and require rigorous security measures. A passive scan cannot determine if the payment processing is PCI DSS compliant or if it is vulnerable to common web application attacks.

Remediation:

Conduct a thorough security audit and penetration test of the 'pay.sarral.io' and 'www.pay.sarral.io' subdomains. Ensure PCI DSS compliance if applicable. Implement robust input validation, output encoding, and authentication/authorization mechanisms. Regularly update all software and libraries used in the payment processing system.

5. Missing or Weak Security Headers

Severity: MEDIUM **Tool:** Assetfinder

Description:

All domains, including 'sarral.io', 'www.sarral.io', 'sophie.sarral.io', and 'www.pay.sarral.io', may be missing crucial security headers such as HSTS, X-Frame-Options, Content-Security-Policy, and X-Content-Type-Options. This can leave the domains vulnerable to various attacks like clickjacking, cross-site scripting (XSS), and MIME sniffing.

Remediation:

Implement security headers on all domains. Specifically, configure HSTS to enforce HTTPS, X-Frame-Options to prevent clickjacking, Content-Security-Policy to mitigate XSS, and X-Content-Type-Options to prevent MIME sniffing. Regularly review and update these headers.

6. Subdomain Takeover Vulnerability

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'sophie.sarral.io' subdomain, if not actively used or properly configured, could be vulnerable to subdomain takeover. An attacker could claim this subdomain if it points to a non-existent service or resource.

Remediation:

Verify the purpose and configuration of 'sophie.sarral.io'. If it's no longer needed, remove the DNS record. If it's in use, ensure it's properly configured and secured. Regularly monitor DNS records for orphaned subdomains.

7. Outdated OpenSSH Version

Severity: MEDIUM **Tool:** Nmap Top 1000

Description:

The scan identifies OpenSSH version 9.6p1. While not immediately vulnerable, older versions of OpenSSH may contain known security vulnerabilities that could be exploited. Regular updates are crucial to patch these vulnerabilities.

Remediation:

Upgrade OpenSSH to the latest stable version available for the Ubuntu distribution. Regularly check for and apply security patches.

8. Outdated Apache HTTPd Version

Severity: MEDIUM **Tool:** Nmap Top 1000

Description:

The scan identifies Apache HTTPd version 2.4.58. Older versions of Apache HTTPd may contain known security vulnerabilities that could be exploited. Regular updates are crucial to patch these vulnerabilities.

Remediation:

Upgrade Apache HTTPd to the latest stable version available for the Ubuntu distribution. Regularly check for and apply security patches. Review Apache modules for any unnecessary or vulnerable components.

9. Outdated Apache Version

Severity: MEDIUM **Tool:** WhatWeb

Description:

The server is running Apache version 2.4.58. Older versions of Apache may contain known security vulnerabilities that could be exploited by attackers.

Remediation:

Upgrade Apache to the latest stable version to patch any known vulnerabilities. Regularly check for and apply security updates.

10. Absence of Web Application Firewall (WAF)

Severity: MEDIUM **Tool:** WafW00f

Description:

The scan indicates that no WAF was detected protecting the application. A WAF provides a crucial layer of defense against common web attacks such as SQL injection, cross-site scripting (XSS), and other OWASP Top 10 vulnerabilities. Without a WAF, the application is more exposed to these threats.

Remediation:

Implement a WAF (either cloud-based or on-premise) to filter malicious traffic and protect the application from web-based attacks. Configure the WAF with appropriate rulesets and regularly update them to address emerging threats. Consider using a combination of signature-based and anomaly-based detection for comprehensive protection. Evaluate alternative security measures if a WAF is not feasible.

11. Lack of DNSSEC

Severity: LOW **Tool:** Whois

Description:

DNSSEC is not enabled for the domain. This makes the domain potentially vulnerable to DNS spoofing and cache poisoning attacks, although the risk is mitigated by other security measures that may be in place at the server level.

Remediation:

Implement DNSSEC to digitally sign DNS records, ensuring their authenticity and integrity. This will protect against DNS-based attacks.

12. 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.

13. Subdomain Takeover Vulnerability

Severity: LOW **Tool:** Subfinder

Description:

If any of the subdomains (e.g., sophie.sarral.io) are pointing to a service that is no longer in use (e.g., an old AWS S3 bucket or a Heroku app), an attacker could potentially claim that service and host malicious content on the subdomain. This is a subdomain takeover vulnerability.

Remediation:

Regularly audit DNS records to identify subdomains pointing to unused or decommissioned services. Remove or update DNS records for these subdomains. Implement preventative measures such as using CNAME flattening or ALIAS records to avoid dangling DNS entries.

14. General Web Application Vulnerabilities

Severity: LOW **Tool:** Amass Passive

Description:

All identified subdomains (sarral.io, sophie.sarral.io, www.sarral.io) are potential targets for common web application vulnerabilities such as XSS, SQL injection, CSRF, and others. A passive scan cannot detect these vulnerabilities, but their potential existence should be considered.

Remediation:

Perform vulnerability scanning and penetration testing on all identified subdomains. Implement a Web Application Firewall (WAF) to mitigate common web application attacks. Follow secure coding practices and regularly update all software and libraries.

15. Subdomain Takeover Risk

Severity: LOW **Tool:** Amass Passive

Description:

If any of the subdomains (sarral.io, sophie.sarral.io, www.sarral.io, www.pay.sarral.io, pay.sarral.io) are pointing to a cloud service (e.g., AWS S3 bucket, Azure Blob Storage, GitHub Pages) that is not properly configured or has been abandoned, they could be vulnerable to subdomain takeover. This is a low severity issue because it requires further investigation to confirm.

Remediation:

Verify that all subdomains are properly configured and pointing to active resources. Regularly audit DNS records and cloud service configurations to prevent subdomain takeover vulnerabilities. Implement proper access controls and security measures for all cloud services.

16. Inconsistent Domain Configuration

Severity: LOW

Tool: Assetfinder

Description:

The presence of both 'sarral.io' and 'www.sarral.io' suggests a potential for inconsistent configuration. Users might access different versions of the site depending on whether they type 'www' or not. This can lead to confusion and potential security issues if not handled correctly.

Remediation:

Implement a proper redirect from 'www.sarral.io' to 'sarral.io' (or vice versa) to ensure a consistent user experience and avoid duplicate content issues. Ensure both domains are configured with the same security policies.

17. Plaintext HTTP Enabled

Severity: LOW

Tool: Nmap Top 1000

Description:

Port 80 (HTTP) is open, potentially allowing for unencrypted communication. This can expose sensitive information if users are not consistently redirected to HTTPS.

Remediation:

Implement a permanent redirect from HTTP to HTTPS at the server level. Consider disabling HTTP entirely if HTTPS is the primary method of access.

18. Information Disclosure - Email Address

Severity: LOW **Tool:** WhatWeb

Description:

The website publicly exposes the email address info@sarral.io. This could be used for spamming or phishing attacks.

Remediation:

Consider using a contact form instead of directly displaying the email address. Implement email filtering and anti-spam measures.

19. WHOIS Privacy Protection

Severity: INFO **Tool:** Whois

Description:

The domain uses a privacy service (Domains By Proxy, LLC) to mask the actual registrant's contact information. While not inherently a vulnerability, it can hinder identifying the true owner in cases of abuse or legal issues. This makes attribution more difficult.

Remediation:

Consider the implications of using a privacy service. If transparency is required, remove the privacy protection. Otherwise, ensure the underlying contact information is accurate and up-to-date with the privacy service provider.

20. Reliance on GoDaddy's Name Servers

Severity: INFO **Tool:** Whois

Description:

The domain relies on GoDaddy's name servers (ns63.domaincontrol.com, ns64.domaincontrol.com). While GoDaddy is a reputable provider, a compromise of their infrastructure could impact the domain's availability. This is a general risk associated with using any third-party DNS provider.

Remediation:

Consider using a geographically diverse set of name servers from different providers to increase redundancy and resilience. Regularly monitor the performance and security of the DNS infrastructure.

21. Client EPP Status Locks

Severity: INFO **Tool:** Whois

Description:

The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited status codes set. While these are security features to prevent unauthorized changes, they could also hinder legitimate administrative actions if the account is compromised or access is lost. This is not a vulnerability, but a configuration that needs to be understood.

Remediation:

Document the purpose of these locks and ensure that the process for removing them is well-understood and accessible to authorized personnel. Implement strong account security measures (MFA, strong passwords) to prevent unauthorized access to the domain management interface.

22. Lack of HTTP Strict Transport Security (HSTS)

Severity: INFO **Tool:** Subfinder

Description:

The scan doesn't explicitly confirm or deny the presence of HSTS. However, it's crucial to ensure that all subdomains, especially 'www.sarral.io' and 'pay.sarral.io', enforce HTTPS connections using HSTS to prevent man-in-the-middle attacks.

Remediation:

Configure all web servers to send the HSTS header with a long max-age value (e.g., one year). Consider preloading the domain on the HSTS preload list to ensure HSTS is enforced from the first connection. Verify that all subdomains are accessible via HTTPS.

23. Non-Informative HTTP Redirect Title

Severity: INFO **Tool:** WhatWeb

Description:

The HTTP to HTTPS redirect page has a title of '301 Moved Permanently'. This is not user-friendly and could be improved.

Remediation:

Configure the server to return a blank page or a more informative message for the HTTP redirect, or ideally, handle the redirect without displaying a separate page.

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: 2025-11-26T09:42:39Z <<< 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 www.sarral.io [INF] Found 4 subdomains for
sarral.io in 30 seconds 959 microseconds sophie.sarral.io pay.sarral.io
www.pay.sarral.io
```

Tool: Amass Passive

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

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 04:44 EST Nmap scan report for
sarral.io (159.89.216.111) Host is up (0.092s latency). Not shown: 996 filtered tcp
ports (no-response) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 9.6p1 Ubuntu
3ubuntu13.11 (Ubuntu Linux; protocol 2.0) 80/tcp open http Apache httpd 2.4.58
((Ubuntu)) 443/tcp open ssl/http Apache httpd 2.4.58 3306/tcp closed mysql Service Info:
Host: sarral.io; OS: Linux; CPE: cpe:/o:linux:linux_kernel Service detection performed.
Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP
address (1 host up) scanned in 53.28 seconds
```

Tool: WhatWeb

```
ERROR Opening: https://sarral.io/ - execution expired http://sarral.io [301 Moved
Permanently] Apache[2.4.58], Country[CANADA][CA], HTTPServer[Ubuntu
Linux][Apache/2.4.58 (Ubuntu)], IP[159.89.216.111],
RedirectLocation[https://sarral.io/], Title[301 Moved Permanently] https://sarral.io
[200 OK] Apache[2.4.58], Country[CANADA][CA], Email[info@sarral.io], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[159.89.216.111], JQuery, Script,
Title[SARRAL :: CYBER SECURITY]
```

Tool: WafW00f

```
? ,. ( . ) . " __ ?? (" ) )' ,' ) . (` '` (___()'`; ??? .; ) ' (( (" ) ;(, (( ( ;) " )")
/,___ /` _"., ,._'_.,)_(..,( . )_ _' )_') (. _..( ' ) \\ \\
|____|____|____|____|____|____|____|____|____| ~ WAFW00F : v2.3.1 ~ ~ Sniffing Web
Application Firewalls since 2014 ~ [*] Checking https://sarral.io [+] Generic Detection
results: [-] No WAF detected by the generic detection [~] Number of requests: 7
```

Tool: HTTPx

```
__ __ __ _ __ / /_ / /_/ /_____ | |/ / / __ \/ __/ __/ __ \| / / / / / /_/ /_/ /_/ / |
/_/ /_/\__/\__/ .___/_/|_| /_/ v1.1.5 projectdiscovery.io Use with caution. You are
responsible for your actions. Developers assume no liability and are not responsible for
any misuse or damage. [System] Command timed out.
```