SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 34

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	8
Low	6
Info	8

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 Vulnerabilities in 'pay.sarral.io'

Severity: HIGH **Tool:** Assetfinder

Description:

The 'pay.sarral.io' subdomain likely handles sensitive payment information. This subdomain requires rigorous security testing to identify and remediate potential vulnerabilities such as SQL injection, cross-site scripting (XSS), or insecure direct object references (IDOR). Compromise of this subdomain could lead to financial loss and reputational damage.

Remediation:

1. Conduct a thorough security audit and penetration test of 'pay.sarral.io'. 2. Implement strong input validation and output encoding to prevent injection attacks. 3. Enforce strict access controls and authentication mechanisms. 4. Regularly update all software and libraries used by the application. 5. Implement a web application firewall (WAF) to protect against common web attacks. 6. Ensure compliance with relevant payment card industry (PCI) standards.

3. 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 by manipulating DNS records.

Remediation:

Implement DNSSEC to digitally sign DNS records, ensuring their authenticity and integrity. This will protect users from being redirected to malicious sites due to DNS manipulation.

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. 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.

6. 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.

7. Wildcard DNS and Potential Subdomain Takeover

Severity: MEDIUM **Tool:** Assetfinder

Description:

The presence of multiple subdomains, including 'www' and potentially others not explicitly listed, suggests a possible wildcard DNS configuration. If any of these subdomains are not actively used and properly configured, they could be vulnerable to subdomain takeover attacks. An attacker could claim the unused subdomain and host malicious content, potentially damaging the organization's reputation or launching phishing attacks.

Remediation:

1. Inventory all subdomains associated with 'sarral.io'. 2. Ensure all subdomains point to valid and actively managed resources. 3. Implement proper DNS record management and monitoring. 4. For unused subdomains, either remove the DNS records or configure them to point to a sinkhole server or a static page indicating the subdomain is not in use. 5. Regularly monitor for subdomain takeover vulnerabilities using automated tools.

8. Potential Vulnerabilities in 'sophie.sarral.io'

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'sophie.sarral.io' subdomain could be hosting a personal website, a development environment, or some other application. Without further information, it's impossible to determine the exact function, but it represents a potential attack surface. It should be assessed for common web vulnerabilities.

Remediation:

1. Determine the purpose and functionality of 'sophie.sarral.io'. 2. Conduct a vulnerability scan and penetration test of the subdomain. 3. Implement appropriate security controls based on the application's functionality and data sensitivity. 4. Ensure the application is regularly updated and patched against known vulnerabilities.

9. Outdated OpenSSH Version

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

Description:

While OpenSSH 9.6p1 is relatively recent, vulnerabilities are constantly discovered. Running the latest patched version is crucial. Ubuntu 3ubuntu13.11 may also contain distribution-specific patches or backports, but it's important to verify.

Remediation:

Regularly update OpenSSH to the latest available version from the Ubuntu repositories using `apt update && apt upgrade`. Monitor security advisories for OpenSSH and Ubuntu to address any newly discovered vulnerabilities promptly.

10. Outdated Apache Version

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

Description:

Apache httpd 2.4.58 is a relatively recent version, but vulnerabilities are constantly discovered. Running the latest patched version is crucial. The Ubuntu distribution may also contain distribution-specific patches or backports, but it's important to verify.

Remediation:

Regularly update Apache to the latest available version from the Ubuntu repositories using `apt update && apt upgrade`. Monitor security advisories for Apache and Ubuntu to address any newly discovered vulnerabilities promptly.

11. WHOIS Privacy Service Usage

Severity: LOW **Tool:** Whois

Description:

The domain uses a WHOIS privacy service (Domains By Proxy, LLC) to mask the actual registrant's contact information. While this is a legitimate privacy measure, it can hinder investigations in cases of abuse or malicious activity, making it harder to identify the true owner.

Remediation:

Consider the trade-offs between privacy and accountability. While maintaining privacy, ensure that a clear and accessible channel exists for legitimate inquiries from law enforcement or security researchers. Review the privacy service's policies on revealing registrant information under specific circumstances.

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. 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.

14. 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.

15. Lack of HTTPS Enforcement

Severity: LOW **Tool:** Assetfinder

Description:

While not explicitly stated, it's crucial to verify that all subdomains, especially 'pay.sarral.io', enforce HTTPS. Failure to do so could expose sensitive data transmitted over unencrypted HTTP connections to eavesdropping attacks.

Remediation:

1. Ensure all subdomains are configured to use HTTPS. 2. Implement HTTP Strict Transport Security (HSTS) to force browsers to use HTTPS. 3. Regularly monitor SSL/TLS certificate validity and configuration.

16. Exposed SSH Service

Severity: LOW **Tool:** Nmap Top 1000

Description:

The SSH service is exposed on the standard port 22. While not inherently a vulnerability, it increases the attack surface. Brute-force attacks and vulnerability exploitation attempts are more likely when SSH is exposed.

Remediation:

Consider changing the SSH port to a non-standard port, implementing rate limiting, and using strong authentication methods such as key-based authentication. Implement fail2ban to block brute-force attempts.

17. 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, relying solely on a single provider introduces a single point of failure. If GoDaddy's DNS infrastructure experiences an outage, the domain will become inaccessible.

Remediation:

Consider using a geographically diverse set of name servers from multiple providers to improve redundancy and resilience against DNS outages. This could involve using a secondary DNS provider or a content delivery network (CDN) with DNS services.

18. Standard Domain Status Protections

Severity: INFO **Tool:** Whois

Description:

The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited status codes set. While these are generally good security practices to prevent unauthorized changes to the domain, they can also complicate legitimate domain management tasks if the owner loses access to their account.

Remediation:

Ensure that the domain owner has secure and reliable access to their GoDaddy account to manage these settings. Document the process for recovering access to the account in case of emergencies.

19. 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.

20. 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.

21. Exposed HTTP/HTTPS Services

Severity: INFO **Tool:** Nmap Top 1000

Description:

The HTTP and HTTPS services are exposed on standard ports 80 and 443. This is normal for a web server, but it's important to ensure the web application and server configuration are secure.

Remediation:

Regularly audit the web application for vulnerabilities (e.g., using a web application scanner). Ensure proper SSL/TLS configuration (e.g., using strong ciphers and disabling weak protocols). Implement a Web Application Firewall (WAF) to protect against common web attacks.

22. Closed MySQL Port

Severity: INFO **Tool:** Nmap Top 1000

Description:

The MySQL port 3306 is closed. This is generally good if the database is not intended to be accessed from outside the server. However, it's important to verify that this is the intended configuration and that the database is properly secured if it is accessed internally.

Remediation:

If the MySQL database is not intended to be accessed from outside the server, ensure that the firewall rules are properly configured to block external access to port 3306. If the database is accessed internally, ensure that proper authentication and authorization mechanisms are in place.

23. Lack of Identifiable WAF

Severity: INFO **Tool:** WafW00f

Description:

The WafW00f scan was unable to identify a specific Web Application Firewall (WAF) protecting the target website. This could indicate a lack of WAF protection or a WAF that is difficult to fingerprint using generic methods.

Remediation:

Investigate whether a WAF is intentionally absent. If a WAF is desired, implement and configure one. If a WAF is present but not detected, consider more advanced WAF detection techniques and ensure the WAF is properly configured to protect against common web application attacks.

24. Target Unreachable/Invalid

Severity: INFO **Tool:** HTTPx

Description:

HTTPx was unable to reach or resolve the specified target(s). This could be due to an incorrect URL, DNS resolution failure, network connectivity issues, or the target server being down.

Remediation:

Verify the target URL(s) are correct and accessible. Check DNS resolution and network connectivity. Ensure the target server is running and accepting connections.

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: 2025-11-26T08:32:56Z <<< 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 1 second 768 milliseconds 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 03:34 EST Nmap scan report for
sarral.io (159.89.216.111) Host is up (0.083s 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 37.52 seconds
```

Tool: WhatWeb

```
/usr/bin/whatweb:257:in `require_relative': cannot load such file --
/usr/bin/lib/messages (LoadError) from /usr/bin/whatweb:257:in `'
```

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

```
Usage: httpx [OPTIONS] URL Error: No such option: -l
```