SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 38

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	8
Info	3

2. Detailed Findings

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

Severity: HIGH **Tool:** Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment processing system. These subdomains are prime targets for attackers seeking to intercept or manipulate financial transactions. Common vulnerabilities include XSS, SQL injection, and insecure direct object references (IDOR).

Remediation:

Conduct a thorough security audit and penetration test of the 'pay.sarral.io' and 'www.pay.sarral.io' subdomains. Ensure that all payment processing components are PCI DSS compliant and that appropriate security controls are in place to protect sensitive financial data. Implement strong input validation and output encoding to prevent XSS and SQL injection attacks. Regularly update all software and libraries to patch known vulnerabilities.

---

2. Insecure Configuration of 'pay.sarral.io'

Severity: HIGH **Tool:** Assetfinder

Description:

The 'pay.sarral.io' subdomain likely handles sensitive financial data. If not properly secured, it could be vulnerable to attacks such as SQL injection, cross-site scripting (XSS), or man-in-the-middle attacks, leading to data breaches and financial loss.

Remediation:

Conduct a thorough security audit and penetration test of 'pay.sarral.io'. Implement strong encryption (HTTPS), input validation, and output encoding to prevent common web vulnerabilities. Ensure compliance with relevant security standards (e.g., PCI DSS).

---

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 malicious actors can redirect users to fake websites.

Remediation:

Enable DNSSEC for the domain through the domain registrar (GoDaddy). This involves generating and configuring DNSSEC keys and updating the domain's DNS records.

---

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. Subdomain Takeover Vulnerability

Severity: MEDIUM **Tool:** Subfinder

Description:

If any of these subdomains are pointing to a service that is no longer in use (e.g., a defunct cloud service), an attacker could potentially claim the subdomain and host malicious content, leading to phishing attacks or reputational damage. This is especially relevant if the DNS records are not properly managed.

Remediation:

Regularly audit DNS records to ensure that all subdomains are pointing to active and properly configured services. Implement subdomain takeover prevention measures, such as verifying ownership

of cloud services before pointing a subdomain to them. Monitor for any unauthorized changes to DNS records.

6. Potential Subdomain Takeover

Severity: MEDIUM **Tool:** Assetfinder

Description:

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

Remediation:

Regularly audit DNS records to ensure all subdomains point to valid and actively managed services. Implement subdomain verification mechanisms where possible. Monitor for unauthorized changes to DNS records.

7. Outdated Apache HTTPD Version

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

Description:

The Apache httpd version 2.4.58 is identified. While not ancient, it's crucial to ensure it's the latest patch release within the 2.4.x branch. Older versions may contain known vulnerabilities that could be exploited.

Remediation:

Upgrade Apache httpd to the latest available version within the 2.4.x branch or, if possible, to a newer major version (e.g., 2.5) after thorough testing. Regularly check for and apply security patches.

8. Outdated Apache Version

Severity: MEDIUM **Tool:** WhatWeb

Description:

Apache version 2.4.58 might have known vulnerabilities. While not immediately critical, using the latest stable version is crucial for security.

Remediation:

Upgrade Apache to the latest stable version. Regularly check for security updates and apply them promptly.

9. Outdated Ubuntu Linux

Severity: MEDIUM **Tool:** WhatWeb

Description:

The Ubuntu Linux server might have known vulnerabilities. While not immediately critical, using the latest stable version is crucial for security.

Remediation:

Upgrade Ubuntu to the latest stable version. Regularly check for security updates and apply them promptly.

10. Missing Web Application Firewall

Severity: MEDIUM **Tool:** WafW00f

Description:

The scan indicates that no WAF was detected. While not a vulnerability in itself, the absence of a WAF increases the attack surface and potential impact of web application vulnerabilities such as SQL injection, cross-site scripting (XSS), and remote code execution (RCE).

Remediation:

Implement a WAF (either hardware or software-based) to filter malicious traffic and protect against common web application attacks. Consider cloud-based WAF solutions for ease of deployment and management. Regularly update WAF rulesets to address emerging threats. Alternatively, ensure robust

input validation, output encoding, and other security measures are in place within the application itself.

11. Redacted Contact Information

Severity: LOW **Tool:** Whois

Description:

The registrant, admin, and tech contact information are redacted using a privacy service (Domains By Proxy, LLC). While this protects privacy, it can hinder incident response and make it difficult to directly contact the domain owner in case of security issues or abuse reports.

Remediation:

Consider providing a publicly accessible contact email address for security-related inquiries, even if other information remains redacted. Alternatively, ensure that the privacy service forwards security-related inquiries promptly.

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 Subdomain Enumeration

Severity: LOW **Tool:** Subfinder

Description:

Enumerating subdomains provides attackers with a broader understanding of the target organization's infrastructure and services. This information can be used to identify potential attack vectors and vulnerabilities.

Remediation:

While hiding subdomains entirely is often impractical, consider implementing rate limiting and other security measures to make subdomain enumeration more difficult. Regularly review and update the organization's security posture based on the information revealed by subdomain enumeration.

---

14. 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 accessible. Review the Amass configuration to ensure proper settings and sufficient data sources are enabled. Consider running the scan with increased verbosity for debugging. If the target is intentionally obscuring its infrastructure, consider alternative information gathering techniques.

---

15. Lack of HTTP Strict Transport Security (HSTS)

Severity: LOW **Tool:** Assetfinder

Description:

Without HSTS, users connecting to the website via HTTP may be vulnerable to man-in-the-middle attacks that downgrade the connection to HTTP, exposing sensitive data.

Remediation:

Enable HSTS on all subdomains, including the root domain, to force browsers to use HTTPS. Configure the 'max-age' directive appropriately and consider including subdomains and preloading HSTS.

16. Missing Security Headers

Severity: LOW **Tool:** Assetfinder

Description:

The absence of security headers like Content Security Policy (CSP), X-Frame-Options, and X-XSS-Protection can make the website vulnerable to various client-side attacks.

Remediation:

Implement appropriate security headers on all subdomains to mitigate client-side attacks. Configure CSP to restrict the sources of content that the browser is allowed to load. Set X-Frame-Options to prevent clickjacking attacks. Enable X-XSS-Protection to filter out reflected XSS attacks.

17. MySQL Port Closed but Present

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

Description:

The MySQL port (3306) is closed, but the fact that it's present in the scan results suggests that MySQL might be installed on the server. If MySQL is not intended to be exposed, ensure the firewall rules are configured correctly to prevent any external access. If it *is* intended to be exposed, ensure it is properly secured.

Remediation:

If MySQL is not needed, uninstall it. If it is needed, ensure it is only accessible from authorized IP addresses or internal networks via firewall rules. Implement strong authentication and authorization mechanisms for MySQL.

18. JQuery Version Disclosure

Severity: LOW **Tool:** WhatWeb

Description:

The scan identifies the use of JQuery. While not a direct vulnerability, knowing the version allows attackers to target known JQuery vulnerabilities if an outdated version is in use.

Remediation:

Ensure JQuery is updated to the latest version. Implement Subresource Integrity (SRI) to verify the integrity of the JQuery file.

---

19. OpenSSH Version Disclosure

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

Description:

The scan reveals the specific version of OpenSSH (9.6p1). While this version is relatively recent, disclosing the exact version can aid attackers in targeting known vulnerabilities specific to that version. This is more of an information disclosure issue than a direct vulnerability.

Remediation:

Consider disabling version disclosure in the SSH configuration file (sshd_config) by setting `Protocol 2` and removing or commenting out the `Banner` directive. Keep OpenSSH updated to the latest version.

---

20. Filtered TCP Ports

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

Description:

The scan reports 996 filtered TCP ports. This indicates the presence of a firewall or other network device blocking connections to these ports. While not a vulnerability in itself, it's important to review the firewall rules to ensure they are configured correctly and only necessary ports are open.

Remediation:

Review firewall rules to ensure they are configured according to the principle of least privilege, allowing only necessary traffic. Regularly audit firewall configurations.

21. No URLs Discovered - Potential Scan Configuration Issue

Severity: INFO **Tool:** HTTPx

Description:

The HTTPx scan returned an empty result, indicating that no URLs were discovered for the specified target(s). This could be due to incorrect target specification, network connectivity problems, or misconfiguration of the HTTPx tool itself. It does not directly indicate a vulnerability in the target, but rather a problem with the scanning process.

Remediation:

1. Verify the target URL(s) are correct and accessible. 2. Check network connectivity between the scanning machine and the target. 3. Review the HTTPx command-line arguments and configuration file for any errors. 4. Ensure the target is not blocking the scanning machine's IP address. 5. Try a simple ping or curl command to the target to confirm basic connectivity.

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: 2025-11-26T09:22:28Z <<< 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

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

Tool: Amass Passive

```
```

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 04:23 EST Nmap scan report for
sarral.io (159.89.216.111) Host is up (0.080s 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 36.37 seconds
```

Tool: WhatWeb

```
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] 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

```
______ / \ ( Woof! ) \ ____/ ) ,, ) (_ .-. - _______ ( |__| ()``; |==|_______) .)|__| / (' /|\ ( |__| ( / ) / | \ . |__| \(_)_)) / | \ |__| ~ WAFW00F : v2.3.1 ~ The Web Application Firewall Fingerprinting Toolkit [*] 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
```