SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 37

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	0
Medium	7
Low	7
Info	6

2. Detailed Findings

1. Unsigned DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

The domain's DNSSEC is unsigned, meaning DNS records are not cryptographically signed. 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 cryptographic keys and signing the DNS records with the private key. Then, publish the corresponding public key in the domain's DNS zone.

2. 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.

3. Vulnerability in 'pay' Subdomain

Severity: MEDIUM **Tool:** Subfinder

Description:

The 'pay.sarral.io' subdomain suggests a payment processing or related service. Any vulnerabilities in this subdomain could lead to sensitive financial data exposure, unauthorized transactions, or other financial crimes.

Remediation:

Conduct a thorough security assessment of the 'pay.sarral.io' subdomain, including penetration testing and vulnerability scanning. Ensure all payment processing components are up-to-date with the latest security patches and follow PCI DSS compliance standards.

4. Outdated OpenSSH Version

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

Description:

The OpenSSH version 9.6p1 is running. While not immediately vulnerable, older versions may contain known security flaws 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 security updates and apply them promptly.

5. Outdated Apache HTTPD Version

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

Description:

The Apache HTTPD version 2.4.58 is running. Older versions may contain known security flaws 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 security updates and apply them promptly.

6. 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.

7. 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.

8. Privacy Protection Obscuring Registrant Details

Severity: LOW **Tool:** Whois

Description:

The registrant information is hidden behind a privacy service (Domains By Proxy, LLC). While this is not inherently a vulnerability, it can hinder incident response and attribution in case of malicious activity originating from the domain. It also makes it harder to verify the legitimacy of the domain owner.

Remediation:

Consider the implications of privacy protection. While it offers anonymity, it can also raise suspicion. Depending on the organization's needs and risk tolerance, consider making registrant information publicly available or using a more transparent privacy service that allows for legitimate contact requests.

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. Potential Takeover of Unused Subdomains

Severity: LOW

Tool: Subfinder

Description:

If any of these subdomains are not actively used or properly configured, they could be vulnerable to subdomain takeover. An attacker could claim the subdomain and host malicious content, potentially damaging the organization's reputation and phishing users.

Remediation:

Regularly audit all subdomains to ensure they are actively used and properly configured. Implement preventative measures like DNS record monitoring and automated checks for dangling DNS records. If a subdomain is no longer needed, remove its DNS record.

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 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.

12. Target Domain Unreachable/Non-Existent

Severity: LOW **Tool:** Assetfinder

Description:

The target domain might be unreachable due to DNS issues, network problems, or the domain simply not existing. This prevents asset discovery.

Remediation:

Confirm the target domain resolves to a valid IP address using tools like `ping` or `nslookup`. Ensure there are no network connectivity issues preventing access to the target domain.

13. Lack of Information on TLS Configuration

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

Description:

The scan identifies HTTPS as running on port 443, but provides no information about the TLS configuration (e.g., supported protocols, cipher suites). Weak TLS configurations can expose the server to various attacks.

Remediation:

Use tools like SSL Labs' SSL Server Test (https://www.ssllabs.com/ssltest/) to analyze the TLS configuration and ensure it meets industry best practices. Disable weak ciphers and protocols.

14. 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.

15. Reliance on GoDaddy's Name Servers

Severity: INFO **Tool:** Whois

Description:

The domain relies on GoDaddy's name servers (ns63.domaincontrol.com and ns64.domaincontrol.com). While GoDaddy is a reputable provider, relying solely on a single provider introduces a single point of failure. If GoDaddy experiences an outage, the domain's availability could be affected.

Remediation:

Consider using a geographically diverse set of name servers from multiple providers to improve redundancy and resilience against outages. This is especially important for critical services.

16. 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.

17. Lack of HTTPS on 'sarral.io' and 'sophie.sarral.io'

Severity: INFO **Tool:** Subfinder

Description:

The scan doesn't explicitly confirm HTTPS usage. If 'sarral.io' and 'sophie.sarral.io' are not using HTTPS, communication between users and the server is unencrypted, making it vulnerable to eavesdropping and man-in-the-middle attacks.

Remediation:

Enforce HTTPS on all subdomains, including 'sarral.io' and 'sophie.sarral.io'. Implement HSTS (HTTP Strict Transport Security) to ensure browsers always connect via HTTPS.

18. Potential Scan Configuration Issue

Severity: INFO **Tool:** Assetfinder

Description:

Assetfinder returned no domains, which could indicate a problem with the scan configuration (e.g., incorrect target domain, network connectivity issues, or tool malfunction).

Remediation:

Verify the target domain is correct and reachable. Check Assetfinder's configuration and ensure it has the necessary permissions and network access. Rerun the scan with verbose output to identify any errors.

19. 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.

20. 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: 2025-11-26T09:09:50Z <<< 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
```

Tool: Amass Passive

```
```

Tool: Assetfinder

```
```

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 04:11 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/https Apache/2.4.58 (Ubuntu) 3306/tcp closed mysql Service
Info: 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 38.59 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

```
? ,. ( . ) . " __ ?? (" ) )' ,' ) . (` '` (___()'`; ??? .; ) ' (( (" ) ;(, (( ( ;) " )")
/,___ /` _"., ,._'_.,)_(..,( . )_ _' )_') (. _..( ' ) \\ \\
|____|____|____|____|____|____|____|____|____| ~ 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
```