SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 26, 2025
Scan ID: 41

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	10
Low	7
Info	6

2. Detailed Findings

1. Single Point of Failure: Reliance on GoDaddy's Name Servers

Severity: MEDIUM **Tool:** Whois

Description:

The domain relies solely on GoDaddy's name servers (ns63.domaincontrol.com and ns64.domaincontrol.com). If GoDaddy experiences a DNS outage, the domain will become inaccessible.

Remediation:

Implement DNS redundancy by using a secondary DNS provider or a geographically diverse set of name servers. This will ensure that the domain remains accessible even if one DNS provider experiences an outage.

---

2. Lack of DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

The DNSSEC field is 'unsigned', indicating that DNSSEC is not enabled. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks, where attackers can redirect users to malicious websites.

Remediation:

Enable DNSSEC for the domain. This will digitally sign DNS records, ensuring their authenticity and integrity. Consult with the domain registrar (GoDaddy) for instructions on enabling DNSSEC.

---

3. DNS Server Communication Timeout

Severity: MEDIUM **Tool:** NSLookup

Description:

The NSLookup query experienced multiple communication timeouts when attempting to contact the DNS server 10.77.145.30. This indicates a potential problem with the DNS server's availability, network connectivity, or configuration, leading to unreliable DNS resolution.

Remediation:

Investigate the health and configuration of the DNS server 10.77.145.30. Check network connectivity between the client and the DNS server. Review DNS server logs for errors. Consider using alternative DNS servers or implementing DNS server redundancy to improve reliability.

---

4. Potential Subdomain Takeover

Severity: MEDIUM **Tool:** Subfinder

Description:

If any of the subdomains (pay.sarral.io, www.pay.sarral.io, sophie.sarral.io) are pointing to a service that is no longer in use or has been decommissioned (e.g., a defunct cloud service), an attacker could claim the subdomain and host malicious content, potentially leading to phishing or data theft.

Remediation:

Regularly audit DNS records to ensure they point to active and properly configured services. Implement subdomain verification mechanisms with cloud providers to prevent unauthorized takeover. Monitor for dangling DNS records.

---

5. Exposed Internal Services

Severity: MEDIUM **Tool:** Subfinder

Description:

Subdomains like 'pay.sarral.io' and 'sophie.sarral.io' might expose internal services or applications to the public internet. This could allow attackers to discover sensitive information or exploit vulnerabilities in these services.

Remediation:

Implement strict access control policies and network segmentation to limit access to internal services. Ensure all services are properly secured with strong authentication and authorization mechanisms. Regularly scan for open ports and vulnerabilities.

6. Exposed 'pay' Subdomain

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'pay.sarral.io' suggests a payment processing function. If not properly secured, it could be vulnerable to attacks targeting sensitive financial data, such as credit card information or transaction details. This subdomain should be hardened and regularly audited.

Remediation:

Implement strong security measures on 'pay.sarral.io', including encryption (HTTPS), robust access controls, regular security audits, and PCI DSS compliance if applicable. Ensure all software and libraries used by the subdomain are up-to-date with the latest security patches.

7. 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 to protect against known exploits. Ubuntu 3ubuntu13.11 may also have its own specific vulnerabilities.

Remediation:

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

8. Outdated Apache Version

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

Description:

Apache httpd 2.4.58, while not ancient, may contain known vulnerabilities. Keeping Apache up-to-date is essential for security. The specific Ubuntu version should also be considered for distribution-specific patches.

Remediation:

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

9. Outdated Apache Version

Severity: MEDIUM **Tool:** WhatWeb

Description:

The server is running Apache version 2.4.58. While not immediately vulnerable, older versions of Apache may contain known security vulnerabilities that could be exploited by attackers. It's crucial to verify if this specific version has any known vulnerabilities.

Remediation:

Check for known vulnerabilities associated with Apache 2.4.58. If vulnerabilities exist, upgrade to the latest stable version of Apache or apply relevant security patches provided by the Apache project or Ubuntu.

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. Privacy Concerns due to Domains By Proxy

Severity: LOW **Tool:** Whois

Description:

The domain is registered using Domains By Proxy, which obscures the actual owner's contact information. While this enhances privacy, it can complicate incident response and legal inquiries if malicious activity originates from the domain.

Remediation:

Consider the trade-offs between privacy and transparency. If transparency is required, update the registration information with accurate contact details. Ensure that internal policies and procedures are in place to handle legal requests for owner information.

12. Misconfigured DNS Records

Severity: LOW **Tool:** Subfinder

Description:

Incorrectly configured DNS records can lead to various issues, including email spoofing, denial-of-service attacks, and redirection to malicious websites.

Remediation:

Regularly review and validate DNS records for accuracy and consistency. Implement DNSSEC to protect against DNS spoofing and cache poisoning attacks. Use a DNS monitoring service to detect and alert on any anomalies.

13. General Subdomain Takeover Risk

Severity: LOW **Tool:** Amass Passive

Description:

Each subdomain represents a potential attack surface. If any of these subdomains are pointing to inactive or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage), they could be vulnerable to subdomain takeover attacks. An attacker could claim the subdomain and use it for malicious purposes, such as phishing or distributing malware.

Remediation:

Regularly audit DNS records and associated services for all subdomains. Ensure that all subdomains are actively used and properly configured. Implement preventative measures against subdomain takeovers, such as verifying ownership of cloud resources and setting up monitoring alerts.

---

14. Target Unreachable/Non-Existent

Severity: LOW **Tool:** Assetfinder

Description:

The target domain might be unreachable due to network issues, DNS resolution problems, or the domain simply not existing. This prevents any vulnerability assessment.

Remediation:

Confirm the target domain is valid and resolves to a valid IP address. Use tools like `ping` or `nslookup` to verify reachability and DNS resolution. If the domain is invalid, correct the target and rerun the scan.

---

15. Exposed HTTP Service

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

Description:

The presence of an HTTP service (port 80) alongside HTTPS (port 443) may indicate that HTTP traffic is not being redirected to HTTPS. This can lead to man-in-the-middle attacks and exposure of sensitive data transmitted over HTTP.

Remediation:

Configure the web server to redirect all HTTP traffic to HTTPS. Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS connections.

16. Default Apache Configuration

Severity: LOW

Tool: Nmap Top 1000

Description:

The scan identifies the Apache version and OS. Default Apache configurations often contain unnecessary modules and information disclosure vulnerabilities. Attackers can leverage this information to fingerprint the server and identify potential weaknesses.

Remediation:

Review and harden the Apache configuration. Disable unnecessary modules, configure proper access controls, and remove or obfuscate server version information.

17. Information Disclosure: Server Version

Severity: LOW

Tool: WhatWeb

Description:

The scan reveals the specific version of Apache being used (2.4.58) and the underlying operating system (Ubuntu Linux). This information can be used by attackers to target known vulnerabilities specific to this software stack.

Remediation:

Configure Apache to suppress the server version and operating system information in HTTP headers. This can be achieved by modifying the `ServerTokens` and `ServerSignature` directives in the Apache configuration file (e.g., `httpd.conf` or `apache2.conf`). Set `ServerTokens Prod` and `ServerSignature Off`.

18. Domain Status: Prohibited Actions

Severity: INFO

Tool: Whois

Description:

The domain status flags (clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited) indicate that the domain owner has taken steps to prevent unauthorized deletion, renewal, transfer, or updates. This is a positive security measure.

Remediation:

These statuses are generally good practice and should be maintained unless there is a specific reason to change them. Regularly review these statuses to ensure they align with the organization's security policies.

19. Registrar Abuse Contact

Severity: INFO **Tool:** Whois

Description:

The presence of a registrar abuse contact email and phone number is standard and allows for reporting of abuse related to the domain.

Remediation:

Ensure that the abuse contact information is readily available and that internal procedures are in place to respond to abuse reports promptly.

20. Lack of HTTPS on Subdomains

Severity: INFO **Tool:** Subfinder

Description:

While not directly a vulnerability, the absence of HTTPS on subdomains like 'sophie.sarral.io' can expose user data transmitted over these subdomains to eavesdropping and man-in-the-middle attacks.

Remediation:

Implement HTTPS on all subdomains using TLS certificates. Enforce HTTPS redirection to ensure all traffic is encrypted. Use HSTS to instruct browsers to always connect to the subdomain over HTTPS.

21. Lack of Security Headers

Severity: INFO **Tool:** Amass Passive

Description:

The passive scan doesn't reveal the presence or absence of security headers. However, it's crucial to ensure that all subdomains are configured with appropriate security headers (e.g., Content-Security-Policy, Strict-Transport-Security, X-Frame-Options) to mitigate common web application attacks.

Remediation:

Implement and configure security headers on all subdomains. Regularly review and update the header configurations to address emerging threats. Use tools like securityheaders.com to verify the effectiveness of the implemented headers.

---

22. Potential Scan Configuration Issue

Severity: INFO **Tool:** Assetfinder

Description:

Assetfinder returned no domains, suggesting a possible misconfiguration or network connectivity problem preventing the tool from identifying subdomains. This could lead to a false sense of security if vulnerabilities exist but are not being discovered.

Remediation:

Verify the target domain is correct, ensure Assetfinder is properly configured with API keys (if required), and check network connectivity to the target. Rerun the scan after confirming these aspects.

---

23. MySQL Port Exposure (Closed)

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

Description:

Although the MySQL port (3306) is closed, its presence in the scan results suggests that MySQL might be installed on the server. Even if closed, it's good practice to ensure it's not externally accessible unless absolutely necessary. A closed port can still be probed for information.

Remediation:

If MySQL is not intended to be accessed externally, ensure that the firewall is configured to block all external connections to port 3306. If external access is required, implement strong authentication and access control measures.

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: 2025-11-26T10:16:16Z <<< 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 ;; communications error to 10.77.145.30#53: timed out ;;
communications error to 10.77.145.30#53: timed out ;; communications error to
10.77.145.30#53: timed out
```

Tool: Subfinder

```
__ _____ __ _______ __/ /_ / __(_)___ ____/ /__ _____ / ___/ / / / __ \/ /_/ / __ \/ __
/ _ \/ ___/ (__ ) /_/ / /_/ / __/ / / / / /_/ / __/ / /____/\__,_/_.___/_/ /_/_/
/_/\__,_/\___/_/ projectdiscovery.io [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 2 seconds 720
milliseconds sophie.sarral.io pay.sarral.io www.pay.sarral.io
```

Tool: Amass Passive

```
pay.sarral.io www.pay.sarral.io sophie.sarral.io sarral.io www.sarral.io The
enumeration has finished Discoveries are being migrated into the local database
```

Tool: Assetfinder

```
```

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 05:17 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 45.69 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

```
__ __ __ _ __ / /_ / /_/ /_____ | |/ / / __ \/ __/ __/ __ \| / / / / / /_/ /_/ /_/ / |
/_/ /_/\__/\__/ .___/_/|_| /_/ 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.
```