SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 28, 2025
Scan ID: 55

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **sarral.io** on 2025-11-28. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	1
Medium	6
Low	6
Info	4

2. Detailed Findings

1. Unknown Vulnerability

Severity: HIGH **Tool:** WebScraperRecon

Description:

The 'pay.sarral.io' subdomain experiences read timeouts and returns a 404 Not Found error. This indicates a potential misconfiguration, service outage, or that the payment service is not properly deployed. This could lead to a denial of service for payment processing and potential loss of revenue. The timeout errors suggest network connectivity issues or an overloaded server.

Remediation:

No mitigation provided.

2. Unknown Vulnerability

Severity: MEDIUM **Tool:** Whois

Description:

The domain's DNSSEC record is unsigned, meaning that DNS Security Extensions are not enabled. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks. Attackers could potentially redirect users to malicious websites by manipulating DNS records.

Remediation:

No mitigation provided.

3. Unknown Vulnerability

Severity: MEDIUM **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 due to hardware failure, network issues, or a DDoS attack, the website and any services associated with the domain will be inaccessible. This lack

of redundancy can lead to significant downtime and business disruption.

Remediation:

No mitigation provided.

4. Unknown Vulnerability

Severity: MEDIUM **Tool:** Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment gateway or related services are hosted on these subdomains. If not properly secured, these subdomains could be vulnerable to attacks such as man-in-the-middle attacks, cross-site scripting (XSS), or SQL injection, potentially leading to unauthorized access to sensitive payment information or fraudulent transactions.

Remediation:

No mitigation provided.

5. Unknown Vulnerability

Severity: MEDIUM **Tool:** Amass Passive

Description:

The discovery of 'pay.sarral.io' and 'www.pay.sarral.io' indicates the existence of a payment gateway. Payment gateways are critical components that handle sensitive financial data. Without further investigation, it's impossible to determine if the gateway is properly secured. Potential vulnerabilities could include insecure configurations, outdated software, lack of proper access controls, or susceptibility to common web application attacks (e.g., SQL injection, XSS).

Remediation:

No mitigation provided.

6. Unknown Vulnerability

Severity: MEDIUM **Tool:** Assetfinder

Description:

The Assetfinder scan only provides the domain name. Without further investigation, the services and applications running on the domain are unknown. These services may contain vulnerabilities that could be exploited by attackers. This includes outdated software, misconfigurations, and known security flaws.

Remediation:

No mitigation provided.

7. Unknown Vulnerability

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The main domain (sarral.io) and its 'www' subdomain are missing crucial security headers such as HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. This absence makes the website vulnerable to various attacks, including Cross-Site Scripting (XSS), Clickjacking, and Man-in-the-Middle (MitM) attacks.

Remediation:

No mitigation provided.

8. Unknown Vulnerability

Severity: LOW **Tool:** NSLookup

Description:

The NSLookup output doesn't explicitly confirm the presence of DNSSEC records. DNSSEC (Domain Name System Security Extensions) helps prevent DNS spoofing and cache poisoning attacks by digitally signing DNS records. Without DNSSEC, attackers could potentially redirect users to malicious websites by manipulating DNS responses.

Remediation:

No mitigation provided.

9. Unknown Vulnerability

Severity: LOW **Tool:** Subfinder

Description:

The existence of multiple subdomains ('sophie.sarral.io', 'pay.sarral.io', 'www.pay.sarral.io', 'www.sarral.io') increases the attack surface and the potential for subdomain takeover. If any of these subdomains are pointing to non-existent or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage accounts, GitHub Pages), an attacker could claim the subdomain and use it for malicious purposes, such as phishing or distributing malware.

Remediation:

No mitigation provided.

10. Unknown Vulnerability

Severity: LOW **Tool:** Amass Passive

Description:

While not directly a vulnerability, the enumeration of these domains highlights the importance of proper domain management. If any of these domains are not actively monitored or properly configured (e.g., pointing to non-existent servers), they could be susceptible to domain takeover attacks. An attacker could potentially hijack the domain and use it for malicious purposes, such as phishing or distributing malware.

Remediation:

No mitigation provided.

11. Unknown Vulnerability

Severity: LOW **Tool:** Assetfinder

Description:

The Assetfinder scan doesn't provide information about security headers. The absence of security headers like Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), and X-Frame-Options can leave the domain vulnerable to client-side attacks such as Cross-Site Scripting (XSS) and clickjacking.

Remediation:

No mitigation provided.

---

12. Unknown Vulnerability

Severity: LOW **Tool:** WebScraperRecon

Description:

The 'sophie.sarral.io' subdomain contains a large number of phone numbers, many of which appear to be test data or placeholders (e.g., '0 0 0 9999', '0123456789', '1 1 0 0 1 0-1'). While these may not be real numbers, their presence could indicate a lack of proper data sanitization or a development environment exposed to the public. The presence of numbers like '465794806718' and '7019607843' should be investigated to ensure they are not real and sensitive.

Remediation:

No mitigation provided.

---

13. Unknown Vulnerability

Severity: LOW **Tool:** WebScraperRecon

Description:

The scan reports NameResolutionError for www.pay.sarral.io, indicating that the domain name could not be resolved to an IP address. While the scan also shows that pay.sarral.io resolves to an IP, the failure of www.pay.sarral.io could indicate a DNS configuration issue or a missing DNS record. This can lead to users being unable to access the payment subdomain using the 'www' prefix.

Remediation:

No mitigation provided.

14. Unknown Vulnerability

Severity: INFO **Tool:** Whois

Description:

The domain uses a privacy service (Domains By Proxy, LLC) to mask the actual registrant information. While legitimate, this can be abused by malicious actors to hide their identity and make it difficult to trace them in case of illegal activities or abuse. It also makes direct communication with the domain owner challenging.

Remediation:

No mitigation provided.

15. Unknown Vulnerability

Severity: INFO **Tool:** Whois

Description:

The domain is registered with GoDaddy. While GoDaddy is a reputable registrar, it's important to stay informed about any security incidents or vulnerabilities specific to their platform. Past incidents have shown that registrar accounts can be targeted, potentially leading to domain hijacking.

Remediation:

No mitigation provided.

16. Unknown Vulnerability

Severity: INFO **Tool:** Assetfinder

Description:

The Assetfinder scan only identified the root domain 'sarral.io'. A more comprehensive subdomain enumeration could reveal additional subdomains and associated services that may be vulnerable. Without a complete picture of the attack surface, it's impossible to assess the full range of potential risks.

Remediation:

No mitigation provided.

---

17. Unknown Vulnerability

Severity: INFO **Tool:** WebScraperRecon

Description:

The 'pay.sarral.io' subdomain has a Content Security Policy (CSP) that allows framing from 'https://online-order.godaddy.com'. This may be unexpected and could potentially be exploited if the GoDaddy domain is compromised or if there's a vulnerability in how the framing is handled. It's important to verify if this is intentional and necessary.

Remediation:

No mitigation provided.

---

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: 2025-11-28T09:32:01Z <<<

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
pay.sarral.io
[INF] Found 4 subdomains for sarral.io in 21 seconds 418 milliseconds
www.pay.sarral.io
www.sarral.io
sophie.sarral.io
```

Tool: Amass Passive

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

The enumeration has finished
Discoveries are being migrated into the local database
```

Tool: Assetfinder

```
sarral.io
```

Tool: WebScraperRecon


```
{"www.pay.sarral.io": {"target": "www.pay.sarral.io", "base_url":
"https://www.pay.sarral.io", "alive": false, "pages_visited": 0, "max_depth": 2,
"emails": [], "phones": [], "internal_ips": [], "social_profiles": [], "api_endpoints":
[], "comments": [], "visited_urls": [], "errors": ["[probe] https://www.pay.sarral.io
-> HTTPSConnectionPool(host='www.pay.sarral.io', port=443): Max retries exceeded with
url: / (Caused by NameResolutionError(\"<urllib3.connection.HTTPSConnection object at
0x7f694b72d6d0>: Failed to resolve 'www.pay.sarral.io' ([Errno -2] Name or service not
known)\"))", "[probe] https://www.pay.sarral.io ->
HTTPSConnectionPool(host='www.pay.sarral.io', port=443): Max retries exceeded with url:
/ (Caused by NameResolutionError(\"<urllib3.connection.HTTPSConnection object at
0x7f694b72d950>: Failed to resolve 'www.pay.sarral.io' ([Errno -2] Name or service not
known)\"))", "[probe] http://www.pay.sarral.io ->
HTTPConnectionPool(host='www.pay.sarral.io', port=80): Max retries exceeded with url: /
(Caused by NameResolutionError(\"<urllib3.connection.HTTPConnection object at
0x7f694b771a90>: Failed to resolve 'www.pay.sarral.io' ([Errno -2] Name or service not
known)\"))"], "duration_sec": 0.71, "resolved_ips": ["159.89.216.111"], "http_probe":
{}, "tls_info": {}, "headers": {}, "security_headers": {}, "favicon_hash": {},
"technologies": [], "waf": "", "http_methods": []}, "sophie.sarral.io": {"target":
"sophie.sarral.io", "base_url": "https://sophie.sarral.io", "alive": true,
"pages_visited": 4, "max_depth": 2, "emails": [], "phones": ["0 0 0 9999", "0 0 12 12",
"0 0 16 16", "0 0 20 20", "0 0 30 30", "0 0 512 512", "0009765625", "0123456789", "1 1 0
0 1 0-1", "1 1 0 0 1 1", "1 1 0 0 1-1", "1 1 0 1 1 1", "134217727", "134217728", "2 5 6
```

```
6 6-6", "201326741", "2147483647", "2147483648", "2147483649", "268435456", "28-1 0 0
-1 512 512", "29-1315-4923-9", "311 16 235", "311 16 267", "4294967295", "4294967296",
"4294967297", "465794806718", "5 0 0 1 0", "536870912", "536870913", "6 10 3 3 6-6",
"6103515625", "7019607843", "7760674-9", "8571428571"], "internal_ips": [],
"social_profiles": ["https://github.com/coreui/coreui-chartjs/blob/main/LICENSE)",
"https://github.com/coreui/coreui-free-react-admin-template/blob/main/LICENSE)",
"https://github.com/coreui/coreui/blob/main/LICENSE)",
"https://github.com/zloirock/core-js",
"https://github.com/zloirock/core-js/blob/v3.45.1/LICENSE"], "api_endpoints": [],
"comments": ["* Sarral Template\n* @version v5.5.0\n* @link
https://coreui.io/product/free-react-admin-template/\n* Copyright (c) 2025 creativeLabs
Å■ukasz Holeczek\n* Licensed under MIT
(https://github.com/coreui/coreui-free-react-admin-template/blob/main/LICENSE)", "built
files will be auto injected"], "visited_urls":
["http://sophie.sarral.io/assets/index-BitQyrv4.js",
"http://sophie.sarral.io/assets/index-C8P3A5wp.css",
"http://sophie.sarral.io/manifest.json", "https://sophie.sarral.io"], "errors":
["[probe] https://sophie.sarral.io -> HTTPSConnectionPool(host='sophie.sarral.io',
port=443): Max retries exceeded with url: / (Caused by
NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f694b72d590>:
Failed to establish a new connection: [Errno 111] Connection refused'))", "[probe]
https://sophie.sarral.io -> HTTPSConnectionPool(host='sophie.sarral.io', port=443): Max
retries exceeded with url: / (Caused by
NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f694b72e490>:
Failed to establish a new connection: [Errno 111] Connection refused'))"],
"duration_sec": 9.11, "resolved_ips": ["159.89.216.111"], "http_probe": {"initial_url":
"http://sophie.sarral.io", "final_url": "http://sophie.sarral.io/", "status_code": 200,
"content_length": 1190, "redirect_chain": ["http://sophie.sarral.io/"]}, "tls_info":
{}, "headers": {"Server": "nginx/1.18.0 (Ubuntu)", "Date": "Fri, 28 Nov 2025 09:33:25
GMT", "Content-Type": "text/html", "Last-Modified": "Thu, 06 Nov 2025 06:52:17 GMT",
"Transfer-Encoding": "chunked", "Connection": "keep-alive", "ETag":
"W/\"690c45a1-4a6\"", "Content-Encoding": "gzip"}, "security_headers": {"hsts": null,
"csp": null, "x_frame_options": null, "x_content_type_options": null,
"referrer_policy": null, "permissions_policy": null, "x_xss_protection": null},
"favicon_hash": {"url": "http://sophie.sarral.io/favicon.ico", "md5":
"22e6c3956309a5dfabed53ff62f76e91", "sha1": "5ea09a9d8a03d3ad990eb14dfd4d1b16b544e5ab",
"sha256": "e0aebdef7da8bc36dfdad3ceaf5a45c0aa5141cf5737603553ffdfebf4790d08"},
"technologies": ["Nginx", "React"], "waf": "", "http_methods": ["", "TRACE"]},
"sarral.io": {"target": "sarral.io", "base_url": "https://sarral.io", "alive": true,
"pages_visited": 38, "max_depth": 2, "emails": ["Info@sarral.io", "info@sarral.io"],
"phones": ["303035 100"], "internal_ips": [], "social_profiles":
["http://github.com/davist11/jQuery-One-Page-Nav",
"https://github.com/w3c/IntersectionObserver/tree/master/polyfill",
"https://www.linkedin.com/company/sarral", "
...[Truncated]
```