SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 27, 2025
Scan ID: 50

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **sarral.io** on 2025-11-27. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	2
Medium	14
Low	9
Info	5

2. Detailed Findings

1. Misconfigured Payment Gateway (pay.sarral.io)

Severity: HIGH **Tool:** Amass Passive

Description:

The subdomain 'pay.sarral.io' suggests a payment gateway. If this gateway is not properly secured, it 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 financial data.

Remediation:

Conduct a thorough security audit of the 'pay.sarral.io' subdomain, including penetration testing and vulnerability scanning. Ensure that the payment gateway is PCI DSS compliant and that all security best practices are followed, including proper encryption, input validation, and access controls.

---

2. Vulnerability in 'pay' subdomain

Severity: HIGH **Tool:** Assetfinder

Description:

The 'pay.sarral.io' subdomain, likely handling payment information, is a high-value target. Any vulnerabilities in this subdomain could lead to financial data breaches, fraud, and reputational damage. This subdomain should be prioritized for security testing.

Remediation:

Conduct thorough penetration testing and vulnerability scanning of the 'pay.sarral.io' subdomain. Ensure that all payment processing components are PCI DSS compliant. Implement strong authentication and authorization mechanisms. Regularly review and update security protocols.

---

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 attackers can redirect users to malicious websites.

Remediation:

Enable DNSSEC for the domain through the registrar (GoDaddy). This involves generating DNSSEC keys and adding the appropriate records to the domain's DNS zone.

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. Potential Payment Processing Security Risks

Severity: MEDIUM **Tool:** Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment processing system. Without further investigation, it's impossible to determine specific vulnerabilities, but potential risks include insecure data storage, lack of proper encryption, and vulnerabilities in the payment processing software itself.

Remediation:

Conduct a thorough security audit of the payment processing system, including penetration testing and code review. Ensure PCI DSS compliance if applicable. Implement strong encryption for sensitive data both in transit and at rest. Keep all payment processing software up-to-date with the latest security patches.

6. Potential Subdomain Takeover

Severity: MEDIUM **Tool:** Amass Passive

Description:

Subdomains like 'sophie.sarral.io' might be pointing to inactive or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage, GitHub Pages). If these services are not properly configured or have been abandoned, 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 all subdomains point to active and properly configured services. Implement subdomain takeover prevention measures, such as verifying ownership of cloud resources associated with subdomains.

7. Exposed Development/Testing Environment (sophie.sarral.io)

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'sophie.sarral.io' could be a development or testing environment. If this environment is not properly secured, it could expose sensitive data, such as API keys, database credentials, or customer information. It could also provide an entry point for attackers to compromise the production environment.

Remediation:

Isolate development and testing environments from the production environment. Implement strong access controls and regularly audit the security of these environments. Remove any sensitive data from development and testing environments or use anonymized data.

8. Missing Security Headers on Subdomains

Severity: MEDIUM **Tool:** Assetfinder

Description:

Subdomains like 'pay.sarral.io' and 'sophie.sarral.io' might be missing crucial security headers (e.g., HSTS, X-Frame-Options, Content-Security-Policy). This can leave them vulnerable to attacks like clickjacking, cross-site scripting (XSS), and man-in-the-middle attacks.

Remediation:

Implement security headers on all subdomains. Use a tool like Mozilla Observatory to assess the current header configuration and identify missing or misconfigured headers. Ensure HSTS is enabled with includeSubDomains and preload directives.

9. Potential for Subdomain Takeover

Severity: MEDIUM **Tool:** Assetfinder

Description:

If any of these subdomains ('pay.sarral.io', 'sophie.sarral.io', 'www.pay.sarral.io') are pointing to inactive or misconfigured cloud services (e.g., AWS S3 bucket, Azure Blob Storage, GitHub Pages), they could be vulnerable to subdomain takeover. An attacker could claim the subdomain and host malicious content.

Remediation:

Regularly audit DNS records and cloud service configurations to ensure that all subdomains are pointing to active and properly configured resources. Remove or reconfigure any subdomains pointing to inactive services. Implement proper access controls on cloud resources.

10. Lack of SSL/TLS on all subdomains

Severity: MEDIUM **Tool:** Assetfinder

Description:

If any of the subdomains are not using HTTPS, communication between the user and the server is unencrypted, making it vulnerable to eavesdropping and man-in-the-middle attacks. Even if the main domain uses HTTPS, all subdomains should also be secured with SSL/TLS.

Remediation:

Ensure that all subdomains are configured to use HTTPS. Obtain and install SSL/TLS certificates for each subdomain. Enforce HTTPS redirection to ensure that all traffic is encrypted.

11. Missing Security Headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, X-XSS-Protection)

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The main domain (sarral.io and www.sarral.io) is missing several crucial security headers, including HSTS (HTTP Strict Transport Security), CSP (Content Security Policy), X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. This makes the website vulnerable to various attacks such as Man-in-the-Middle attacks, Cross-Site Scripting (XSS), and clickjacking.

Remediation:

Implement the missing security headers on the web server. Specifically: - HSTS: Configure the server to send the Strict-Transport-Security header to enforce HTTPS. - CSP: Define a Content Security Policy to restrict the sources of content the browser is allowed to load. - X-Frame-Options: Set the X-Frame-Options header to 'DENY' or 'SAMEORIGIN' to prevent clickjacking. - X-Content-Type-Options: Set the X-Content-Type-Options header to 'nosniff' to prevent MIME sniffing. - Referrer-Policy: Set the Referrer-Policy header to control how much referrer information is sent with requests. - Permissions-Policy: Set the Permissions-Policy header to control browser features. - X-XSS-Protection: While largely deprecated, consider setting X-XSS-Protection to '1; mode=block' for older browsers.

12. Potential Data Leak: Large Number of Phone Numbers on sophie.sarral.io

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The subdomain sophie.sarral.io contains a large number of phone numbers. This could be a data leak if these numbers are not intended to be publicly accessible or if they are sensitive in nature. Many of the phone numbers appear to be test data or placeholders.

Remediation:

Review the content of sophie.sarral.io and determine the purpose of the phone numbers. If they are not intended to be public, remove them or implement access controls. Sanitize the data to remove test data and placeholders.

13. Outdated OpenSSH Version

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

Description:

While OpenSSH 9.6p1 is relatively recent, it's crucial to ensure it's the absolute latest version and patched against known vulnerabilities. Older versions may contain exploitable flaws.

Remediation:

Upgrade OpenSSH to the latest available version and apply all security patches. Regularly monitor security advisories for OpenSSH.

14. Outdated Apache Version

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

Description:

Apache httpd 2.4.58, while not ancient, may have known vulnerabilities. Keeping Apache up-to-date is crucial for security.

Remediation:

Upgrade Apache httpd to the latest available version and apply all security patches. Regularly monitor security advisories for Apache.

15. 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.

---

16. Lack of Web Application Firewall (WAF)

Severity: MEDIUM **Tool:** WafW00f

Description:

The scan did not detect a WAF. A WAF provides a layer of security against common web application attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Without a WAF, the application is more vulnerable to these attacks.

Remediation:

Implement a WAF (either cloud-based or on-premise) and configure it with appropriate rulesets to protect against common web application attacks. Regularly update the WAF rulesets to address new threats.

---

17. 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.

18. Subdomain Takeover Risk

Severity: LOW **Tool:** Subfinder

Description:

If any of these subdomains are pointing to inactive or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage accounts, GitHub Pages), they could be vulnerable to subdomain takeover. An attacker could claim the inactive service and host malicious content on the subdomain.

Remediation:

Verify that all subdomains are actively used and properly configured. If a subdomain is no longer needed, remove the DNS record. For subdomains pointing to cloud services, ensure the service is properly configured and secured. Regularly audit DNS records to identify and remove unused or misconfigured entries.

19. Lack of Security Headers on www.sarral.io and sarral.io

Severity: LOW **Tool:** Amass Passive

Description:

The main domains 'www.sarral.io' and 'sarral.io' might be missing important security headers (e.g., Content Security Policy, HTTP Strict Transport Security, X-Frame-Options). This could make the website vulnerable to various attacks, such as cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks.

Remediation:

Implement security headers on 'www.sarral.io' and 'sarral.io' to mitigate common web application vulnerabilities. Regularly review and update these headers to ensure they are effective.

20. pay.sarral.io returns 404 Not Found

Severity: LOW **Tool:** WebScraperRecon

Description:

The subdomain pay.sarral.io returns a 404 Not Found error. This could indicate a misconfiguration, an abandoned service, or a broken link. It might expose sensitive information about the application structure.

Remediation:

Investigate the purpose of pay.sarral.io. If it's a valid service, ensure it's properly configured and accessible. If it's no longer needed, remove the DNS record to prevent confusion and potential exploitation.

21. TRACE Method Enabled

Severity: LOW **Tool:** WebScraperRecon

Description:

The TRACE HTTP method is enabled on pay.sarral.io, sophie.sarral.io, sarral.io and www.sarral.io. This method can be used in conjunction with Cross-Site Tracing (XST) attacks to steal cookies or other sensitive information.

Remediation:

Disable the TRACE HTTP method on the web server configuration. This can typically be done by modifying the AllowMethods directive in Apache or similar configurations in other web servers.

22. Default Apache Configuration

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

Description:

The scan indicates a standard Ubuntu Apache installation. Default configurations often contain unnecessary modules or settings that can be exploited. The version information disclosure itself can aid attackers.

Remediation:

Review and harden the Apache configuration. Disable unnecessary modules, restrict directory listing, and configure appropriate access controls. Consider removing the version information from server responses.

23. Information Disclosure: OS and Software Versions

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

Description:

The Nmap scan reveals the operating system (Linux) and specific versions of OpenSSH and Apache. This information can be used by attackers to identify known vulnerabilities specific to these versions.

Remediation:

Disable or minimize version information disclosure in server banners and headers. Implement security measures to prevent attackers from easily identifying the specific versions of software in use.

24. 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`.

25. HTTP Error Codes (404, 405, 403, 502, 500)

Severity: LOW **Tool:** WafW00f

Description:

The WafW00f output displays various HTTP error codes (404, 405, 403, 502, 500). These errors can indicate misconfiguration, resource unavailability, or potential security issues. While not directly exploitable, they can provide information to attackers or disrupt service.

Remediation:

Investigate the root cause of each error code. For 404 errors, ensure that requested resources exist and are accessible. For 405 errors, review allowed HTTP methods. For 403 errors, check permissions and access control. For 502 and 500 errors, investigate server-side issues and ensure proper resource allocation and error handling. Implement proper error logging and monitoring to quickly identify and resolve these issues.

---

26. Privacy Protection Enabled

Severity: INFO **Tool:** Whois

Description:

The registrant information is hidden using a privacy service (Domains By Proxy, LLC). While this protects the registrant's personal information, it can also make it difficult to identify the true owner of the domain in case of abuse or legal issues.

Remediation:

While not a vulnerability per se, consider the implications of using a privacy service. Ensure that contact information is still accessible through the registrar in case of legitimate inquiries. This is more of an awareness item than a direct mitigation.

---

27. Standard Domain Status Locks

Severity: INFO **Tool:** Whois

Description:

The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited status codes set. These are standard security measures to prevent unauthorized changes to the domain registration.

Remediation:

These status codes are generally beneficial and should remain enabled unless there is a specific reason to disable them. No action is required unless a legitimate change is needed, in which case the locks must be temporarily removed.

---

28. Information Disclosure via Subdomain Enumeration

Severity: INFO **Tool:** Subfinder

Description:

The enumeration of subdomains itself can provide attackers with valuable information about the organization's infrastructure and services. This information can be used to target specific systems or identify potential attack vectors.

Remediation:

Implement proper access controls and security measures on all subdomains. Regularly monitor for unauthorized access attempts. Consider using a Content Security Policy (CSP) to restrict the sources from which the website can load resources, mitigating the impact of potential cross-site scripting (XSS) attacks.

---

29. DNS Resolution Failure for www.pay.sarral.io

Severity: INFO **Tool:** WebScraperRecon

Description:

The subdomain www.pay.sarral.io is not resolving, indicating a potential DNS configuration issue. This prevents users from accessing the service and could be a sign of a larger problem.

Remediation:

Verify the DNS configuration for www.pay.sarral.io and ensure that the A record is correctly pointing to the server's IP address. If the service is no longer needed, remove the DNS record.

30. MySQL Port Closed but Present

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

Description:

The MySQL port (3306) is closed, but the fact that it's present suggests MySQL is installed. This could indicate a misconfiguration or a potential attack surface if the service is unintentionally exposed in the future.

Remediation:

If MySQL is not required, uninstall it. If it is required, ensure it is properly secured, bound to a specific interface (e.g., localhost), and protected by a strong password. Regularly audit the firewall rules to ensure the port remains closed to external access if that is the intention.

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: 2025-11-27T10:04:07Z <<< 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 460 milliseconds sophie.sarral.io pay.sarral.io www.pay.sarral.io
```

Tool: Amass Passive

```
www.sarral.io sarral.io sophie.sarral.io pay.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: 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(\": 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(\": 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(\": Failed to resolve 'www.pay.sarral.io' ([Errno -2]
Name or service not known)\"))"], "duration_sec": 0.55, "resolved_ips":
["159.89.216.111"], "http_probe": {}, "tls_info": {}, "headers": {},
"security_headers": {}, "favicon_hash": {}, "technologies": [], "waf": "",
"http_methods": []}, "pay.sarral.io": {"target": "pay.sarral.io", "base_url":
"https://pay.sarral.io", "alive": true, "pages_visited": 1, "max_depth": 2, "emails":
[], "phones": [], "internal_ips": [], "social_profiles": [], "api_endpoints": [],
"comments": ["TODO: replace with variable/translation for this", "TODO: replace this
```

```
with stylesheet from this repo", "TODO: replace with variable/translation for this",
"TODO: replace with variable/translation for this"], "visited_urls":
["https://pay.sarral.io"], "errors": [], "duration_sec": 6.58, "resolved_ips":
["159.89.216.111"], "http_probe": {"initial_url": "https://pay.sarral.io", "final_url":
"https://pay.sarral.io/", "status_code": 404, "content_length": 1211, "redirect_chain":
["https://pay.sarral.io/"]}, "tls_info": {"hostname": "pay.sarral.io", "issuer":
"countryName=US, stateOrProvinceName=Arizona, localityName=Scottsdale,
organizationName=GoDaddy.com, Inc.,
organizationalUnitName=http://certs.godaddy.com/repository/, commonName=Go Daddy Secure
Certificate Authority - G2", "subject": "commonName=pay.sarral.io", "not_before": "Aug
14 15:09:48 2025 GMT", "not_after": "Sep 12 23:25:23 2026 GMT", "san": ["pay.sarral.io",
"www.pay.sarral.io"]}, "headers": {"date": "Thu, 27 Nov 2025 10:05:16 GMT",
"content-type": "text/html; charset=utf-8", "transfer-encoding": "chunked",
"connection": "close", "vary": "Origin, Accept-Encoding",
"access-control-allow-credentials": "true", "access-control-expose-headers":
"X-Trace-Id", "x-trace-id": "c81ecf717a0e271770390db855b9d449",
"content-security-policy": "frame-ancestors 'self' https://online-order.godaddy.com",
"etag": "W/\"4bb-N3Oyyq8QVbNLPTrykAbDNz6IO/0\"", "content-encoding": "gzip"},
"security_headers": {"hsts": null, "csp": "frame-ancestors 'self'
https://online-order.godaddy.com", "x_frame_options": null, "x_content_type_options":
null, "referrer_policy": null, "permissions_policy": null, "x_xss_protection": null},
"favicon_hash": {}, "technologies": [], "waf": "", "http_methods": ["", "TRACE"]},
"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", "86-1015-4956-8730"], "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] ht ...[Truncated]
```


Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 05:05 EST Nmap scan report for
sarral.io (159.89.216.111) Host is up (0.074s 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 43.25 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

```
______ / \ ( W00f! ) \ ____/ ,, __ 404 Hack Not Found |`-.__ / / __ __ /" _/ /_/ \ \ / /
*===* / \ \_/ / 405 Not Allowed / )__// \ / /| / /---` 403 Forbidden \\/` \ | / _ \ `\
/_\\_ 502 Bad Gateway / / \ \ 500 Internal Error `_____``-` /_/ \_\\ ~ 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
```