SECURITY ASSESSMENT REPORT

Target: sarral.io
Date: November 27, 2025
Scan ID: 51

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	11
Info	8

2. Detailed Findings

1. Exposed 'pay' Subdomains

Severity: HIGH

Tool: Subfinder

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' indicates potential payment processing functionality. These subdomains are prime targets for attackers seeking to intercept or manipulate financial transactions. Lack of proper security measures on these subdomains could lead to data breaches and financial losses.

Remediation:

Implement robust security measures on all 'pay' subdomains, including strong authentication, encryption (HTTPS), regular security audits, and penetration testing. Ensure compliance with relevant payment card industry (PCI) standards if applicable. Implement rate limiting and input validation to prevent abuse.

2. Insecure 'pay' Subdomain

Severity: HIGH

Tool: Assetfinder

Description:

The 'pay.sarral.io' and 'www.pay.sarral.io' subdomains likely handle sensitive payment information. If not properly secured, they could be vulnerable to various attacks, including cross-site scripting (XSS), SQL injection, and man-in-the-middle (MITM) attacks, potentially leading to data breaches and financial loss.

Remediation:

Conduct a thorough security assessment of the 'pay' subdomain, including penetration testing and code review. Implement strong input validation, output encoding, and parameterized queries to prevent injection attacks. Enforce HTTPS with a valid SSL/TLS certificate and implement HSTS to prevent MITM attacks. Ensure compliance with relevant payment card industry (PCI) standards.

3. 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.

4. Subdomain Takeover Potential

Severity: MEDIUM

Tool: Subfinder

Description:

If any of the subdomains (sophie.sarral.io, pay.sarral.io, www.sarral.io, www.pay.sarral.io) are pointing to inactive or misconfigured cloud services (e.g., AWS S3 bucket, Azure Blob Storage, GitHub Pages), an attacker could potentially claim the subdomain and host malicious content, leading to phishing attacks or reputational damage.

Remediation:

Regularly audit DNS records and ensure that all subdomains point to active and properly configured services. Implement subdomain takeover prevention measures, such as verifying ownership of cloud resources associated with subdomains.

5. Potential for Subdomain Takeover

Severity: MEDIUM

Tool: Amass Passive

Description:

If any of the subdomains (sophie.sarral.io, pay.sarral.io, www.sarral.io, www.pay.sarral.io) are pointing to inactive or misconfigured cloud services (e.g., AWS S3 buckets, Azure Storage accounts, Heroku apps), they could be vulnerable to subdomain takeover attacks.

Remediation:

Verify that all subdomains are actively used and properly configured. Regularly audit DNS records and cloud service configurations to identify and remediate any potential subdomain takeover vulnerabilities. Implement preventative measures like DNS record monitoring and automated configuration checks.

6. Exposure of 'pay' Subdomain

Severity: MEDIUM **Tool:** Amass Passive

Description:

The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment processing system. This subdomain is a high-value target for attackers seeking to steal financial data.

Remediation:

Prioritize security assessments of the 'pay' subdomain. Ensure that it adheres to PCI DSS standards (if applicable) and implements robust security controls, including encryption, access controls, and intrusion detection systems. Regularly monitor for suspicious activity and implement strong authentication mechanisms.

7. Subdomain Takeover Potential

Severity: MEDIUM **Tool:** Assetfinder

Description:

If any of the subdomains (sophie.sarral.io, pay.sarral.io, www.pay.sarral.io) are pointing to inactive or misconfigured cloud services (e.g., AWS S3 bucket, Azure Blob Storage, Heroku app), they could be vulnerable to subdomain takeover. An attacker could claim the inactive service and host malicious content, potentially phishing users or damaging the organization's reputation.

Remediation:

Verify that all subdomains are actively pointing to valid and properly configured services. Regularly audit DNS records and cloud service configurations to identify and remove dangling DNS entries. Implement proper access controls and security configurations for all cloud services.

8. Vulnerable Third-Party Libraries

Severity: MEDIUM **Tool:** Assetfinder

Description:

The scan doesn't provide information about the libraries used. The domains and subdomains might be using outdated or vulnerable third-party libraries (e.g., JavaScript libraries, frameworks) which could introduce security vulnerabilities.

Remediation:

Perform a software composition analysis (SCA) to identify and assess the security risks associated with third-party libraries used on the domains and subdomains. Regularly update libraries to the latest versions to patch known vulnerabilities.

9. Missing Security Headers (HSTS)

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The HSTS (HTTP Strict Transport Security) header is missing on www.sarral.io and sarral.io. This allows man-in-the-middle attackers to downgrade HTTPS connections to HTTP, potentially exposing sensitive data.

Remediation:

Implement the HSTS header on the web server configuration. Ensure the 'max-age' directive is set appropriately (e.g., one year) and consider including 'includeSubDomains' and 'preload' directives.

10. Missing Security Headers (CSP)

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The Content Security Policy (CSP) header is missing on www.sarral.io and sarral.io. CSP helps prevent cross-site scripting (XSS) attacks by defining the sources from which the browser is allowed to load resources.

Remediation:

Implement a restrictive CSP header that only allows resources from trusted sources. Carefully define the 'default-src', 'script-src', 'style-src', 'img-src', and other directives based on the application's requirements.

11. www.pay.sarral.io DNS Resolution Failure

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The www.pay.sarral.io subdomain is failing to resolve to an IP address. This indicates a DNS configuration issue that prevents users from accessing the service.

Remediation:

Verify the DNS records for www.pay.sarral.io and ensure they are correctly configured to point to the appropriate IP address. Check for any typos or errors in the DNS settings.

12. Outdated OpenSSH Version

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

Description:

The server is running OpenSSH 9.6p1. While not immediately vulnerable, older versions of OpenSSH may contain known security vulnerabilities that could be exploited by attackers. It's crucial to stay up-to-date with security patches.

Remediation:

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

13. Outdated Apache HTTPd Version

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

Description:

The server is running Apache HTTPd 2.4.58. Older versions of Apache HTTPd may contain known security vulnerabilities that could be exploited by attackers. It's crucial to stay up-to-date with security patches.

Remediation:

Upgrade Apache HTTPd to the latest stable version available for the Ubuntu distribution. Regularly check for and apply security updates. Review Apache configuration for best practices.

---

14. 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.

---

15. 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.

16. 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.

17. Reliance on Third-Party Registrar (GoDaddy)

Severity: LOW **Tool:** Whois

Description:

The domain's reliance on GoDaddy as the registrar introduces a potential supply chain risk. A compromise of GoDaddy's systems could potentially impact the domain's availability or control.

Remediation:

Implement strong account security measures with the registrar, including multi-factor authentication. Regularly review registrar security policies and consider diversifying registrar relationships for critical assets.

18. DNS Reliance on Registrar's Name Servers

Severity: LOW **Tool:** Whois

Description:

The domain uses GoDaddy's name servers (ns63.domaincontrol.com, ns64.domaincontrol.com). A compromise or outage affecting these name servers could disrupt domain resolution and website availability.

Remediation:

Consider using a geographically diverse and highly available DNS provider, potentially independent of the registrar. Implement DNSSEC for enhanced security and integrity of DNS records.

19. 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.

20. Lack of Security Headers

Severity: LOW **Tool:** Assetfinder

Description:

The scan doesn't provide information about security headers. The absence of security headers like Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), X-Frame-Options, and X-XSS-Protection can make the website more vulnerable to various attacks.

Remediation:

Implement security headers on all domains and subdomains. Configure CSP to restrict the sources of content that the browser is allowed to load. Enable HSTS to enforce HTTPS connections. Set X-Frame-Options to prevent clickjacking attacks. Configure X-XSS-Protection to enable the browser's built-in XSS filter.

21. Missing Security Headers (X-Frame-Options)

Severity: LOW **Tool:** WebScraperRecon

Description:

The X-Frame-Options header is missing on www.sarral.io and sarral.io. This header helps prevent clickjacking attacks by controlling whether the site can be embedded in an iframe.

Remediation:

Implement the X-Frame-Options header with a value of 'DENY' or 'SAMEORIGIN', depending on whether the site needs to be framed by other sites within the same domain.

22. Missing Security Headers (X-Content-Type-Options)

Severity: LOW **Tool:** WebScraperRecon

Description:

The X-Content-Type-Options header is missing on www.sarral.io and sarral.io. This header prevents MIME-sniffing vulnerabilities, where the browser incorrectly interprets the type of a resource.

Remediation:

Implement the X-Content-Type-Options header with a value of 'nosniff'.

23. TRACE Method Enabled

Severity: LOW **Tool:** WebScraperRecon

Description:

The TRACE HTTP method is enabled on pay.sarral.io, sophie.sarral.io, www.sarral.io and sarral.io. This method can be used to potentially expose sensitive information, such as cookies, in certain scenarios.

Remediation:

Disable the TRACE HTTP method on the web server configuration. This can typically be done by modifying the server's configuration file (e.g., httpd.conf or nginx.conf).

24. pay.sarral.io returns 404

Severity: LOW **Tool:** WebScraperRecon

Description:

The pay.sarral.io subdomain returns a 404 Not Found error. This could indicate a misconfiguration, an abandoned service, or a broken link.

Remediation:

Investigate the purpose of pay.sarral.io. If it is a valid service, ensure it is properly configured and accessible. If it is no longer needed, remove the DNS record and any associated configurations.

25. Outdated Software Components (React Template)

Severity: LOW **Tool:** WebScraperRecon

Description:

The sophie.sarral.io subdomain uses a React template (CoreUI) that is based on older versions of core-js and other libraries. Using outdated components can expose the application to known vulnerabilities.

Remediation:

Update the React template and its dependencies to the latest versions. Regularly monitor for security updates and apply them promptly.

26. Exposed SSH Service

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

Description:

The SSH service is exposed on the standard port 22. While not inherently a vulnerability, it increases the attack surface. Brute-force attacks and vulnerability exploitation attempts are more likely when SSH is exposed.

Remediation:

Consider changing the SSH port to a non-standard port, implementing strong password policies, using key-based authentication, and enabling fail2ban to mitigate brute-force attacks. Ensure SSH configuration follows security best practices.

27. 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.

28. Privacy Protection Service (Domains By Proxy, LLC)

Severity: INFO **Tool:** Whois

Description:

While privacy protection obscures registrant details, it also introduces a potential point of failure. If the privacy service is compromised or becomes unavailable, it could impact the ability to manage the domain or resolve disputes.

Remediation:

Understand the privacy service's terms and conditions, and ensure a clear process for verifying domain ownership in case of issues with the privacy service. Consider the legal implications of using a privacy service in relation to domain ownership and liability.

29. Unsigned DNSSEC

Severity: INFO **Tool:** Whois

Description:

The DNSSEC field indicates that DNSSEC is unsigned. DNSSEC helps prevent DNS spoofing and cache poisoning attacks.

Remediation:

Implement DNSSEC to digitally sign DNS records, ensuring their authenticity and integrity. This helps protect against DNS-based attacks.

30. 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.

31. Information Disclosure via Subdomain Enumeration

Severity: INFO **Tool:** Subfinder

Description:

The enumeration of subdomains reveals information about the organization's infrastructure and services. This information can be used by attackers to map the attack surface and identify potential vulnerabilities.

Remediation:

While hiding subdomains entirely is often impractical, consider using wildcard certificates to reduce the visibility of specific subdomain names. Implement strong access controls and security measures on all subdomains to minimize the impact of information disclosure.

32. Expanded Attack Surface

Severity: INFO **Tool:** Amass Passive

Description:

The discovery of multiple subdomains (sophie.sarral.io, pay.sarral.io, www.sarral.io, www.pay.sarral.io) increases the overall attack surface. Each subdomain represents a potential entry point for attackers.

Remediation:

Conduct thorough security assessments of each subdomain, including vulnerability scanning, penetration testing, and configuration reviews. Ensure consistent security policies and practices across all subdomains.

33. Information Disclosure via robots.txt/sitemap.xml

Severity: INFO **Tool:** Assetfinder

Description:

The existence of robots.txt or sitemap.xml files on any of the domains could inadvertently expose sensitive information about the website's structure and content, potentially aiding attackers in reconnaissance.

Remediation:

Review robots.txt and sitemap.xml files to ensure they do not expose sensitive information. Consider restricting access to these files or removing them altogether if they are not necessary.

34. Potentially Sensitive Phone Numbers Disclosed

Severity: INFO **Tool:** WebScraperRecon

Description:

The subdomain sophie.sarral.io contains a large number of phone numbers that may or may not be sensitive. Further investigation is needed to determine the nature of these numbers.

Remediation:

Review the source code and content of sophie.sarral.io to determine the purpose and sensitivity of the phone numbers. If the numbers are not intended for public disclosure, remove them or implement appropriate access controls.

35. HTTP Service without Redirection to HTTPS

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

Description:

The server is running HTTP on port 80 without an explicit mention of redirection to HTTPS. This means that users might connect to the server over an unencrypted connection, potentially exposing sensitive data.

Remediation:

Implement a redirect from HTTP (port 80) to HTTPS (port 443) to ensure all traffic is encrypted. This can be done through Apache configuration.

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: 2025-11-27T11:15:32Z <<< 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.pay.sarral.io [INF] Found 4 subdomains
for sarral.io in 54 seconds 2 milliseconds www.sarral.io sophie.sarral.io pay.sarral.io
```

Tool: Amass Passive

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

Tool: Assetfinder

```
sarral.io sarral.io www.sarral.io sophie.sarral.io pay.sarral.io www.pay.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": 0.62, "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": 8.08, "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 11:17:44 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": "d87a45582a1ddbaab8f32d741f174bc9",
"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"], "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.i ...[Truncated]
```

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 06:18 EST Nmap scan report for
sarral.io (159.89.216.111) Host is up (0.081s 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 36.92 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
```