SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 28, 2025
Project: SAR-057
Version 1.0

Confidentiality Statement

This document is the exclusive property of the Client and Sarral Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Contact Information

Name	Title	Contact Information
Sarral Scan	Automated Scanner	support@sarral.io
Client	Security Team	security@sarral.io

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range used throughout the document.

Severity	CVSS V3 Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and data loss.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps.
Low	0.1-3.9	Vulnerabilities are non-exploitable but reduce attack surface.
Informational	N/A	No vulnerability exists. Additional information provided.

Executive Summary

Sarral Security evaluated sarral.io's security posture on November 28, 2025. The following sections provide a high-level overview of vulnerabilities discovered.

Testing Summary

The assessment evaluated the target's external network security posture. The team performed vulnerability scanning and reconnaissance to identify potential risks such as exposed services, misconfigurations, and sensitive information disclosure.

Vulnerability Summary & Report Card

1	0	5	9	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Potential Subdomain Takeover	Critical	1. Verify DNS configuration for www.pay.sarral.io.
SAR-002: Lack of DNSSEC	Medium	Implement DNSSEC by generating DNSSEC keys
SAR-003: Single Point of Failure - Server Availability	Medium	Implement multiple geographically diverse servers
SAR-004: Payment Subdomain Exposure	Medium	Conduct a thorough security audit and penetration
SAR-005: Payment Gateway Exposure	Medium	Conduct a thorough security audit and penetration
SAR-006: Missing Security Headers	Medium	1. Implement HSTS (HTTP Strict Transport Secur
SAR-007: WHOIS Privacy Service Obscuring Registrant Identity	Low	While not directly remediable by the domain itself,
SAR-008: Reliance on GoDaddy's Infrastructure	Low	Consider using a secondary DNS provider for redu
SAR-009: Lack of DNSSEC	Low	Implement DNSSEC (Domain Name System Secu
SAR-010: Subdomain Takeover Potential	Low	Verify the configuration of all subdomains, includin
SAR-011: Subdomain Takeover Risk	Low	Verify the DNS configuration of 'sophie.sarral.io' a
SAR-012: Lack of Security Headers	Low	Implement security headers on all subdomains. Us
SAR-013: Potential Scan Configuration Issue	Low	Review the Assetfinder configuration file and com
SAR-014: Potentially Misleading Phone Numbers	Low	1. Review the content of sophie.sarral.io. 2. Remo
SAR-015: TRACE Method Enabled	Low	1. Disable the TRACE method on the web server
SAR-016: Lack of Discoverable Subdomains	Info	Verify the scan configuration and target scope. En

Technical Findings

Finding SAR-001: Potential Subdomain Takeover (Critical)

Description:	The subdomain www.pay.sarral.io is resolving to an IP address (159.89.216.111), but the web server is not configured to serve content for that subdomain. This is indicated by the NameResolutionError in the scan results. An attacker could potentially take over this subdomain by configuring a server at that IP address to serve malicious content, impersonating the Sarral.io payment portal.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

1. Verify DNS configuration for www.pay.sarral.io. Ensure it points to the correct server. 2. If the subdomain is no longer in use, remove the DNS record to prevent takeover. 3. If the subdomain is intended to be used, configure the web server to properly handle requests for it.

Finding SAR-002: Lack of DNSSEC (Medium)

Description:	DNSSEC is not enabled for this domain. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks. An attacker could potentially redirect users to a malicious website by manipulating DNS records.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Implement DNSSEC by generating DNSSEC keys and configuring the domain's DNS records with the appropriate DS records at the registrar. Consult with the DNS provider for specific instructions.

Finding SAR-003: Single Point of Failure - Server Availability (Medium)

Description:	The domain sarral.io resolves to a single IP address (159.89.216.111). This creates a single point of failure. If this server 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 significantly impact business operations and user experience.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	NSLookup
References:	N/A

Remediation

Implement multiple geographically diverse servers for the domain. Configure a load balancer to distribute traffic across these servers. Consider using a Content Delivery Network (CDN) to cache content and further improve availability and performance. Implement monitoring and alerting to quickly detect and respond to server outages.

Finding SAR-004: Payment Subdomain Exposure (Medium)

Description:	The presence of 'pay.sarral.io' and 'www.pay.sarral.io' indicates a payment processing subdomain. If this subdomain is not properly secured, it could be vulnerable to attacks such as cross-site scripting (XSS), SQL injection, or other vulnerabilities that could compromise sensitive payment information. An attacker could potentially intercept or manipulate payment transactions, leading to financial loss and reputational damage.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

Conduct a thorough security audit and penetration test of the 'pay.sarral.io' and 'www.pay.sarral.io' subdomains. Implement robust input validation, output encoding, and secure coding practices to prevent common web vulnerabilities. Ensure that the payment gateway is PCI DSS compliant and that all sensitive data is encrypted both in transit and at rest. Implement strong access controls and regularly monitor the subdomain for suspicious activity.

Finding SAR-005: Payment Gateway Exposure (Medium)

Description:	The subdomain 'pay.sarral.io' suggests the presence of a payment gateway. Without further investigation, it's impossible to determine the security posture of this subdomain. However, any vulnerabilities in the payment gateway could lead to sensitive financial data exposure, including credit card information and transaction details. A misconfigured or outdated payment gateway is a prime target for attackers.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Conduct a thorough security audit and penetration test of 'pay.sarral.io'. Ensure the payment gateway is PCI DSS compliant and uses the latest security patches. Implement strong access controls and monitoring to detect and prevent unauthorized access.

Finding SAR-006: Missing Security Headers (Medium)

Description:	The main Sarral.io domains (sarral.io and www.sarral.io) are missing several important security headers, including HSTS, CSP, 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), clickjacking, and data injection.
Risk:	Likelihood: High Impact: Medium
System:	sarral.io

Tools Used:	WebScraperRecon
References:	N/A

Remediation

1. Implement HSTS (HTTP Strict Transport Security) to enforce HTTPS connections. 2. Implement CSP (Content Security Policy) to prevent XSS attacks. 3. Implement X-Frame-Options to prevent clickjacking. 4. Implement X-Content-Type-Options to prevent MIME sniffing attacks. 5. Implement Referrer-Policy to control referrer information. 6. Implement Permissions-Policy (formerly Feature-Policy) to control browser features. 7. Consider implementing X-XSS-Protection, although CSP is a more robust solution for XSS prevention.

Finding SAR-007: WHOIS Privacy Service Obscuring Registrant Identity (Low)

Description:	The domain registrant is using Domains By Proxy, LLC, a privacy service. This obscures the true owner of the domain, making it difficult to identify and contact them directly in cases of abuse, legal issues, or security incidents. While legitimate for privacy, it can also be used to mask malicious intent.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

While not directly remediable by the domain itself, consider the implications of dealing with a domain using a privacy service. If engaging in business, perform thorough due diligence. Law enforcement or legal professionals may be able to subpoena the registrar for the underlying registrant information if necessary.

Finding SAR-008: Reliance on GoDaddy's Infrastructure (Low)

Description:	The domain relies on GoDaddy's infrastructure for DNS and registration services. While GoDaddy is a reputable provider, any outage or compromise of their systems could impact the availability and integrity of the domain.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Consider using a secondary DNS provider for redundancy. Regularly back up DNS records and domain registration information. Implement monitoring to detect any issues with GoDaddy's services.

Finding SAR-009: Lack of DNSSEC (Low)

Description:	The NSLookup output doesn't explicitly confirm or deny DNSSEC. However, the absence of DNSSEC records implies that the domain is potentially vulnerable to DNS spoofing or cache poisoning attacks. An attacker could potentially redirect users to a malicious website by manipulating DNS records.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	NSLookup
References:	N/A

Remediation

Implement DNSSEC (Domain Name System Security Extensions) to digitally sign DNS records. This will ensure the authenticity and integrity of DNS data, preventing attackers from tampering with DNS responses and redirecting users to malicious sites. Consult with your DNS provider for instructions on enabling DNSSEC.

Finding SAR-010: Subdomain Takeover Potential (Low)

Description:	While not immediately apparent, the existence of 'sophie.sarral.io' raises the possibility of a subdomain takeover vulnerability. If this subdomain is pointing to a service that is no longer in use or has been misconfigured, an attacker could potentially claim the subdomain and use it for malicious purposes, such as phishing or distributing malware. This is especially true if the subdomain is pointing to a cloud service like AWS S3 or Azure Blob Storage that has been deprovisioned.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

Verify the configuration of all subdomains, including 'sophie.sarral.io'. Ensure that each subdomain is properly configured and pointing to a valid and actively managed service. If a subdomain is no longer in use, either remove the DNS record or configure it to point to a placeholder page with appropriate security measures. Implement subdomain takeover prevention measures, such as regularly monitoring DNS records and using a service that alerts you to potential takeover opportunities.

Finding SAR-011: Subdomain Takeover Risk (Low)

Description:	The subdomain 'sophie.sarral.io' could potentially be vulnerable to subdomain takeover if it's pointing to a service that is no longer in use or has been misconfigured. An attacker could claim this subdomain and use it for malicious purposes, such as phishing or distributing malware, damaging the organization's reputation.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Verify the DNS configuration of 'sophie.sarral.io' and ensure it's pointing to a valid and actively managed service. If the subdomain is no longer needed, remove the DNS record. Implement subdomain takeover prevention measures, such as regularly monitoring DNS records and using a service that alerts to potential takeover opportunities.

Finding SAR-012: Lack of Security Headers (Low)

Description:	While not directly evident from the domain names, it's likely that some or all of these subdomains are missing crucial security headers (e.g., Content Security Policy, HTTP Strict Transport Security, X-Frame-Options). The absence of these headers makes the website more vulnerable to attacks like cross-site scripting (XSS) and clickjacking.
Risk:	Likelihood: High Impact: Low
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Implement security headers on all subdomains. Use a tool like securityheaders.com to assess the current header configuration and identify missing or misconfigured headers. Regularly review and update the header configuration to address new threats.

Finding SAR-013: Potential Scan Configuration Issue (Low)

Description:	The Assetfinder scan returned an empty result. This could be due to incorrect configuration of the Assetfinder tool, such as an invalid API key, incorrect target specification, or network connectivity issues preventing the tool from reaching its data sources. It's crucial to ensure the tool is functioning correctly to obtain accurate results.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Assetfinder
References:	N/A

Remediation

Review the Assetfinder configuration file and command-line arguments. Verify the API key (if applicable) is valid and has sufficient permissions. Test network connectivity to ensure the tool can reach its data sources. Try running the scan against a known target to confirm functionality.

Finding SAR-014: Potentially Misleading Phone Numbers (Low)

Description:	The sophie.sarral.io subdomain contains a large number of phone numbers that appear to be test data (e.g., '0 0 0 9999', '0123456789', '1 1 0 0 1 0-1'). While not a direct security vulnerability, this could be confusing or misleading to users if they were to encounter this data.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

1. Review the content of sophie.sarral.io. 2. Remove or replace the test phone numbers with valid contact information or placeholder data. 3. Ensure that test data is not exposed to the public in production environments.

Finding SAR-015: TRACE Method Enabled (Low)

Description:	The HTTP TRACE method is enabled on sophie.sarral.io and pay.sarral.io. While not always exploitable, TRACE can be used in conjunction with other vulnerabilities, such as XSS, to steal cookies or other sensitive information. It's generally recommended to disable TRACE unless specifically required.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

1. Disable the TRACE method on the web server configuration for sophie.sarral.io and pay.sarral.io. This can typically be done in the Apache or Nginx configuration files.

Finding SAR-016: Lack of Discoverable Subdomains (Info)

Description:	The Assetfinder scan returned no subdomains. While this could indicate a secure configuration, it's more likely that the target's subdomain enumeration is being actively blocked or that the target has a very small attack surface. This lack of visibility hinders comprehensive security assessments and penetration testing.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Assetfinder
References:	N/A

Remediation

Verify the scan configuration and target scope. Employ alternative subdomain enumeration techniques (e.g., certificate transparency logs, DNS zone transfers, brute-forcing with custom wordlists). Investigate the target's infrastructure to understand its actual attack surface.
