SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 28, 2025
Project: SAR-056
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

0	1	5	5	5
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: www.pay.sarral.io DNS Resolution Failure	High	Verify the DNS configuration for www.pay.sarral.io
SAR-002: Lack of DNSSEC	Medium	Implement DNSSEC by generating cryptographic
SAR-003: Single Point of Failure - Lack of Redundancy	Medium	Implement multiple A records in the DNS configura
SAR-004: Potential Payment Gateway Exposure	Medium	Conduct a thorough security audit of the 'pay.sarra
SAR-005: Potential Payment Gateway Exposure	Medium	Conduct a thorough security audit of the payment
SAR-006: Missing Security Headers	Medium	Implement the following security headers in the we
SAR-007: Missing DNSSEC Records	Low	Implement DNSSEC for the sarral.io domain. This
SAR-008: Potential Development/Testing Environment Exposure	Low	Review the purpose and security configuration of '
SAR-009: Subdomain Takeover Risk	Low	Regularly audit DNS records for all subdomains to
SAR-010: Potentially Sensitive Phone Numbers Exposed	Low	Review the source code of sophie.sarral.io and re
SAR-011: TRACE Method Enabled	Low	Disable the TRACE HTTP method in the web serv
SAR-012: Privacy Protected Registration	Info	Consider the trade-offs between privacy and trans
SAR-013: Client-Side Prohibitions	Info	Ensure that the domain owner has secure and reli
SAR-014: General Subdomain Takeover Risk	Info	Regularly audit all subdomains to ensure that they
SAR-015: Lack of Discoverable Subdomains	Info	Verify the Assetfinder configuration and target dor
SAR-016: pay.sarral.io returns 404	Info	Investigate the configuration of pay.sarral.io. If the

Technical Findings

Finding SAR-001: www.pay.sarral.io DNS Resolution Failure (High)

Description:	The www.pay.sarral.io subdomain is failing to resolve, indicating a DNS configuration issue. This prevents users from accessing the service and could be exploited by attackers to impersonate the domain or redirect traffic to malicious sites. This is a critical issue if the subdomain is intended to be a payment portal.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

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. Check for any typos or errors in the DNS zone file. If the subdomain is no longer needed, remove the DNS record.

Finding SAR-002: Lack of DNSSEC (Medium)

Description:	The domain sarral.io does not have DNSSEC (Domain Name System Security Extensions) enabled. DNSSEC provides authentication of DNS data, preventing attackers from manipulating DNS records to redirect users to malicious websites. Without DNSSEC, the domain is vulnerable to DNS spoofing and cache poisoning attacks.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Implement DNSSEC by generating cryptographic keys, signing the DNS zone file, and publishing the public key in the domain's parent zone. Consult with the DNS provider (GoDaddy in this case) for specific instructions on

enabling DNSSEC for the domain.

Finding SAR-003: Single Point of Failure - Lack of Redundancy (Medium)

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.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	NSLookup
References:	N/A

Remediation

Implement multiple A records in the DNS configuration, pointing to different servers in geographically diverse locations. This will provide redundancy and ensure that the website remains accessible even if one server goes down. Consider using a Content Delivery Network (CDN) to further improve availability and performance.

Finding SAR-004: Potential Payment Gateway Exposure (Medium)

Description:	The subdomain 'pay.sarral.io' and 'www.pay.sarral.io' strongly suggest the existence of 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 the theft of sensitive financial information. The presence of 'www' is not necessarily a vulnerability, but it should be checked for consistent security configurations.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

Conduct a thorough security audit of the 'pay.sarral.io' subdomain, including penetration testing and vulnerability scanning. Ensure that all payment processing is PCI DSS compliant and that appropriate security measures, such as strong encryption and input validation, are in place. Implement proper access controls and regularly monitor the gateway for suspicious activity.

Finding SAR-005: Potential Payment Gateway Exposure (Medium)

Description:	The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment gateway is associated with these subdomains. Without further information, it's impossible to determine if the gateway is properly secured. A misconfigured or vulnerable payment gateway could lead to sensitive financial data exposure, including credit card numbers and transaction details.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Conduct a thorough security audit of the payment gateway, including penetration testing and vulnerability scanning. Ensure proper access controls are in place, and that the gateway is PCI DSS compliant. Implement strong encryption for all sensitive data in transit and at rest. Regularly update the payment gateway software and associated libraries.

Finding SAR-006: Missing Security Headers (Medium)

Description:	The main domains (sarral.io and www.sarral.io) are missing several important 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. The sophie.sarral.io subdomain is also missing these headers. The absence of these headers makes the website vulnerable to various attacks, including man-in-the-middle attacks, cross-site scripting (XSS), clickjacking, and other browser-based exploits.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Implement the following security headers in the web server configuration: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. Configure each header with appropriate directives to mitigate specific attack vectors. Regularly review and update the header configurations to address emerging threats.

Finding SAR-007: Missing DNSSEC Records (Low)

Description:	The NSLookup output doesn't explicitly show DNSSEC records. While not definitive proof that DNSSEC is disabled, the absence suggests it might not be implemented. 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.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	NSLookup
References:	N/A

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. Consult with the domain registrar or DNS provider for specific instructions on enabling DNSSEC.

Finding SAR-008: Potential Development/Testing Environment Exposure (Low)

Description:	The subdomain 'sophie.sarral.io' could indicate a development or testing environment. These environments often have weaker security controls than production environments, making them potential targets for attackers. If compromised, an attacker could gain access to sensitive data or use the environment as a stepping stone to attack the production environment.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

Review the purpose and security configuration of 'sophie.sarral.io'. If it is a development or testing environment, ensure that it is isolated from the production environment and that it does not contain any sensitive data. Implement strong authentication and authorization controls, and regularly monitor the environment for suspicious activity. Consider removing the subdomain if it is no longer needed.

Finding SAR-009: Subdomain Takeover Risk (Low)

Description:	While not immediately vulnerable, all subdomains (sophie.sarral.io, www.pay.sarral.io, www.sarral.io, pay.sarral.io) are potential targets for subdomain takeovers if their DNS records point to services that are no longer in use or improperly configured. An attacker could claim these subdomains and use them for malicious purposes, such as phishing or distributing malware.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Regularly audit DNS records for all subdomains to ensure they point to active and properly configured services. Implement a subdomain takeover prevention strategy, including monitoring for dangling DNS records and using services that offer subdomain takeover protection. Consider using a wildcard DNS record with caution, as it can increase the risk of subdomain takeovers.

Finding SAR-010: Potentially Sensitive Phone Numbers Exposed (Low)

Description:	The sophie.sarral.io subdomain contains a large number of phone numbers extracted from the source code. While many appear to be test or placeholder values, the presence of any potentially valid phone numbers could be used for social engineering attacks or other malicious purposes. The context of these numbers is unknown, but their exposure is a potential information disclosure issue.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the source code of sophie.sarral.io and remove any unnecessary or sensitive phone numbers. If phone numbers are required, ensure they are stored and handled securely, and not directly exposed in the client-side code. Implement input validation and sanitization to prevent the accidental inclusion of phone numbers in comments or other publicly accessible areas.

Finding SAR-011: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on pay.sarral.io and sophie.sarral.io. The TRACE method can be used in cross-site tracing (XST) attacks to steal cookies or other sensitive information. While the risk is lower with modern browsers, disabling TRACE is still a recommended security practice.
Risk:	Likelihood: Medium Impact: Low

System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

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

Finding SAR-012: Privacy Protected Registration (Info)

Description:	The domain registration uses 'Domains By Proxy, LLC' to mask the actual registrant's information. While this enhances privacy, it can complicate identifying and contacting the domain owner in cases of abuse or security incidents. It also makes it harder to verify the legitimacy of the domain owner.
Risk:	Likelihood: Medium Impact: Info
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Consider the trade-offs between privacy and transparency. While maintaining privacy is important, ensure that a clear and accessible channel exists for reporting abuse or security concerns related to the domain. Implement a security.txt file on the domain to provide security contact information.

Finding SAR-013: Client-Side Prohibitions (Info)

Description:	The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited status codes set. These prevent unauthorized deletion, renewal, transfer, and updates of the domain. While these are generally good security practices, they can also hinder legitimate administrative actions if the owner loses access to the registrar account.
Risk:	Likelihood: Medium Impact: Info
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Ensure that the domain owner has secure and reliable access to the registrar account to manage the domain. Document the process for recovering access to the account in case of emergencies. Regularly review the domain status codes to ensure they are still appropriate.

Finding SAR-014: General Subdomain Takeover Risk (Info)

Description:	While not immediately exploitable, the existence of these subdomains presents a potential risk of subdomain takeover if they are pointing to services that are no longer in use or are misconfigured. An attacker could claim these subdomains and use them to host malicious content or phish users.
Risk:	Likelihood: Medium Impact: Info
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

Regularly audit all subdomains to ensure that they are properly configured and pointing to active services. Implement DNS record monitoring to detect any changes that could indicate a subdomain takeover attempt. Use a service like Cloudflare or AWS Route 53 to manage DNS records and implement security features such as DNSSEC.

Finding SAR-015: Lack of Discoverable Subdomains (Info)

Description:	The Assetfinder scan returned no subdomains. While this could indicate a strong security posture, it's also possible that the scan was misconfigured, the target is actively preventing subdomain enumeration, or the target simply has a very small online presence. This lack of visibility makes it difficult to assess the overall attack surface and identify potential vulnerabilities.
Risk:	Likelihood: Medium Impact: Info
System:	sarral.io
Tools Used:	Assetfinder
References:	N/A

Remediation

Verify the Assetfinder configuration and target domain. Consider using other subdomain enumeration tools and techniques (e.g., certificate transparency logs, DNS zone transfers, brute-forcing) to expand the scope of the assessment. Investigate if the target is actively blocking subdomain enumeration attempts.

Finding SAR-016: pay.sarral.io returns 404 (Info)

Description:	The pay.sarral.io subdomain returns a 404 Not Found error. This could indicate a misconfiguration, an abandoned service, or a broken link. While not directly a vulnerability, it could lead to user frustration and potentially expose sensitive information if the service was intended to be active.
Risk:	Likelihood: Medium Impact: Info
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Investigate the configuration of pay.sarral.io. If the service is no longer needed, remove the DNS record and web server configuration. If the service is intended to be active, correct the configuration and ensure the application is

properly deployed.