SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 28, 2025
Project: SAR-058
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	6	8	3
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Exposed Payment Gateway Subdomain	Critical	1. Implement strong encryption (HTTPS) with a valid SSL/TLS certificate on 'pay.sarral.io'. 2. Regularly audit the payment gateway's code and configuration for vulnerabilities. 3. Enforce strict acces...
SAR-002: Lack of DNSSEC	Medium	Implement DNSSEC by generating cryptographic keys and configuring them with the domain registrar and DNS servers. Regularly monitor DNS records for any unauthorized changes.
SAR-003: Single Point of Failure - IP Address	Medium	Implement a load balancer and distribute the service across multiple servers with different IP addresses. Consider using a Content Delivery Network (CDN) to cache content and distribute traffic global...
SAR-004: Wildcard Certificate/DNS Misconfiguration	Medium	1. Regularly audit DNS records and remove any unused or misconfigured subdomains. 2. Implement proper subdomain ownership verification. 3. Monitor for subdomain takeover attempts. 4. If using wildcard...
SAR-005: Potential Payment Gateway Exposure	Medium	Conduct a thorough security audit and penetration test of the 'pay.sarral.io' subdomain and any associated payment processing systems. Ensure all payment processing components are PCI DSS compliant an...
SAR-006: Missing Security Headers	Medium	Implement the following security headers in the web server configuration: - HSTS (Strict-Transport-Security): Enforce HTTPS connections. - CSP (Content-Security-Policy): Define allowed sources for var...
SAR-007: Non-Functional Payment Subdomain (pay.sarral.io)	Medium	Investigate the configuration of the pay.sarral.io subdomain. Ensure that the payment service is properly deployed and configured. If the service is no longer needed, remove the subdomain or redirect ...

SAR-008: Information Disclosure via 'sophie.sarral.io'	Low	1. Investigate the purpose of 'sophie.sarral.io'. 2. Implement appropriate access controls and authentication mechanisms. 3. Ensure that no sensitive information is exposed on this subdomain. 4. If th...
SAR-009: Potential Sensitive Data Exposure on 'sophie.sarral.io'	Low	Investigate the purpose and contents of the 'sophie.sarral.io' subdomain. If it contains sensitive data or applications, implement appropriate security measures, including access controls, encryption,...
SAR-010: Lack of Security Headers on Root Domain	Low	Implement security headers on 'sarral.io' and 'www.sarral.io', including Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), X-Frame-Options, and X-XSS-Protection. Regularly review a...
SAR-011: Potential Scan Configuration Issue	Low	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...
SAR-012: Potential Information Disclosure (sophie.sarral.io)	Low	Review the source code and database of sophie.sarral.io to identify the origin of these phone numbers. Remove or mask any sensitive or irrelevant data. Implement proper data validation and sanitizatio...
SAR-013: Outdated React Template (sophie.sarral.io)	Low	Update the CoreUI React Admin Template to the latest stable version. Regularly monitor for updates and apply them promptly to address any newly discovered vulnerabilities.
SAR-014: API Endpoint Discovery	Low	Analyze the functionality of the discovered API endpoints. Implement proper authentication and authorization mechanisms to restrict access to authorized users or applications. Ensure that the API endp...
SAR-015: TRACE Method Enabled	Low	Disable the TRACE HTTP method in the web server configuration. This can typically be done by modifying the AllowMethods directive in Apache or the httpProtocol.allowKeepAlive property in IIS.
SAR-016: Privacy Protected Registration	Info	Consider the implications of privacy protection. While it offers anonymity, it can hinder communication and trust. Ensure that a clear and accessible abuse contact mechanism is in place, even with pri...

SAR-017: Client-Side Prohibitions	Info	Ensure that the domain owner understands the implications of these prohibitions and has a plan for managing the domain in case of legitimate needs for deletion, renewal, transfer, or updates. Document...
SAR-018: Lack of Discoverable Subdomains	Info	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). Inve...

Technical Findings

Finding SAR-001: Exposed Payment Gateway Subdomain (Critical)

Description:	The subdomain 'pay.sarral.io' suggests a payment gateway. If this subdomain 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 payment information, including credit card details and transaction history. An exposed payment gateway can also be targeted for fraudulent transactions.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

1. Implement strong encryption (HTTPS) with a valid SSL/TLS certificate on 'pay.sarral.io'. 2. Regularly audit the payment gateway's code and configuration for vulnerabilities. 3. Enforce strict access controls and authentication mechanisms. 4. Implement a Web Application Firewall (WAF) to protect against common web attacks. 5. Ensure compliance with PCI DSS standards.

Finding SAR-002: Lack of DNSSEC (Medium)

Description:	The domain sarral.io does not have DNSSEC enabled. This makes it vulnerable to DNS spoofing or cache poisoning attacks. An attacker could potentially redirect users to a malicious website by manipulating DNS records.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Implement DNSSEC by generating cryptographic keys and configuring them with the domain registrar and DNS servers. Regularly monitor DNS records for any unauthorized changes.

Finding SAR-003: Single Point of Failure - IP Address (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 entire website or service associated with sarral.io 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 a load balancer and distribute the service across multiple servers with different IP addresses. Consider using a Content Delivery Network (CDN) to cache content and distribute traffic globally, further mitigating the impact of server outages. Implement monitoring and alerting to quickly detect and respond to server failures.

Finding SAR-004: Wildcard Certificate/DNS Misconfiguration (Medium)

Description:	The presence of 'www.pay.sarral.io', 'www.sarral.io', and 'sophie.sarral.io' suggests the possible use of wildcard certificates or a broad DNS configuration. If any of these subdomains are not actively used or properly configured, they could be vulnerable to subdomain takeover attacks. An attacker could claim the subdomain and host malicious content, potentially phishing users or damaging the organization's reputation.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

1. Regularly audit DNS records and remove any unused or misconfigured subdomains. 2. Implement proper subdomain ownership verification. 3. Monitor for subdomain takeover attempts. 4. If using wildcard certificates, ensure they are properly managed and only used for intended subdomains. 5. Implement HTTP Strict Transport Security (HSTS) to prevent man-in-the-middle attacks.

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

Description:	The subdomain 'pay.sarral.io' suggests the presence of a payment gateway or related service. Without further investigation, it's impossible to determine if this service is properly secured. If vulnerable, attackers could potentially intercept payment information, conduct fraudulent transactions, or compromise sensitive customer data. The 'www.pay.sarral.io' also needs to be checked.
Risk:	Likelihood: Low Impact: High
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Conduct a thorough security audit and penetration test of the 'pay.sarral.io' subdomain and any associated payment processing systems. Ensure all payment processing components are PCI DSS compliant and implement robust security measures, including encryption, access controls, and intrusion detection systems. Verify the 'www.pay.sarral.io' subdomain is also secure.

Finding SAR-006: Missing Security Headers (Medium)

Description:	The main Sarral.io domain (www.sarral.io and sarral.io), sophie.sarral.io and pay.sarral.io are missing crucial security headers such as HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. This absence makes the website vulnerable to various attacks, including 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

Implement the following security headers in the web server configuration: - HSTS (Strict-Transport-Security): Enforce HTTPS connections. - CSP (Content-Security-Policy): Define allowed sources for various content types. - X-Frame-Options: Prevent clickjacking attacks. - X-Content-Type-Options: Prevent MIME-sniffing attacks. - Referrer-Policy: Control the amount of referrer information sent with requests. - Permissions-Policy: Control browser features available to the website. - X-XSS-Protection: Enable XSS filtering in older browsers.

Finding SAR-007: Non-Functional Payment Subdomain (pay.sarral.io) (Medium)

Description:	The pay.sarral.io subdomain returns a 404 Not Found error. This indicates that the payment service is either misconfigured, not properly deployed, or has been abandoned. This can lead to customer frustration and potential loss of revenue if customers are unable to make payments. The presence of GoDaddy related headers suggests a possible link to GoDaddy's online order system, but the 404 indicates a problem with the specific configuration.
Risk:	Likelihood: High Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Investigate the configuration of the pay.sarral.io subdomain. Ensure that the payment service is properly deployed and configured. If the service is no longer needed, remove the subdomain or redirect it to a functional page. If the service is intended to be functional, review the GoDaddy configuration and ensure all necessary components are correctly set up.

Finding SAR-008: Information Disclosure via 'sophie.sarral.io' (Low)

Description:	The subdomain 'sophie.sarral.io' could potentially expose sensitive information depending on its purpose. It might be a development or testing environment, or it could be associated with a specific individual. If not properly secured, it could leak internal data, credentials, or other confidential information.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

1. Investigate the purpose of 'sophie.sarral.io'. 2. Implement appropriate access controls and authentication mechanisms. 3. Ensure that no sensitive information is exposed on this subdomain. 4. If the subdomain is no longer needed, consider decommissioning it.

Finding SAR-009: Potential Sensitive Data Exposure on 'sophie.sarral.io' (Low)

Description:	The subdomain 'sophie.sarral.io' is ambiguous and could potentially host sensitive information or applications. Without further investigation, it's impossible to determine the purpose or security posture of this subdomain. It could be a development environment, a staging server, or a forgotten application that is vulnerable to attack. The name 'sophie' could indicate a personal or departmental resource, which might have weaker security controls.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Investigate the purpose and contents of the 'sophie.sarral.io' subdomain. If it contains sensitive data or applications, implement appropriate security measures, including access controls, encryption, and regular security audits. If the subdomain is no longer needed, decommission it to reduce the attack surface.

Finding SAR-010: Lack of Security Headers on Root Domain (Low)

Description:	While not directly revealed by the domain names, the absence of security headers on 'sarral.io' and 'www.sarral.io' could expose the website to various client-side attacks, such as Cross-Site Scripting (XSS) and Clickjacking. Security headers provide an extra layer of defense by instructing the browser on how to handle the website's content.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Implement security headers on 'sarral.io' and 'www.sarral.io', including Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), X-Frame-Options, and X-XSS-Protection. Regularly review and update these headers to ensure they provide adequate protection against emerging threats.

Finding SAR-011: 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-012: Potential Information Disclosure (sophie.sarral.io) (Low)

Description:	The sophie.sarral.io subdomain contains a large number of phone numbers that appear to be randomly generated or test data. While likely not sensitive, their presence could be indicative of poor data handling practices or a development environment exposed to the public. The presence of phone numbers like '0 0 0 9999', '0123456789', and various large numerical strings suggests a lack of proper sanitization or data masking.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the source code and database of sophie.sarral.io to identify the origin of these phone numbers. Remove or mask any sensitive or irrelevant data. Implement proper data validation and sanitization procedures to prevent similar issues in the future.

Finding SAR-013: Outdated React Template (sophie.sarral.io) (Low)

Description:	The sophie.sarral.io subdomain appears to be using an outdated version of the CoreUI React Admin Template (v5.5.0, Copyright 2025). Using outdated libraries and frameworks can expose the application to known vulnerabilities and compatibility issues.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon

References:	N/A

Remediation

Update the CoreUI React Admin Template to the latest stable version. Regularly monitor for updates and apply them promptly to address any newly discovered vulnerabilities.

Finding SAR-014: API Endpoint Discovery (Low)

Description:	The scan discovered API endpoints `/api.js` and `/api.js?render=6LfwfTgrAAAAAF8FCXh_3WsE_uYRB_9I9f6Qx_9R` on the main Sarral.io domain. While the functionality of these endpoints is unknown, their existence should be investigated to ensure they are properly secured and do not expose sensitive data or functionality. The presence of a reCAPTCHA render parameter suggests this API might be related to form submissions or bot detection.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Analyze the functionality of the discovered API endpoints. Implement proper authentication and authorization mechanisms to restrict access to authorized users or applications. Ensure that the API endpoints do not expose sensitive data or functionality without proper security controls. Review the reCAPTCHA integration to ensure it is properly configured and prevents abuse.

Finding SAR-015: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on the main Sarral.io domain and sophie.sarral.io. The TRACE method can be used to expose sensitive information, such as cookies and authentication headers, in the server's response. While the risk is relatively low, disabling TRACE is a best practice.

Risk:	Likelihood: Low 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 AllowMethods directive in Apache or the httpProtocol.allowKeepAlive property in IIS.

Finding SAR-016: Privacy Protected Registration (Info)

Description:	The domain registration uses Domains By Proxy, LLC, which obscures the actual owner's contact information. While this protects privacy, it can make it difficult to directly contact the owner in case of abuse or security incidents. It also makes attribution more difficult in case of malicious activity.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Consider the implications of privacy protection. While it offers anonymity, it can hinder communication and trust. Ensure that a clear and accessible abuse contact mechanism is in place, even with privacy protection enabled.

Finding SAR-017: Client-Side Prohibitions (Info)

Description:	The domain has clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, and clientUpdateProhibited status codes. These are generally positive security measures that prevent unauthorized deletion, renewal, transfer, or updates of the domain. However, they could also complicate legitimate domain management tasks if not properly understood.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Ensure that the domain owner understands the implications of these prohibitions and has a plan for managing the domain in case of legitimate needs for deletion, renewal, transfer, or updates. Document the procedures for removing these prohibitions if necessary.

Finding SAR-018: 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.
