SARRAL SECURITY

sarral.io

Security Assessment Findings Report

Business Confidential

Date: November 28, 2025
Project: SAR-059
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	2	7	7	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Potential Payment Gateway Exposure	High	1. Conduct a thorough security audit and penetration test of 'pay.sarral.io'. 2. Ensure that the payment gateway is PCI DSS compliant. 3. Implement strong authentication and authorization mechanisms. ...
SAR-002: Potential Payment Gateway Vulnerability	High	Conduct a thorough security audit and penetration test of the 'pay.sarral.io' and 'www.pay.sarral.io' subdomains. Ensure that the payment gateway is PCI DSS compliant and that all security patches are...
SAR-003: Lack of DNSSEC	Medium	Implement DNSSEC by generating cryptographic keys and configuring the domain's DNS records with the appropriate digital signatures. Consult with the DNS provider (GoDaddy in this case) for specific in...
SAR-004: 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-005: General Subdomain Takeover Risk	Medium	1. Regularly audit DNS records to identify orphaned or misconfigured subdomains. 2. Implement a process for decommissioning subdomains when they are no longer needed. 3. Use a subdomain takeover detec...
SAR-006: Unidentified Subdomain - 'sophie.sarral.io'	Medium	Investigate the purpose of the 'sophie.sarral.io' subdomain. If it's no longer needed, decommission it. If it's still in use, ensure that it's properly secured with appropriate access controls, securi...
SAR-007: 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 f...

SAR-008: Connection Refused on sophie.sarral.io (HTTPS)	Medium	Ensure that the HTTPS service is properly configured and running on the server hosting sophie.sarral.io. Verify firewall rules to allow HTTPS traffic (port 443). Investigate any network issues that mi...
SAR-009: Outdated Apache Version	Medium	Upgrade Apache to the latest stable version available for the Ubuntu operating system. Regularly check for and apply security patches to the web server software.
SAR-010: Use of Privacy Service (Domains By Proxy)	Low	Consider whether the privacy benefits outweigh the potential drawbacks of obscured ownership. If transparency is desired, the domain owner can choose to reveal their contact information. Ensure that t...
SAR-011: Information Disclosure via Subdomain Enumeration	Low	1. Review the necessity of each subdomain and consider consolidating services where possible. 2. Implement proper access controls to restrict access to sensitive information on each subdomain. 3. Moni...
SAR-012: General Domain Security Posture	Low	Conduct a comprehensive security assessment of the entire 'sarral.io' domain, including vulnerability scanning, penetration testing, and security configuration reviews. Implement a robust security mon...
SAR-013: 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-014: 404 Error on pay.sarral.io	Low	Investigate the purpose of the pay.sarral.io subdomain. If it's no longer needed, remove the DNS record and the associated TLS certificate entry. If it's intended to be a payment gateway, ensure it's ...
SAR-015: TRACE Method Enabled	Low	Disable the TRACE HTTP method in the web server configuration for all subdomains. This can typically be done by modifying the AllowMethods directive in Apache or similar configurations in other web se...
SAR-016: ReCaptcha API Key Exposure	Low	Ensure the reCaptcha API key is properly secured and not being abused. Monitor the key for suspicious activity and consider rotating the key if necessary. Implement server-side validation of the reCap...

SAR-017: 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: Potential Payment Gateway Exposure (High)

Description:	The subdomain 'pay.sarral.io' suggests the presence 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, including credit card details and transaction history. Even if the gateway is secure, the existence of the subdomain itself can be used for phishing attacks.
Risk:	Likelihood: Medium Impact: High
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

1. Conduct a thorough security audit and penetration test of 'pay.sarral.io'. 2. Ensure that the payment gateway is PCI DSS compliant. 3. Implement strong authentication and authorization mechanisms. 4. Regularly monitor the subdomain for suspicious activity. 5. Implement rate limiting to prevent brute-force attacks. 6. Consider using a Web Application Firewall (WAF) to protect against common web vulnerabilities.

Finding SAR-002: Potential Payment Gateway Vulnerability (High)

Description:	The presence of 'pay.sarral.io' and 'www.pay.sarral.io' suggests a payment gateway or related service. Without further information, it's impossible to determine the exact nature of the service. However, any vulnerability in a payment gateway could lead to the exposure of sensitive financial data, including credit card numbers, transaction history, and customer information. This could result in significant financial loss, reputational damage, and legal repercussions.
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 the 'pay.sarral.io' and 'www.pay.sarral.io' subdomains. Ensure that the payment gateway is PCI DSS compliant and that all security patches are up-to-date. Implement strong access controls and monitoring to prevent unauthorized access and detect suspicious activity. Consider implementing multi-factor authentication for administrative access to the payment gateway.

Finding SAR-003: Lack of DNSSEC (Medium)

Description:	The domain sarral.io does not have DNSSEC enabled. DNSSEC 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: Medium
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Implement DNSSEC by generating cryptographic keys and configuring the domain's DNS records with the appropriate digital signatures. Consult with the DNS provider (GoDaddy in this case) for specific instructions.

Finding SAR-004: 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-005: General Subdomain Takeover Risk (Medium)

Description:	Each subdomain, including 'sophie.sarral.io', 'www.pay.sarral.io', 'www.sarral.io', and 'pay.sarral.io', presents a potential subdomain takeover risk. This occurs when a subdomain points to a service that is no longer in use or has been misconfigured. An attacker could then claim the subdomain and use it to host malicious content, conduct phishing attacks, or damage the organization's reputation. The risk is lower if the subdomains are actively managed and properly configured, but it still exists.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

1. Regularly audit DNS records to identify orphaned or misconfigured subdomains. 2. Implement a process for decommissioning subdomains when they are no longer needed. 3. Use a subdomain takeover detection tool to proactively identify vulnerable subdomains. 4. Verify that all subdomains are properly configured and point to the intended resources. 5. Implement proper access controls to prevent unauthorized changes to DNS records.

Finding SAR-006: Unidentified Subdomain - 'sophie.sarral.io' (Medium)

Description:	The subdomain 'sophie.sarral.io' is of unknown purpose. It could be a development environment, a forgotten project, or a test server. If left unmanaged or improperly secured, it could be exploited by attackers to gain a foothold into the network or to host malicious content. Even if it's not directly related to critical systems, it could be used as a stepping stone for lateral movement within the network.
Risk:	Likelihood: Low Impact: Medium
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Investigate the purpose of the 'sophie.sarral.io' subdomain. If it's no longer needed, decommission it. If it's still in use, ensure that it's properly secured with appropriate access controls, security patches, and monitoring.

Consider implementing network segmentation to isolate it from critical systems.

Finding SAR-007: Missing Security Headers (Medium)

Description:	The main domains (sarral.io and www.sarral.io) and the sophie.sarral.io subdomain 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 Cross-Site Scripting (XSS), Clickjacking, and Man-in-the-Middle (MitM) attacks.
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 (though CSP is preferred).

Finding SAR-008: Connection Refused on sophie.sarral.io (HTTPS) (Medium)

Description:	The scan reports 'Connection Refused' errors when attempting to connect to sophie.sarral.io over HTTPS. This indicates that either the HTTPS service is not running on the server, a firewall is blocking the connection, or there is a network issue. While HTTP is responding, the lack of HTTPS is a security risk.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Ensure that the HTTPS service is properly configured and running on the server hosting sophie.sarral.io. Verify firewall rules to allow HTTPS traffic (port 443). Investigate any network issues that might be preventing HTTPS connections. Redirect HTTP to HTTPS to ensure secure communication.

Finding SAR-009: Outdated Apache Version (Medium)

Description:	The scan identifies that sarral.io and www.sarral.io are running Apache/2.4.58 (Ubuntu). While not severely outdated, using the latest stable version of Apache is crucial for patching known vulnerabilities and maintaining security. Older versions may contain exploitable flaws.
Risk:	Likelihood: Medium Impact: Medium
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Upgrade Apache to the latest stable version available for the Ubuntu operating system. Regularly check for and apply security patches to the web server software.

Finding SAR-010: Use of Privacy Service (Domains By Proxy) (Low)

Description:	The domain registrant information is hidden behind Domains By Proxy, LLC. While this protects the owner's privacy, it can also make it difficult to contact the owner directly in case of abuse or security concerns. It also makes it harder to verify the legitimacy of the domain.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Whois
References:	N/A

Remediation

Consider whether the privacy benefits outweigh the potential drawbacks of obscured ownership. If transparency is desired, the domain owner can choose to reveal their contact information. Ensure that the underlying contact information provided to Domains By Proxy is accurate and up-to-date.

Finding SAR-011: Information Disclosure via Subdomain Enumeration (Low)

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 identify potential attack vectors and plan targeted attacks. While not a direct vulnerability, it increases the attack surface and makes it easier for attackers to find weaknesses.
Risk:	Likelihood: High Impact: Low
System:	sarral.io
Tools Used:	Subfinder
References:	N/A

Remediation

1. Review the necessity of each subdomain and consider consolidating services where possible. 2. Implement proper access controls to restrict access to sensitive information on each subdomain. 3. Monitor subdomain usage for suspicious activity. 4. Consider using a Content Security Policy (CSP) to mitigate the risk of cross-site scripting (XSS) attacks.

Finding SAR-012: General Domain Security Posture (Low)

Description:	While the scan only provides a list of domains, it highlights the need for a comprehensive security assessment of the entire 'sarral.io' domain and its associated infrastructure. This includes identifying all assets, assessing their vulnerabilities, and implementing appropriate security controls. A proactive approach to security is essential to prevent attacks and protect sensitive data.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	Amass Passive
References:	N/A

Remediation

Conduct a comprehensive security assessment of the entire 'sarral.io' domain, including vulnerability scanning, penetration testing, and security configuration reviews. Implement a robust security monitoring and incident response plan. Regularly review and update security policies and procedures.

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: 404 Error on pay.sarral.io (Low)

Description:	The pay.sarral.io subdomain returns a 404 Not Found error. This could indicate a misconfiguration, an abandoned service, or a potential attack surface if the subdomain was intended for payment processing. The TLS certificate includes both pay.sarral.io and www.pay.sarral.io, suggesting it was intended to be a valid subdomain.
Risk:	Likelihood: Medium Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Investigate the purpose of the pay.sarral.io subdomain. If it's no longer needed, remove the DNS record and the associated TLS certificate entry. If it's intended to be a payment gateway, ensure it's properly configured and secured. A 404 error on a payment subdomain can damage trust and potentially lead to phishing attacks.

Finding SAR-015: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on multiple subdomains. While not a critical vulnerability on its own, TRACE can be used in conjunction with other vulnerabilities, such as Cross-Site Tracing (XST), to steal cookies or other sensitive information. Modern browsers have largely mitigated XST, but disabling TRACE is still 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 for all subdomains. This can typically be done by modifying the AllowMethods directive in Apache or similar configurations in other web servers.

Finding SAR-016: ReCaptcha API Key Exposure (Low)

Description:	The scan identifies a reCaptcha API key in the source code of www.sarral.io and sarral.io. While the key is likely a public key, it's important to ensure it's properly secured and not being abused. If the key is compromised, attackers could potentially use it to bypass reCaptcha protection on other sites.
Risk:	Likelihood: Low Impact: Low
System:	sarral.io
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Ensure the reCaptcha API key is properly secured and not being abused. Monitor the key for suspicious activity and consider rotating the key if necessary. Implement server-side validation of the reCaptcha response to prevent bypassing the protection.

Finding SAR-017: 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.
