SECURITY ASSESSMENT REPORT

Target: sagarsoft.in
Date: November 27, 2025
Scan ID: 46

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **sagarsoft.in** on 2025-11-27. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	4
Medium	20
Low	12
Info	6

2. Detailed Findings

1. HRMS and PMS Subdomains Security Risks

Severity: HIGH **Tool:** Amass Passive

Description:

The presence of 'hrms.sagarsoft.in' (Human Resources Management System) and 'pms.sagarsoft.in' (Project Management System) subdomains indicates the potential storage and processing of sensitive employee and project data. Compromise of these systems could lead to significant data breaches and reputational damage.

Remediation:

Implement strong access controls and authentication mechanisms for the HRMS and PMS systems. Regularly audit these systems for vulnerabilities and misconfigurations. Ensure data is encrypted both in transit and at rest. Implement robust logging and monitoring to detect and respond to suspicious activity. Conduct regular penetration testing to identify and address potential security weaknesses.

2. Potential Vulnerabilities in Human Resources Management System (HRMS)

Severity: HIGH **Tool:** Assetfinder

Description:

The 'hrms.sagarsoft.in' subdomain likely hosts a human resources management system. HRMS applications often contain highly sensitive employee data, such as personal information, salary details, performance reviews, and medical records. Vulnerabilities in the application could allow attackers to access or modify this data, leading to significant privacy breaches and legal liabilities.

Remediation:

Conduct a thorough security audit and penetration test of the HRMS application. Implement strong access controls and authentication mechanisms to protect sensitive data. Regularly update the application and its dependencies to patch known security flaws. Implement data loss prevention (DLP) measures to prevent unauthorized data exfiltration.

3. HTTP 502 - Bad Gateway

Severity: HIGH **Tool:** WafW00f

Description:

The server returned a 502 error, indicating that it acted as a gateway or proxy and received an invalid response from the upstream server. This could be due to network issues, server overload, or misconfigured proxy settings. It can lead to service unavailability and a poor user experience.

Remediation:

Investigate the upstream server to identify the cause of the invalid response. Check network connectivity and server resources to ensure that the server is not overloaded. Review proxy settings and ensure that they are correctly configured. Implement monitoring and alerting to detect and respond to 502 errors promptly.

---

4. HTTP 500 - Internal Server Error

Severity: HIGH **Tool:** WafW00f

Description:

The server returned a 500 error, indicating that an unexpected error occurred on the server. This could be due to a variety of factors, such as code errors, database issues, or server misconfigurations. It can lead to service unavailability and a poor user experience.

Remediation:

Review server logs to identify the cause of the error. Implement proper error handling and logging to provide more detailed information about errors. Debug and fix any code errors that are causing the errors. Ensure that the server is properly configured and that all dependencies are installed correctly. Implement monitoring and alerting to detect and respond to 500 errors promptly.

---

5. Redacted Contact Information

Severity: MEDIUM **Tool:** Whois

Description:

The Registrant, Admin, Tech, and Billing contact information is redacted for privacy. This makes it difficult to directly contact the domain owner or administrators in case of a security incident or to verify the legitimacy of the domain.

Remediation:

Consider using a privacy service that allows for contact through a proxy or provides a method for legitimate security researchers to contact the domain owner. Ensure that the registrar has a clear process for reporting security issues related to the domain.

6. Exposed Backend Subdomains

Severity: MEDIUM **Tool:** Subfinder

Description:

Subdomains like 'tsbackend.sagarsoft.in' and 'pmsbackend.sagarsoft.in' suggest the presence of backend systems directly exposed to the internet. This increases the risk of unauthorized access and data breaches if these systems are not properly secured.

Remediation:

Implement strict access controls and authentication mechanisms for all backend subdomains. Regularly audit and patch these systems for known vulnerabilities. Consider using a Web Application Firewall (WAF) to protect against common web attacks.

7. Potential for Outdated Software on Subdomains

Severity: MEDIUM **Tool:** Subfinder

Description:

The existence of multiple subdomains (e.g., 'pms.sagarsoft.in', 'hrms.sagarsoft.in', 'demo.sagarsoft.in') increases the likelihood that some may be running outdated or unpatched software, making them vulnerable to known exploits.

Remediation:

Implement a comprehensive vulnerability management program to regularly scan all subdomains for outdated software and known vulnerabilities. Establish a patching schedule to promptly address identified issues. Consider using a centralized management system for software updates.

8. Exposed 'demo' Subdomain

Severity: MEDIUM **Tool:** Amass Passive

Description:

The presence of a 'demo' subdomain often indicates a publicly accessible test environment. This environment may contain sensitive data, outdated software, or misconfigurations that could be exploited to gain unauthorized access to the main domain or other subdomains.

Remediation:

Review the 'demo' subdomain to ensure it does not contain sensitive data or expose vulnerabilities. Implement strong access controls and regularly update the software and configurations on the 'demo' environment. Consider removing the 'demo' subdomain if it is no longer needed.

9. Potential Email Server Vulnerabilities (mail.sagarsoft.in)

Severity: MEDIUM **Tool:** Amass Passive

Description:

The 'mail.sagarsoft.in' subdomain suggests the presence of a mail server. Mail servers are often targeted by attackers due to the sensitive information they handle and the potential for phishing attacks. Outdated mail server software or misconfigurations can lead to vulnerabilities.

Remediation:

Ensure the mail server software is up-to-date with the latest security patches. Implement strong authentication mechanisms, such as multi-factor authentication (MFA). Regularly review mail server configurations to identify and address any potential vulnerabilities. Implement SPF, DKIM, and DMARC records to prevent email spoofing.

10. Timesheet Subdomain Security Risks

Severity: MEDIUM **Tool:** Amass Passive

Description:

The 'timesheet.sagarsoft.in' subdomain likely handles employee time tracking data, which can include sensitive information such as work hours, project assignments, and potentially billing rates. A vulnerability in this system could expose this data to unauthorized access.

Remediation:

Implement strong access controls and authentication mechanisms for the timesheet system. Regularly audit the system for vulnerabilities and misconfigurations. Ensure data is encrypted both in transit and at rest. Implement robust logging and monitoring to detect and respond to suspicious activity.

---

11. Exposed Demo Environment

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'demo.sagarsoft.in' subdomain may contain a publicly accessible demonstration environment. Demo environments often contain default credentials, outdated software, or sensitive data that can be exploited by attackers to gain unauthorized access to the system or network.

Remediation:

Implement strong authentication and authorization mechanisms for the demo environment. Regularly update the software and configurations to the latest versions. Consider restricting access to the demo environment to authorized personnel only or removing it entirely if no longer needed.

---

12. Lack of HTTPS on Subdomains

Severity: MEDIUM **Tool:** Assetfinder

Description:

The scan output doesn't explicitly state the use of HTTPS, but it's a common vulnerability. If subdomains like 'timesheet.sagarsoft.in', 'pms.sagarsoft.in', and 'hrms.sagarsoft.in' are not using HTTPS, sensitive data transmitted between the user and the server can be intercepted by attackers.

Remediation:

Implement HTTPS on all subdomains to encrypt data in transit. Obtain and install SSL/TLS certificates for each subdomain and configure the web servers to enforce HTTPS connections. Redirect HTTP traffic to HTTPS.

13. Potential Vulnerabilities in Timesheet Application

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'timesheet.sagarsoft.in' subdomain likely hosts a timesheet application. Timesheet applications often handle sensitive employee data, such as work hours, project details, and potentially salary information. Vulnerabilities in the application, such as SQL injection or cross-site scripting (XSS), could allow attackers to access or modify this data.

Remediation:

Conduct a thorough security audit and penetration test of the timesheet application. Implement secure coding practices to prevent common web application vulnerabilities. Regularly update the application and its dependencies to patch known security flaws.

14. Potential Vulnerabilities in Project Management System (PMS)

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'pms.sagarsoft.in' subdomain likely hosts a project management system. PMS applications often contain sensitive project data, such as project plans, budgets, and client information. Vulnerabilities in the application could allow attackers to access or modify this data.

Remediation:

Conduct a thorough security audit and penetration test of the PMS application. Implement secure coding practices to prevent common web application vulnerabilities. Regularly update the application and its dependencies to patch known security flaws.

15. SSL Certificate Hostname Mismatch

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The SSL certificate for mail.sagarsoft.in does not match the hostname, indicating a potential man-in-the-middle attack or misconfiguration. The certificate is issued to outlook.com, suggesting a redirection to Microsoft's mail service, but the initial connection attempt to mail.sagarsoft.in fails due to the hostname mismatch.

Remediation:

Ensure the SSL certificate for mail.sagarsoft.in is correctly configured and valid for the domain. If the intention is to redirect to outlook.com, ensure the redirection is properly implemented and the certificate on the outlook.com side is valid.

---

16. Missing Security Headers

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The main websites (www.sagarsoft.in and sagarsoft.in) are missing crucial security headers such as HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and X-XSS-Protection. This makes the website vulnerable to various attacks like cross-site scripting (XSS), clickjacking, and MIME-sniffing attacks.

Remediation:

Implement the following security headers: - Strict-Transport-Security (HSTS) to enforce HTTPS. - Content-Security-Policy (CSP) to prevent XSS attacks. - X-Frame-Options to prevent clickjacking. - X-Content-Type-Options to prevent MIME-sniffing. - Referrer-Policy to control referrer information. - X-XSS-Protection to enable XSS filtering in older browsers.

---

17. Subdomain Inaccessibility (Connection Refused)

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

Multiple subdomains (demo.sagarsoft.in, pmsbackend.sagarsoft.in, pms.sagarsoft.in, timesheet.sagarsoft.in, tsbackend.sagarsoft.in) are inaccessible due to 'Connection refused' errors. This could indicate service outages, misconfiguration, or intentional blocking. hrms.sagarsoft.in is inaccessible due to connection timeout.

Remediation:

Investigate the server configuration and status of each inaccessible subdomain. Ensure the services are running, the firewall is properly configured, and DNS records are correctly pointing to the servers. Address the timeout issue for hrms.sagarsoft.in by checking network connectivity and server responsiveness.

---

18. Outdated Apache HTTPD Version

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

Description:

The Apache HTTPD version 2.4.52 is known to have potential vulnerabilities. While it's not ancient, newer versions contain security patches and improvements. Exploits targeting this specific version may exist or be developed.

Remediation:

Upgrade Apache HTTPD to the latest stable version available for Ubuntu. Regularly apply security patches and updates to the server operating system and all installed software.

---

19. Outdated WordPress Version

Severity: MEDIUM **Tool:** WhatWeb

Description:

The website is running WordPress version 6.4.3. While not severely outdated, it's crucial to keep WordPress updated to the latest version to patch security vulnerabilities and benefit from performance improvements. Older versions may have known exploits.

Remediation:

Update WordPress to the latest stable version. Regularly check for updates and apply them promptly.

20. Outdated Slider Revolution Plugin

Severity: MEDIUM **Tool:** WhatWeb

Description:

The website is using Slider Revolution version 6.5.8. Older versions of Slider Revolution have been known to have security vulnerabilities, including remote code execution. It's crucial to keep this plugin updated.

Remediation:

Update the Slider Revolution plugin to the latest stable version. Regularly check for updates and apply them promptly.

21. Outdated WPBakery Page Builder Plugin

Severity: MEDIUM **Tool:** WhatWeb

Description:

The website is using WPBakery Page Builder. While the version is not explicitly stated, it's important to ensure it's up-to-date. Outdated versions of WPBakery Page Builder have been known to have security vulnerabilities.

Remediation:

Update the WPBakery Page Builder plugin to the latest stable version. Regularly check for updates and apply them promptly.

22. HTTP 405 - Not Allowed

Severity: MEDIUM **Tool:** WafW00f

Description:

The server returned a 405 error, indicating that the HTTP method used in the request is not allowed for the requested resource. This could be due to misconfigured server settings or incorrect API endpoint configurations. It might also indicate an attempt to exploit a vulnerability by using an unexpected HTTP method.

Remediation:

Review server configuration and API endpoint definitions to ensure that allowed HTTP methods are correctly configured. Implement proper input validation and sanitization to prevent malicious requests from reaching the server. Consider implementing rate limiting to prevent abuse.

---

23. HTTP 403 - Forbidden

Severity: MEDIUM **Tool:** WafW00f

Description:

The server returned a 403 error, indicating that the server understands the request but refuses to authorize it. This could be due to incorrect file permissions, IP address restrictions, or other access control mechanisms. It might also indicate an attempt to access sensitive resources without proper authorization.

Remediation:

Review file permissions and access control lists to ensure that only authorized users can access sensitive resources. Implement proper authentication and authorization mechanisms to verify user identity and grant appropriate access privileges. Monitor 403 errors to identify potential unauthorized access attempts.

---

24. Lack of WAF

Severity: MEDIUM **Tool:** WafW00f

Description:

The scan did not detect a Web Application Firewall (WAF). A WAF provides an additional layer of security by filtering malicious traffic and protecting against common web application attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

Remediation:

Implement a Web Application Firewall (WAF) to protect against common web application attacks. Configure the WAF to block malicious traffic and monitor for suspicious activity. Regularly update the WAF rules to protect against new threats.

25. Reliance on RDDS Queries for Contact Information

Severity: LOW **Tool:** Whois

Description:

The WHOIS output instructs users to query the RDDS service for contact information. This adds an extra step and potential complexity for security researchers or law enforcement trying to reach the domain owner, potentially delaying incident response.

Remediation:

Ensure the RDDS service is properly configured and accessible. Consider providing a direct contact method for security-related inquiries, even if other contact information is redacted.

26. Inconsistent Updated Date

Severity: LOW **Tool:** Whois

Description:

The WHOIS output contains two different sets of data with different 'Updated Date' values (2025-06-01 and 2021-04-24). This inconsistency could indicate data synchronization issues or potentially manipulation.

Remediation:

Investigate the discrepancy in the 'Updated Date' values by querying the RDAP service and comparing the results. Contact the registrar (GoDaddy) to clarify the reason for the inconsistency.

27. Single Point of Failure (Single IP Address)

Severity: LOW **Tool:** NSLookup

Description:

The domain resolves to a single IP address. This creates a single point of failure. If the server at that IP address becomes unavailable, the website will be inaccessible. It also makes the server a more attractive target for DDoS attacks.

Remediation:

Implement redundancy by using multiple servers with different IP addresses. Consider using a Content Delivery Network (CDN) to distribute the website's content across multiple servers and geographic locations. This will improve availability and resilience against attacks.

28. Information Disclosure via 'demo.sagarsoft.in'

Severity: LOW **Tool:** Subfinder

Description:

The 'demo.sagarsoft.in' subdomain may contain sensitive information or configurations intended for demonstration purposes only. If not properly secured, it could lead to information disclosure.

Remediation:

Review the content and configuration of the 'demo.sagarsoft.in' subdomain to ensure that no sensitive information is exposed. Implement access controls to restrict access to authorized personnel only. Consider using dummy data instead of real data in the demo environment.

29. General Subdomain Takeover Risk

Severity: LOW **Tool:** Amass Passive

Description:

Each subdomain represents a potential target for subdomain takeover if the DNS records point to a service that is no longer in use or is misconfigured. An attacker could claim the subdomain and use it for malicious purposes, such as phishing or distributing malware.

Remediation:

Regularly audit DNS records to ensure they are accurate and point to active services. Implement monitoring to detect any changes to DNS records. Implement preventative measures to avoid dangling DNS records.

30. Subdomain Takeover Vulnerability

Severity: LOW **Tool:** Assetfinder

Description:

If any of these subdomains are pointing to a service that is no longer in use or has been misconfigured (e.g., pointing to a non-existent cloud service), an attacker could potentially claim the subdomain and use it for malicious purposes, such as phishing or distributing malware.

Remediation:

Regularly audit DNS records to ensure that all subdomains are pointing to valid and active services. Remove any orphaned or misconfigured DNS records. Implement subdomain takeover prevention measures, such as using a CNAME record to point to a service that is actively monitored and protected.

31. Excessive Phone Numbers Exposed

Severity: LOW **Tool:** WebScraperRecon

Description:

The main websites (www.sagarsoft.in and sagarsoft.in) expose a large number of phone numbers. While some may be legitimate contact numbers, the sheer quantity and format variations raise concerns about potential data leakage or scraping, which could be used for social engineering or spam campaigns.

Remediation:

Review the website content and remove any unnecessary or outdated phone numbers. Implement measures to prevent phone number scraping, such as CAPTCHAs or rate limiting. Educate employees about potential social engineering attacks targeting these exposed numbers.

32. Name Resolution Errors for www Subdomains

Severity: LOW **Tool:** WebScraperRecon

Description:

The 'www' subdomains for pmsbackend, pms, timesheet, and tsbackend fail to resolve, indicating a DNS configuration issue. While the non-www versions also have connection issues, this DNS problem adds another layer of inaccessibility.

Remediation:

Verify and correct the DNS records for the 'www' subdomains to ensure they properly resolve to the server IP address. This may involve adding or modifying A records or CNAME records in the DNS zone file.

33. Exposed Apache Version Information

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

Description:

The Nmap scan was able to identify the specific version of Apache HTTPD running on the server. This information can be used by attackers to target known vulnerabilities specific to that version.

Remediation:

Configure Apache to suppress the display of the server version in HTTP responses. This can be done by modifying the `ServerTokens` and `ServerSignature` directives in the Apache configuration file (e.g., `httpd.conf` or `apache2.conf`). Set `ServerTokens Prod` and `ServerSignature Off`.

34. Lack of HTTP to HTTPS Redirection

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

Description:

The server is running on both port 80 (HTTP) and port 443 (HTTPS). Users accessing the site via HTTP may be vulnerable to man-in-the-middle attacks if they are not automatically redirected to the secure HTTPS version.

Remediation:

Implement a permanent (301) redirect from HTTP to HTTPS. This can be done in the Apache configuration file or using a `.htaccess` file. Ensure all traffic is forced to use HTTPS for secure communication.

35. Outdated Bootstrap Version

Severity: LOW **Tool:** WhatWeb

Description:

The website is using Bootstrap version 1.1.1. This is a very old version of Bootstrap. While the impact might be limited, using such an old version can introduce compatibility issues and potentially expose the site to vulnerabilities present in older versions of the framework.

Remediation:

Update Bootstrap to the latest stable version. Ensure compatibility with the existing website design and functionality.

36. HTTP 404 - Hack Not Found

Severity: LOW **Tool:** WafW00f

Description:

The server returned a 404 error, indicating that the requested resource (likely a probe by WafW00f) was not found. While not directly a vulnerability, excessive 404 errors can indicate broken links, misconfigured URLs, or attempts to access non-existent resources, potentially revealing information about the application's structure.

Remediation:

Review website links and ensure all resources are accessible. Implement custom 404 error pages to provide a better user experience and prevent information leakage. Monitor 404 errors to identify potential issues.

37. Outdated WHOIS Server

Severity: INFO **Tool:** Whois

Description:

The WHOIS output indicates that the WHOIS server is being retired and suggests using RDAP instead. Continuing to rely on the outdated WHOIS server may result in inaccurate or unavailable information.

Remediation:

Transition to using RDAP (Registration Data Access Protocol) for domain information retrieval. Update scripts and tools to use RDAP endpoints instead of the WHOIS server.

---

38. Standard Domain Status Locks

Severity: INFO **Tool:** Whois

Description:

The domain has clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, and clientRenewProhibited status codes. While these are good security practices, they are standard and don't represent a specific vulnerability.

Remediation:

These locks are already in place and should be maintained to prevent unauthorized changes to the domain registration.

---

39. Lack of DNS Security Records (e.g., DNSSEC)

Severity: INFO **Tool:** NSLookup

Description:

The NSLookup output doesn't provide information about DNSSEC records (like DS, DNSKEY, RRSIG). The absence of DNSSEC makes the domain vulnerable to DNS spoofing and cache poisoning attacks, where attackers can redirect users to malicious websites by manipulating DNS records.

Remediation:

Implement DNSSEC by generating cryptographic keys and signing the DNS zone. Publish the DS record with the domain registrar. Regularly monitor DNSSEC configuration for errors.

40. Lack of Security Headers on Subdomains

Severity: INFO **Tool:** Subfinder

Description:

The scan doesn't provide information about security headers. Subdomains might be missing crucial security headers (e.g., HSTS, X-Frame-Options, Content-Security-Policy), making them vulnerable to various attacks like clickjacking and cross-site scripting (XSS).

Remediation:

Implement security headers on all subdomains to enhance their security posture. Use a tool like securityheaders.com to analyze the current header configuration and identify missing or misconfigured headers.

41. Email Address Exposure

Severity: INFO **Tool:** WhatWeb

Description:

The website exposes email addresses (info@sagarsoft.com, info@sagarsoft.in, info@infowaysoftware.com) in the HTML source. This can make the website a target for spam and phishing campaigns.

Remediation:

Implement measures to obfuscate or protect email addresses from being easily harvested by bots. Consider using a contact form instead of directly displaying email addresses.

42. X-Redirect-By Header

Severity: INFO **Tool:** WhatWeb

Description:

The presence of the 'X-Redirect-By' header can sometimes reveal information about the redirect mechanism used by the server. While not a direct vulnerability, it can aid attackers in understanding the server's configuration.

Remediation:

Consider removing or masking the 'X-Redirect-By' header to reduce information leakage. This can usually be configured in the web server settings.

3. Appendix: Raw Tool Output

The following section contains raw output from the security tools used during the assessment.

Tool: Whois

```
Domain Name: sagarsoft.in Registry Domain ID: D2196678-IN Registrar WHOIS Server:
whois.godaddy.com Registrar URL: www.godaddy.com Updated Date: 2025-06-01T19:23:52.269Z
Creation Date: 2006-03-09T14:29:29.513Z Registry Expiry Date: 2027-03-09T14:29:29.513Z
Registrar: GoDaddy Registrar IANA ID: 146 Registrar Abuse Contact Email:
reg_admin@godaddy.com Registrar Abuse Contact Phone: +1.4805058800 Domain Status:
clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status:
clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status:
clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status:
clientRenewProhibited https://icann.org/epp#clientRenewProhibited Registry Registrant
ID: REDACTED FOR PRIVACY Registrant Name: REDACTED FOR PRIVACY Registrant Organization:
Sagarsoft (India) Ltd., Registrant Street: REDACTED FOR PRIVACY Registrant City:
REDACTED FOR PRIVACY Registrant State/Province: Telangana Registrant Postal Code:
REDACTED FOR PRIVACY Registrant Country: IN Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY Registrant Email: Please query the RDDS service of
the Registrar of Record identified in this output for information on how to contact the
Registrant, Admin, or Tech contact of the queried domain name. Registry Admin ID:
REDACTED FOR PRIVACY Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR
PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin
State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin
Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Fax: REDACTED FOR
PRIVACY Admin Email: Please query the RDDS service of the Registrar of Record identified
in this output for information on how to contact the Registrant, Admin, or Tech contact
of the queried domain name. Registry Tech ID: REDACTED FOR PRIVACY Tech Name: REDACTED
FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal
Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR
PRIVACY Tech Fax: REDACTED FOR PRIVACY Tech Email: Please query the RDDS service of the
Registrar of Record identified in this output for information on how to contact the
Registrant, Admin, or Tech contact of the queried domain name. Registry Billing ID:
REDACTED FOR PRIVACY Billing Name: REDACTED FOR PRIVACY Billing Organization: REDACTED
FOR PRIVACY Billing Street: REDACTED FOR PRIVACY Billing City: REDACTED FOR PRIVACY
Billing State/Province: REDACTED FOR PRIVACY Billing Postal Code: REDACTED FOR PRIVACY
Billing Country: REDACTED FOR PRIVACY Billing Phone: REDACTED FOR PRIVACY Billing Fax:
REDACTED FOR PRIVACY Billing Email: Please query the RDDS service of the Registrar of
Record identified in this output for information on how to contact the Registrant,
Admin, or Tech contact of the queried domain name. Name Server: ns56.domaincontrol.com
Name Server: ns55.domaincontrol.com DNSSEC: unsigned URL of the ICANN RDDS Inaccuracy
Complaint Form: https://icann.org/wicf >>> Last update of WHOIS database:
2025-11-27T09:20:28.863Z <<< For more information on domain status codes, please visit
https://icann.org/epp The WHOIS information provided in this page has been redacted in
compliance with ICANN's Temporary Specification for gTLD Registration Data. The data in
this record is provided by Tucows Registry for informational purposes only, and it does
not guarantee its accuracy. Tucows Registry is authoritative for whois information in
top-level domains it operates under contract with the Internet Corporation for Assigned
Names and Numbers. Whois information from other top-level domains is provided by a
third-party under license to Tucows Registry. This service is intended only for
query-based access. By using this service, you agree that you will use any data
presented only for lawful purposes and that, under no circumstances will you use (a)
data acquired for the purpose of allowing, enabling, or otherwise supporting the
transmission by e-mail, telephone, facsimile or other communications mechanism of mass
unsolicited, commercial advertising or solicitations to entities other than your
existing customers; or (b) this service to enable high volume, automated, electronic
```

```
processes that send queries or data to the systems of any Registrar or any Registry
except as reasonably necessary to register domain names or modify existing domain name
registrations. Tucows Registry reserves the right to modify these terms at any time. By
submitting this query, you agree to abide by this policy. All rights reserved. Domain
Name: sagarsoft.in Registry Domain ID: D2196678-IN Registrar WHOIS Server:
whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date:
2021-04-24T07:28:30Z Creation Date: 2006-03-09T14:29:29Z Registrar Registration
Expiration D ...[Truncated]
```

Tool: NSLookup

```
Server: 10.77.145.30 Address: 10.77.145.30#53 Non-authoritative answer: Name:
sagarsoft.in Address: 65.20.67.161
```

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 sagarsoft.in pmsbackend.sagarsoft.in [INF] Found 7
subdomains for sagarsoft.in in 11 seconds 542 milliseconds timesheet.sagarsoft.in
tsbackend.sagarsoft.in www.sagarsoft.in demo.sagarsoft.in hrms.sagarsoft.in
pms.sagarsoft.in
```

Tool: Amass Passive

```
www.sagarsoft.in hrms.sagarsoft.in demo.sagarsoft.in pmsbackend.sagarsoft.in
mail.sagarsoft.in pms.sagarsoft.in sagarsoft.in timesheet.sagarsoft.in
tsbackend.sagarsoft.in The enumeration has finished Discoveries are being migrated into
the local database
```

Tool: Assetfinder

```
www.sagarsoft.in timesheet.sagarsoft.in tsbackend.sagarsoft.in hrms.sagarsoft.in
pms.sagarsoft.in demo.sagarsoft.in pmsbackend.sagarsoft.in sagarsoft.in
www.sagarsoft.in sagarsoft.in
```

Tool: WebScraperRecon

```
{"demo.sagarsoft.in": {"target": "demo.sagarsoft.in", "base_url":
"https://demo.sagarsoft.in", "alive": false, "pages_visited": 0, "max_depth": 2,
"emails": [], "phones": [], "internal_ips": [], "social_profiles": [], "api_endpoints":
[], "comments": [], "visited_urls": [], "errors": ["[probe] https://demo.sagarsoft.in
-> HTTPSConnectionPool(host='demo.sagarsoft.in', port=443): Max retries exceeded with
url: / (Caused by NewConnectionError(': Failed to establish a new connection: [Errno
111] Connection refused'))", "[probe] https://demo.sagarsoft.in ->
HTTPSConnectionPool(host='demo.sagarsoft.in', port=443): Max retries exceeded with url:
/ (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111]
Connection refused'))", "[probe] http://demo.sagarsoft.in ->
```

HTTPConnectionPool(host='demo.sagarsoft.in', port=80): Max retries exceeded with url: / (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111] Connection refused'))", "[probe] https://www.demo.sagarsoft.in -> HTTPSConnectionPool(host='www.demo.sagarsoft.in', port=443): Max retries exceeded with url: / (Caused by NameResolutionError(\": Failed to resolve 'www.demo.sagarsoft.in' ([Errno -2] Name or service not known)\"))", "[probe] http://www.demo.sagarsoft.in -> HTTPConnectionPool(host='www.demo.sagarsoft.in', port=80): Max retries exceeded with url: / (Caused by NameResolutionError(\": Failed to resolve 'www.demo.sagarsoft.in' ([Errno -2] Name or service not known)\"))"], "duration_sec": 0.88, "resolved_ips": ["65.20.67.161"], "http_probe": {}, "tls_info": {}, "headers": {}, "security_headers": {}, "favicon_hash": {}, "technologies": [], "waf": "", "http_methods": []}, "pmsbackend.sagarsoft.in": {"target": "pmsbackend.sagarsoft.in", "base_url": "https://pmsbackend.sagarsoft.in", "alive": false, "pages_visited": 0, "max_depth": 2, "emails": [], "phones": [], "internal_ips": [], "social_profiles": [], "api_endpoints": [], "comments": [], "visited_urls": [], "errors": ["[probe] https://pmsbackend.sagarsoft.in -> HTTPSConnectionPool(host='pmsbackend.sagarsoft.in', port=443): Max retries exceeded with url: / (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111] Connection refused'))", "[probe] https://pmsbackend.sagarsoft.in -> HTTPSConnectionPool(host='pmsbackend.sagarsoft.in', port=443): Max retries exceeded with url: / (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111] Connection refused'))", "[probe] http://pmsbackend.sagarsoft.in -> HTTPConnectionPool(host='pmsbackend.sagarsoft.in', port=80): Max retries exceeded with url: / (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111] Connection refused'))", "[probe] https://www.pmsbackend.sagarsoft.in -> HTTPSConnectionPool(host='www.pmsbackend.sagarsoft.in', port=443): Max retries exceeded with url: / (Caused by NameResolutionError(\": Failed to resolve 'www.pmsbackend.sagarsoft.in' ([Errno -2] Name or service not known)\"))", "[probe] http://www.pmsbackend.sagarsoft.in -> HTTPConnectionPool(host='www.pmsbackend.sagarsoft.in', port=80): Max retries exceeded with url: / (Caused by NameResolutionError(\": Failed to resolve 'www.pmsbackend.sagarsoft.in' ([Errno -2] Name or service not known)\"))"], "duration_sec": 1.23, "resolved_ips": ["65.20.67.161"], "http_probe": {}, "tls_info": {}, "headers": {}, "security_headers": {}, "favicon_hash": {}, "technologies": [], "waf": "", "http_methods": []}, "pms.sagarsoft.in": {"target": "pms.sagarsoft.in", "base_url": "https://pms.sagarsoft.in", "alive": false, "pages_visited": 0, "max_depth": 2, "emails": [], "phones": [], "internal_ips": [], "social_profiles": [], "api_endpoints": [], "comments": [], "visited_urls": [], "errors": ["[probe] https://pms.sagarsoft.in -> HTTPSConnectionPool(host='pms.sagarsoft.in', port=443): Max retries exceeded with url: / (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111] Connection refused'))", "[probe] https://pms.sagarsoft.in -> HTTPSConnectionPool(host='pms.sagarsoft.in', port=443): Max retries exceeded with url: / (Caused by NewConnectionError(': Failed to establish a new connection: [Errno 111] Connection refused'))", "[probe] http://pms.sagarsoft ...[Truncated]

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 04:22 EST Nmap scan report for sagarsoft.in (65.20.67.161) Host is up (0.046s latency). rDNS record for 65.20.67.161: 65.20.67.161.vultrusercontent.com Not shown: 998 filtered tcp ports (no-response) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.52 ((Ubuntu)) 443/tcp open ssl/http Apache httpd 2.4.52 Service Info: Host: sagarsoft.com Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 22.18 seconds
```

Tool: WhatWeb

```
http://sagarsoft.in [301 Moved Permanently] Apache[2.4.52], Country[UNITED STATES][US],
HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[65.20.67.161],
RedirectLocation[http://www.sagarsoft.in/], UncommonHeaders[x-redirect-by]
https://sagarsoft.in [301 Moved Permanently] Apache[2.4.52], Country[UNITED
STATES][US], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[65.20.67.161],
RedirectLocation[https://www.sagarsoft.in/], UncommonHeaders[x-redirect-by]
http://www.sagarsoft.in/ [200 OK] Apache[2.4.52], Bootstrap[1.1.1], Country[UNITED
STATES][US],
Email[Group-8609@2x.png,info@infowaysoftware.com,info@sagarsoft.com,info@sagarsoft.in],
HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[65.20.67.161],
JQuery[3.7.1], MetaGenerator[Elementor 3.21.0; features: e_optimized_assets_loading,
e_optimized_css_loading, additional_custom_breakpoints; settings:
css_print_method-external, google_font-enabled, font_display-swap,Powered by Slider
Revolution 6.5.8 - responsive, Mobile-Friendly Slider Plugin for WordPress with
comfortable drag and drop interface.,Powered by WPBakery Page Builder - drag and drop
page builder for WordPress.,WordPress 6.4.3], PoweredBy[Slider,WPBakery],
Script[text/html,text/javascript], Title[Sagarsoft], UncommonHeaders[link],
WordPress[6.4.3] https://www.sagarsoft.in/ [200 OK] Apache[2.4.52], Bootstrap[1.1.1],
Country[UNITED STATES][US],
Email[Group-8609@2x.png,info@infowaysoftware.com,info@sagarsoft.com,info@sagarsoft.in],
HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[65.20.67.161],
JQuery[3.7.1], MetaGenerator[Elementor 3.21.0; features: e_optimized_assets_loading,
e_optimized_css_loading, additional_custom_breakpoints; settings:
css_print_method-external, google_font-enabled, font_display-swap,Powered by Slider
Revolution 6.5.8 - responsive, Mobile-Friendly Slider Plugin for WordPress with
comfortable drag and drop interface.,Powered by WPBakery Page Builder - drag and drop
page builder for WordPress.,WordPress 6.4.3], PoweredBy[Slider,WPBakery],
Script[text/html,text/javascript], Title[Sagarsoft], UncommonHeaders[link],
WordPress[6.4.3]
```

Tool: WafW00f

```
______ / \ ( W00f! ) \ ____/ ,, __ 404 Hack Not Found |`-.__ / / __ __ /" _/ /_/ \ \ / /
*===* / \ \_/ / 405 Not Allowed / )__// \ / /| / /---` 403 Forbidden \\/` \ | / _ \ `\
/_\\_ 502 Bad Gateway / / \ \ 500 Internal Error `_____``-` /_/ \_\\ ~ WAFW00F : v2.3.1
~ The Web Application Firewall Fingerprinting Toolkit [*] Checking https://sagarsoft.in
[+] Generic Detection results: [-] No WAF detected by the generic detection [~] Number
of requests: 7
```