SECURITY ASSESSMENT REPORT

Target: sagarsoft.in
Date: November 26, 2025
Scan ID: 40

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **sagarsoft.in** on 2025-11-26. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	3
Medium	8
Low	6
Info	3

2. Detailed Findings

1. Exposed HR Management System (HRMS)

Severity: HIGH **Tool:** Subfinder

Description:

The subdomain 'hrms.sagarsoft.in' suggests the presence of a Human Resources Management System. HRMS systems typically contain highly sensitive employee data, including personal information, performance reviews, salary details, and banking information. A breach of this system could have severe legal and reputational consequences.

Remediation:

Implement multi-factor authentication (MFA) for all HRMS users. Enforce strict access control policies based on the principle of least privilege. Regularly audit the HRMS for security vulnerabilities and misconfigurations. Encrypt sensitive data both in transit and at rest. Consider data loss prevention (DLP) measures.

2. Exposed Demo Environment

Severity: HIGH **Tool:** Assetfinder

Description:

The subdomain 'demo.sagarsoft.in' suggests a demo environment. Demo environments often have weaker security controls than production environments and may contain sensitive data or vulnerable code. If compromised, an attacker could use this environment to gain a foothold into the internal network or access production data.

Remediation:

Immediately review the security configuration of the demo environment. Remove any sensitive data, implement strong authentication, and ensure the environment is isolated from the production network. Consider using dummy data or anonymized data in the demo environment. If the demo environment is no longer needed, decommission it.

3. HRMS Exposure

Severity: HIGH **Tool:** Assetfinder

Description:

The subdomain 'hrms.sagarsoft.in' indicates a Human Resources Management System. HRMS systems contain highly sensitive employee data, including personal information, salary details, performance reviews, and other confidential records. A compromise of the HRMS could lead to identity theft, financial fraud, and significant reputational damage.

Remediation:

Conduct an immediate and thorough security audit of the HRMS. Implement multi-factor authentication, strong access controls, and data encryption. Regularly update the HRMS and its dependencies. Ensure compliance with relevant data privacy regulations. Consider penetration testing to identify and address any vulnerabilities.

4. Privacy Redaction Hinders Contact

Severity: MEDIUM **Tool:** Whois

Description:

The Registrant, Admin, Tech, and Billing contact information are redacted for privacy. This makes it difficult to directly contact the domain owner or administrators for legitimate purposes, such as security concerns or policy violations. While privacy is important, it can also be abused.

Remediation:

Consider using a contact form or a publicly available security contact email address on the website associated with the domain. Ensure that the registrar has accurate and up-to-date contact information, even if it's not publicly displayed.

5. Exposed Timesheet Application

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'timesheet.sagarsoft.in' suggests the existence of a timesheet application. If not properly secured, this application could expose sensitive employee data such as work hours, project assignments, and potentially salary information.

Remediation:

Implement strong authentication and authorization mechanisms for the timesheet application. Regularly audit access logs and ensure data is encrypted both in transit and at rest. Conduct a penetration test to identify vulnerabilities.

6. Exposed Project Management System (PMS)

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'pms.sagarsoft.in' indicates a Project Management System. This system likely contains sensitive project-related data, including client information, project plans, budgets, and internal communications. Unauthorized access could lead to data breaches and competitive disadvantage.

Remediation:

Implement robust access controls and authentication for the PMS. Regularly update the PMS software to patch known vulnerabilities. Conduct security awareness training for employees using the PMS.

7. Backend API Exposure

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomains 'tsbackend.sagarsoft.in' and 'pmsbackend.sagarsoft.in' suggest the existence of backend APIs for the timesheet and project management systems, respectively. If these APIs are not properly secured, they could be vulnerable to attacks such as API injection, broken authentication, and excessive data exposure.

Remediation:

Implement strong authentication and authorization for all backend APIs. Use API gateways to manage and secure API traffic. Regularly audit the APIs for security vulnerabilities. Implement rate limiting to prevent denial-of-service attacks. Ensure proper input validation and output encoding to prevent injection attacks.

8. Sensitive Subdomain Exposure

Severity: MEDIUM

Tool: Amass Passive

Description:

The discovery of subdomains like 'timesheet.sagarsoft.in', 'pms.sagarsoft.in', and 'hrms.sagarsoft.in' suggests the presence of sensitive applications. If these applications are not properly secured, they could be vulnerable to unauthorized access, data breaches, or other attacks.

Remediation:

Conduct thorough security assessments (penetration testing, vulnerability scanning) of each sensitive subdomain. Implement strong authentication and authorization mechanisms. Ensure data is encrypted both in transit and at rest. Regularly update software and apply security patches.

9. Exposed Timesheet Application

Severity: MEDIUM

Tool: Assetfinder

Description:

The subdomain 'timesheet.sagarsoft.in' suggests a timesheet application. If not properly secured, this could expose sensitive employee data such as work hours, project details, and potentially salary information. Weak authentication, authorization flaws, or SQL injection vulnerabilities could lead to data breaches.

Remediation:

Conduct a thorough security audit of the timesheet application, focusing on authentication, authorization, and input validation. Implement multi-factor authentication, regularly update the application and its dependencies, and ensure proper access controls are in place.

10. Exposed Project Management System (PMS)

Severity: MEDIUM

Tool: Assetfinder

Description:

The subdomain 'pms.sagarsoft.in' indicates a Project Management System. Similar to the timesheet application, a vulnerable PMS could expose sensitive project data, client information, and internal communications. Unauthorized access could lead to data leaks, competitive disadvantage, or reputational damage.

Remediation:

Perform a comprehensive security assessment of the PMS, paying close attention to access controls, data encryption, and input validation. Implement strong authentication mechanisms, regularly patch the system, and restrict access based on the principle of least privilege.

11. Backend Services Exposure

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomains 'tsbackend.sagarsoft.in' and 'pmsbackend.sagarsoft.in' suggest backend services for the timesheet and project management systems, respectively. Exposing backend services directly to the internet is a significant security risk. These services may lack proper authentication or authorization, allowing attackers to bypass front-end security measures and directly access sensitive data or execute arbitrary code.

Remediation:

Restrict access to the backend services to only authorized internal networks or specific IP addresses. Implement strong authentication and authorization mechanisms for all backend services. Use a web application firewall (WAF) to protect against common web attacks. Regularly monitor the backend services for suspicious activity.

12. Reliance on Registrar's WHOIS Service

Severity: LOW **Tool:** Whois

Description:

The WHOIS output indicates a reliance on the registrar's (GoDaddy) WHOIS service for contact information. If GoDaddy's service is compromised or unavailable, it could hinder communication with the domain owner.

Remediation:

Maintain redundant contact information through other channels, such as a security.txt file on the website or a publicly listed security contact email address.

13. DNSSEC Unsigned

Severity: LOW **Tool:** Whois

Description:

The domain is not using DNSSEC. DNSSEC helps prevent DNS spoofing and cache poisoning attacks by digitally signing DNS records.

Remediation:

Implement DNSSEC to improve the security and integrity of the domain's DNS records. Consult with the registrar or DNS provider for instructions on enabling DNSSEC.

14. 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.

15. Exposed Demo Environment

Severity: LOW **Tool:** Subfinder

Description:

The subdomain 'demo.sagarsoft.in' suggests a demo environment. Demo environments often have weaker security controls than production environments, making them a potential entry point for attackers. They may also contain outdated or vulnerable software.

Remediation:

Ensure the demo environment is isolated from the production environment. Regularly update the software used in the demo environment. Implement basic security controls, such as strong passwords and access restrictions. Consider removing the demo environment if it is no longer needed.

16. Missing Security Headers on www.sagarsoft.in

Severity: LOW **Tool:** Subfinder

Description:

The main domain 'www.sagarsoft.in' should be checked for the presence of security headers such as Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), and X-Frame-Options. Missing or misconfigured security headers can make the website vulnerable to various attacks, including cross-site scripting (XSS) and clickjacking.

Remediation:

Implement and properly configure security headers on the main domain. Regularly review and update the security header configuration to address emerging threats.

17. Backend Subdomain Exposure

Severity: LOW **Tool:** Amass Passive

Description:

The presence of 'tsbackend.sagarsoft.in' and 'pmsbackend.sagarsoft.in' subdomains indicates backend systems are potentially exposed. Direct access to backend systems can bypass security controls and lead to severe vulnerabilities.

Remediation:

Restrict access to backend subdomains. Implement strong authentication and authorization. Consider using a reverse proxy to hide the backend infrastructure. Ensure proper input validation and output encoding to prevent injection attacks.

18. Multiple Domain Status Locks

Severity: INFO **Tool:** Whois

Description:

The domain has multiple status locks (clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, clientRenewProhibited). While these are generally good security practices to prevent unauthorized changes, they could also hinder legitimate administrative actions if the owner loses access to their account or needs to make urgent changes.

Remediation:

Document the process for removing these locks in case of emergency. Ensure that the domain owner understands the implications of these locks and has a plan for managing them.

19. 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.

20. Missing Security Headers (Potential)

Severity: INFO **Tool:** Amass Passive

Description:

Without further investigation, it's impossible to confirm, but the lack of information about security headers suggests they might be missing or misconfigured. Missing security headers can make the website vulnerable to various attacks, such as Cross-Site Scripting (XSS) and Clickjacking.

Remediation:

Implement security headers such as Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), X-Frame-Options, and X-XSS-Protection. Regularly review and update security header configurations.

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:
2025-11-26T09:50:17.179Z <<< 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 [INF] Found 7 subdomains for sagarsoft.in
in 11 seconds 824 milliseconds timesheet.sagarsoft.in tsbackend.sagarsoft.in
hrms.sagarsoft.in pms.sagarsoft.in demo.sagarsoft.in pmsbackend.sagarsoft.in
www.sagarsoft.in
```

Tool: Amass Passive

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