Date: 7/31/2024

CYBERQ CONSULTING PVT LTD

Application Security Testing Report

(Final Audit)

Call Center Solution

Web Application Security Test Report of Call Center Solution

Report Release Date	31-07-2024
Type of Audit	Web Application Security
Type of Audit Report	Follow up Audit Report (Final Report)
Period	01-04-2024 to 31-07-2024

Document Control

Document Preparation	
Document Title	Web Application Security Test Report of **Call Center Solution**
Document ID	CQ/A-TS-SANS-24-195/I/03
Document Version	V1.0
Prepared by	Mr. Sushil Tomar
Reviewed by	Mr. Nikhil Rastogi
Approved by	Mr. Hemant Tiwari
Released by	Mr. Sushil Tomar
Release date	31/07/2024

Document Change History

Version	Date	Remarks / Reason of change
V1.0	31/07/2024	Final Audit

Document Distribution List

Name	Organization	Designation	Email Id
Bhupesh Kumar	SAN Softwares Pvt Ltd	Support Engineer	bhupesh.kumar@sansoftwares.com
Deepak Kumar	SAN Softwares Pvt Ltd	-	deepak.kumar@sansoftwares.com
Anil Mehta	SAN Softwares Pvt Ltd	-	anil.mehta@sansoftwares.com
Tarun Verma	SAN Softwares Pvt Ltd	-	tarun.verma@sansoftwares.com
Pramod Kumar Pant	CyberQ Consulting Pvt. Ltd.	Head (Information Security)	pramod.pant@cyberqindia.com
Sujeet Kumar	CyberQ Consulting Pvt. Ltd.	Principal Consultant	sujeet.kumar@cyberqindia.com
Hemant Tiwari	CyberQ Consulting Pvt. Ltd.	Team Lead	hemant.tiwari@cyberqindia.com

Contents

Introduction

Purpose

CyberQ was asked to conduct a Web Application Security Test on the application provided by **SAN Softwares Pvt Ltd.** Details were provided to the extent mentioned in “Scope of Work”. The testing was carried out from **CyberQ Consulting Pvt. Ltd. J-1917, Chittaranjan Park, New Delhi-110019.** The objective of this testing was to ensure the security of the network and web server from external threats through the web application.

Scope

Call Center Solution Web site was hosted on **https://vaptcrm.sansoftwares.com/crm/caller/** was tested. This was a Level-2 testing. Vulnerabilities reported by us throughout the web application have been closed by the client during the Level-1 audit. The Website will be hosted on this URL **https://vaptcrm.sansoftwares.com/crm/caller/.**

Engagement Scope

S. No	Asset Description	Criticality of Asset	Internal IP Address	URL	Public IP Address	Location	Hash Value (in case of applications)	Version (in case of applications)	Other details such as make and model in case of network devices or security devices.
1.	Call Center Solution Web Application	NA	NA	https://vaptcrm.sansoftwares.com/crm/caller/	NA	NA	E0E4E16C1EA3A6B0394D47DC5172CBB7A2322A5DAF3919A9BCB42C125F5C2BE8E21D734E4F9EA5D0798FAFF4CA385446E6780A1FFD9471B0598ADF7E1080545B	-	NA

Date up to which the list has been updated: 28/03/2024

Details of the Auditing team

S. No	Name	Designation	Email Id	Professional Qualifications/ Certifications	Whether the resource has been listed in the Snapshot information published on CERT-In’s website (Yes/No)
1.	Mr. Nikhil Rastogi	Information Security Consultant	nikhil.rastogi@cyberqindia.com	B. Tech, CEH	No
2.	Mr. Sushil Tomar	Information Security Consultant	sushil.tomar@cyberqindia.com	B. Tech, CEH	No

Audit Activities and Timelines

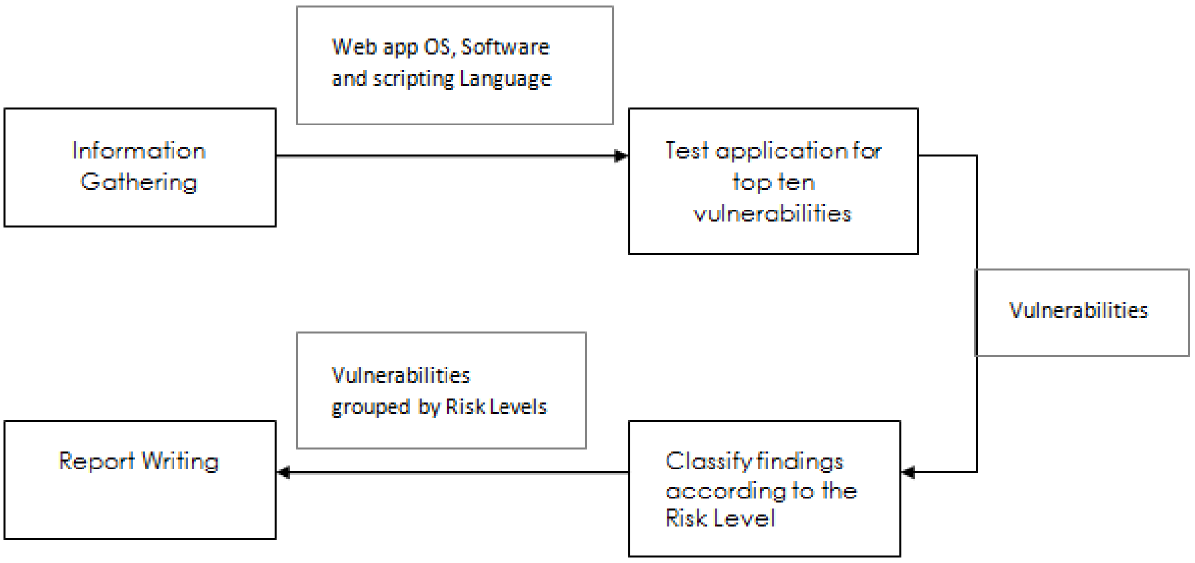
Application Testing Conducted On (Final Audit):

01-04-2024 to 31-07-2024

Audit Methodology and Criteria / Standard referred for audit

Methodology

The methodology applied in Web Application Security Testing is explained in the diagram below:


Web app OS, Software and scripting Language
Information Gathering
Test application for top ten vulnerabilities
Vulnerabilities
Vulnerabilities grouped by Risk Levels
Report Writing
Classify findings according to the Risk Level

Information Gathering: One of the first steps of this test is to identify the Web application environment, including the scripting language and Web server software in use, and the operating system of the target server. However, this step is generally omitted if the testing is limited to just the web application and not the host.

Test Application: While testing the application, we follow but are not limited to the OWASP standards. The OWASP framework vulnerabilities are tested for static and dynamic websites. Our testing is done manually as well as using tools. An indicative list of tools is given in the section below.

After an exhaustive testing, the findings are compiled and classified according to a Risk Level of High, Medium or Low depending on the harm they may cause to the Web Application, server or to the network.

Application Security Observations based on OWASP framework for “Call Center Solution”.

Open Web Applications Security Project (OWASP) has included the different vulnerabilities in its OWASP, list found in web applications worldwide. The table shows how the application stacks up with respect to the OWASP framework.

S. No.	OWASP 2021 Vulnerabilities
1.	Broken Access Control
2.	Cryptographic Failures
3.	Injection
4.	Insecure Design
5.	Security Misconfiguration
6.	Vulnerable and Outdated Components
7.	Identification and Authentication Failures
8.	Software and Data Integrity Failures
9.	Security Logging and Monitoring Failures
10.	Server-Side Request Forgery
OWASP 2013 Vulnerabilities	
11.	Cross-Site Request Forgery (CSRF)
OWASP 2010 Vulnerabilities	
12.	Malicious File Execution
13.	Denial Of Service

Tools/ Software used

S. No	Name of Tool/Software used	Version of the tool /Software used	Open Source/Licensed
1.	Burp Suite	11.1.2	Licensed
2.	SQLmap	3.0.1	Open Source
3.	NMAP	7.90	Open Source

Executive Summary

S. No	Affected Asset i.e. IP/URL/Application etc.	Observation/ Vulnerability title (Detailed observation)	CVE/CWE	Control Objective #	Control Name #	Audit Requirement #	Severity	Recommendation	Reference	New or Repeat observation	Current Status
1.	Call Center Solution Web Application	It is possible to upload malicious files in the application.	CWE-434	NA	NA	NA	**Critical**	Following things should be implemented in file upload module: • Inspect the content of uploaded files, and enforce a white list of accepted, non-executable content types. Additionally, enforce a blacklist of common executable formats, to hinder hybrid file attacks. • Enforce a white list of accepted, non-executable file extensions. • If uploaded files are downloaded by users, supply an accurate non-generic Content-type header, and also a Content-disposition header which specifies that browsers should handle the file as an attachment. • Enforce a size limit on uploaded files (max 8-10 MB); this can be implemented both within application code and in the web server's configuration. • Reject attempts to upload archive formats such as ZIP. • Multiple file extension like test.pdf.txt.php.jif.jpg should not be allowed for upload. • Proper checks to be put on Content type and MIME type as well. Validation at the server end must be	https://cwe.mitre.org/data/definitions/434.html, https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload	-	Closed

								mandatory			
2.	Call Center Solution Web Application	Cross Site scripting attack (XSS) is possible in the application.	CWE-79	NA	NA	NA	**High**	Implement whitelisting and html encoding for every input field present in the application. Also, output encoding should be implemented. The input data should be validated for special characters both in value fields and in URL. Application should not save scripts in the database. Validation at the server end is mandatory. been configured as tight as possible, if the path is set to the root directory "/" then it can be vulnerable to less secure applications on the same server.	https://cwe.mitre.org/data/definitions/79.html, https://www.acunetix.com/websitesecurity/cross-site-scripting/	-	Closed
3.	Call Center Solution Web Application	HTML injection attack is possible in the application.	CWE-80	NA	NA	NA	**High**	Implement whitelisting and html encoding for every input field present in the application. Also, output encoding should be implemented. The input data should be validated for special characters both in value fields and in URL. Application should not save scripts in the database. Validation at the server end is mandatory.	https://cwe.mitre.org/data/definitions/80.html, https://www.invicti.com/learn/html-injection/	-	Closed
4.	Call Center Solution Web Application	I-Frame injection attack is possible in the application.	CWE-1021	NA	NA	NA	**High**	Implement whitelisting and html encoding for every input field present in the application. Also, output encoding should be implemented. The input data should be validated for special characters both in value fields and in URL. Application should not save scripts in the database. Validation at the server end is mandatory.	https://cwe.mitre.org/data/definitions/1021.html, https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/frame-injection/	-	Closed
5.	Call Center Solution Web Application	Pass the hash (Password Replay) attack is possible in the application.	CWE-836	NA	NA	NA	**High**	SHA-256 Salted Hashing technique in “authentication or login module” should be implemented. The pre-requisite to this is that the backend database stores a SHA-256 or	https://cwe.mitre.org/data/definitions/836.html, https://www.bleepingcomput	New	Closed

								hash of the password. (SHA-256 hash is a cryptographic technique in which the actual value can never be recovered). Here is how the salted hash technique works: When a client requests for the login page, the server generates a random number, the salt, and sends it to the client along with the page. A JavaScript code on the client computes the (SHA-256) hash of the password entered by the user. It then concatenates the salt to the hash and re-computes the (SHA-256) hash. This result is then sent to the server. The server picks the hash of the password from its database, concatenates the salt and computes the (SHA-256) hash. If the user entered the correct password these two hashes should match. The server compares the two and if they match, the user is authenticated. Please note that every time a new "salt" value must be generated at the call of login page at the server end. As this "salt" is used it should be expired & deleted at the server end. If it is not used for login for more than a standard time (say 5 minutes), the "salt" value again should be expired & deleted. The SALT value should be properly implemented such that it meets the following conditions: • SALT value should not be visible in the POST request. • SALT value should be alphanumeric and minimum of 16 characters. • SALT value should not be generated on the client side but always on the	er.com/news/security/pass-the-hash-attacks-and-how-to-prevent-them-in-windows-domains/		

								server side.			

6.	Call Center Solution Web Application	Session Hijacking is possible in the application due to the cookie settings being misconfigured in the application.	CAPEC-593, CWE-384	NA	NA	NA	**High**	1. Add a new cookie that randomly changes for each login attempt. Generate different session id before and after authentication. Also, every request after the successful authentication should be associated with an extra auth cookie: It is possible to view the sensitive information by fetching the page from the cache option of the browser. session identifier cookie which also randomly changes and expires when user logs out from the application or closes the browser. For example,
								Cookie: AUTHCookie=69BK7F0D8KL; ASP.NET_SessionId= JNHG7H0LKJ57CF4;
								Cookie: AUTHCookie=5A0KN5F9ER5; ASP.NET_SessionId= JNHG7H0LKJ57CF4;
								Cookie: AUTHCookie=CG4K8L3T5H; ASP.NET_SessionId= JNHG7H0LKJ57CF4;
								Cookie: AUTHCookie=L6D3G0JA3S; ASP.NET_SessionId= JNHG7H0LKJ57CF4.
								2. SSL should be implemented.
									https://capec.mitre.org/data/definitions/593.html,https://owasp.org/www-community/attacks/Session_hijacking_attack,https://www.malcare.com/blog/session-hijacking/	New	Closed

7.	Call Center Solution Web Application	Cross Site Request Forgery (CSRF) attack is po ssible which forces a logged-on victim's browser to send a request to a vulnerable web application, which then performs the chosen action on behalf of the victim.	CWE-352	NA	NA	NA	**High**	Here the problem is - sharing of Cookie values across different instances of the same browser for the same host page. The application should implement the following techniques to prevent the CSRF attack: Insert custom random tokens into every form (page) – • Such that to validate each request a random token is generated for that request on the server side with the server response to the previous request.	https://cwe.mitre.org/data/definitions/352.html, https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html	New	Closed

								• These tokens will not be shared across different instances of the same browser accessing the same host page. Thus, these tokens will not be automatically submitted by the browser. • Validate the submitted token at the server end. • If the request doesn't contain the token or if the submitted token is incorrect then don't address the request. • Token value should change on each and every request. • Token value should be implemented on Page body. • Token value should be alphanumeric and minimum 32 characters. • Token should also be implemented on logout button. For example: It is recommended the token value should change at each page load event and should be validated on the server side before addressing the request. Also, make sure that server does not address the request if the CSRF token contains previously used values.			
8.	Call Center Solution Web Application	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.	CWE-89	NA	NA	NA	**High**	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.	https://cwe.mitre.org/data/definitions/89.html	New	Closed
9.	Call Center Solution Web Application	The passwords are shown in Clear Text to the end user.	CWE-256	NA	NA	NA	**Medium**	It is recommended that passwords should not be displayed in cleartext to end users by default and should be masked when being displayed with an option to temporarily	https://cwe.mitre.org/data/definitions/256.html, https://www.securecodewar	-	Closed

								remove the masking when needed.	rior.com/article/coders-conquer-security-infrastructure-as-codesensitive-data-storage-plaintext-storage-of-passwords		
10.	Call Center Solution Web Application	Sensitive File disclosure is occurring in the application	CWE-200	NA	NA	NA	Medium	Access should be restricted to sensitive files in the application. Only authorized personnel should be able to access sensitive files and proper access control should be maintained/configured to control that.	https://cwe.mitre.org/data/definitions/200.html	New	Closed
11.	Call Center Solution Web Application	One or more configuration files are publicly accessible in this application.	CWE-200	NA	NA	NA	Medium	Remove or restrict access to all configuration files accessible from internet.	https://cwe.mitre.org/data/definitions/200.html	New	Closed
12.	Call Center Solution Web Application	Clickjacking attack is possible in application.	CWE-1021	NA	NA	NA	Medium	The server-side header “X-frame Options” can permit or forbid displaying the page inside a frame. Thus, the application will not be able to open in any third-party application.	https://cwe.mitre.org/data/definitions/1021.html, https://www.pingidentity.com/en/resources/cybersecurity-fundamentals/threats/clickjacking.html	-	Closed
13.	Call Center Solution Web Application	Banner grabbing (application is displaying Server name/version and web technology name/version which may help attacker to learn more about his target) is possible in the application.	CWE-200	NA	NA	NA	Medium	Server and Web technology version should not be displayed to the end user.	https://cwe.mitre.org/data/definitions/200.html, https://support.smarten.com/support/solutions/articles/9000203049-banner-grabbing-vulnerabilities-and-	-	Closed

									solutions		
14.	Call Center Solution Web Application	All HTTP Security Headers are missing at some pages in the application.	CWE-693	NA	NA	NA	Medium	HTTP security headers are a fundamental part of website security. Upon implementation, they protect you against the types of attacks that your site is most likely to come across. These headers protect against XSS, code injection, click jacking, etc. The following headers should be implemented. • Cross Site Scripting Protection (X-XSS) • Content Security Policy (CSP) • HTTP Strict Transport Security (HSTS) • X-Frame-Option • X-Content-Type-Options	https://cwe.mitre.org/data/definitions/693.html, https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html	-	Closed
15.	Call Center Solution Web Application	There is no limit on number of incorrect passwords retries while trying to login. This may lead to Brute force attack.	CWE-307	NA	NA	NA	Medium	Users should be restricted to a defined number of logins attempts per unit of time. After that defined number of login attempt, application should block that user account or CAPTCHA can be implemented at login page. This way automated attempt to login can be checked and brute force attacks can be prevented. CAPTCHA should follow the following condition: a) The combination of alphanumeric value. b) Combination of Upper case and lower-case letters. c) Case-Sensitive d) Its length should be minimum 6 characters. e) Should not be a third-party CAPTCHA: f) Should be Random and not follow a pattern. g) Example: Ab73jy, PT34h8, Hos3t3, nic23n etc.	https://cwe.mitre.org/data/definitions/757.html, https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks	-	Closed
16.	Call Center Solution Web Application	HTTP Methods are enabled in the application.	CWE-650	NA	NA	NA	Medium	HTTP methods should be disabled in the application which may prevent the application from security breach. Only GET and POST	https://cwe.mitre.org/data/definitions/650.html, https://do	-	Closed

								method should be enabled in the application.	cs.fluidattacks.com/criteria/vulnerabilities/044/		
17.	Call Center Solution Web Application	Old and Vulnerable version of libraries and environment are being used in the application.	CWE-1104	NA	NA	NA	**Medium**	It is recommended to use latest and stable version for more secured application.	https://cwe.mitre.org/data/definitions/1104.html	-	Closed
18.	Call Center Solution Web Application	Client-side desync (CSD) vulnerabilities occur when a web server fails to correctly process the Content-Length of POST requests. By exploiting this behavior, an attacker can force a victim's browser to desynchronize its connection with the website, typically leading to XSS.	CWE-444	NA	NA	NA	**Low**	This vulnerability can be resolved by patching the server so that it either processes POST requests correctly or closes the connection after handling them. You could also disable connection reuse entirely, but this may reduce performance. You can also resolve this issue by enabling HTTP/2	https://cwe.mitre.org/data/definitions/444.html	New	Closed
19.	Call Center Solution Web Application	Password History is not maintained in the application.	CWE-262	NA	NA	NA	**Low**	Users should be prevented from reusing their current or previous 3 passwords. Password history should ideally be 3.	https://cwe.mitre.org/data/definitions/262.html	-	Closed
20.	Call Center Solution Web Application	Password Complexity is not implemented properly in the application	CWE-521	NA	NA	NA	**Low**	Password should be complex	https://cwe.mitre.org/data/definitions/521.html	-	Closed
21.	Call Center Solution Web Application	Multiple Ports are open in the application.	CWE-1125	NA	NA	NA	**Low**	Only port 443 must be open in the application, all other remaining ports must be closed.	https://cwe.mitre.org/data/definitions/1125.html, https://blog.netwrix.com/2022/08/16/open-network-ports/	-	Closed
22.	Call Center Solution Web Application	Input validations not implemented properly in the application.	CWE-20	NA	NA	NA	**Low**	Input validations should be properly implemented in the application.	https://cwe.mitre.org/data/definitions/20.html	-	Closed
23.	Call Center Solution Web	Path is set to default root i.e. '/'.	CWE-41	NA	NA	NA	**Low**	Verify that the path attribute, just as the Domain attribute, has not been set too	https://cwe.mitre.org/data/definitions/4	-	Closed

	Application							loosely. Even if the Domain attribute has been configured as tight as possible, if the path is set to the root directory "/" then it can be vulnerable to less secure applications on the same server.	1.html		
24.	Call Center Solution Web Application	Cookie is displaying without SECURE flag.	CWE-614	NA	NA	NA	Low	Secure flag should be "True" in website's configuration file.	https://cwe.mitre.org/data/definitions/614.html	-	Closed
25.	Call Center Solution Web Application	HTTPonly flag is not set properly in the application.	CWE-1004	NA	NA	NA	Low	HTTPonly flag should be set to "True" in website's configuration file.	https://cwe.mitre.org/data/definitions/1004.html	-	Closed
26.	Call Center Solution Web Application	Same Site attribute set to none.	CWE-1275	NA	NA	NA	Low	Same Site attribute should be set to "LAX or STRICT".	https://cwe.mitre.org/data/definitions/1275.html, https://probely.com/vulnerabilities/cookie-with-samesite-attribute-set-to-none	-	Closed
27.	Call Center Solution Web Application	There is no forgot password option available for the user.	CWE-620	NA	NA	NA	Low	Users may be required to retrieve their password. Users should be provided with a "forgot password" option through which user will retrieve their password whenever required. Forgot password should be enabled with the users email address. There are following conditions that should be met in the forget password function: 1. A reset link should be sent to the user registered email address instead of password directly. 2. Reset Password link should expire in 24 hours. 3. Reset Password link should not be reused again once the link is used for resetting password. 4. In the Reset	https://cwe.mitre.org/data/definitions/620.html	-	Closed

								Password page, Mandatory fields i.e. new password, Confirm Password and CAPTCHA field must present and should be validated at the client end. Server end validations are also mandatory. However, if the password retrieval is internal in the application, then it is recommended to implement a hyperlink on login page resulting to a static page containing a message. “Please contact your site administrator at mail_id[at]domain[dot] com”. Please note that the email address in the message should not be a hyperlink			
28.	Call Center Solution Web Application	Session termination due to user inactivity is not properly configured in the application.	CWE-613	NA	NA	NA	Low	In case of session termination by the application due to inactivity of the user within his session for more than 15 minutes, application must terminate session completely and login page must be loaded in the main window instead of in a child frame of the window.	https://cwe.mitre.org/data/definitions/613.html	New	Closed
29.	Call Center Solution Web Application	Email spamming is possible in the application.	CWE-799	NA	NA	NA	Low	The application should properly customize the email addresses while posting on the website as: 1. Email addresses should be posted as an image not as a hyperlink. Alternatively, instead of @symbol, [at] should be used. Similarly, the dot character (.) should be replaced by [dot]. So abc@nic.in should be written as abc[at]nic[dot]in. 2. High privilege email addresses should not be posted on the website.	https://cwe.mitre.org/data/definitions/799.html	New	Closed
30.	Call Center Solution Web	Autofill is enabled in forms	CWE-200	NA	NA	NA	Low	Application should not have the option to remember information entered by the user as	https://portswigger.net/kb/issues/0050	-	Closed

	Application	.						this may cause unavailability of services to valid users. AutoComplete option should be turned off by the application so as to override any settings by the user from the browser.	0800_password-field-with-autocomplete-enabled https://cwe.mitre.org/data/definitions/200.html		
31.	Call Center Solution Web Application	Old TLS versions are still being used in the application.	CWE-757	NA	NA	NA	Low	TLS v1.2 or higher should be used. All other TLS versions should be removed.	https://cwe.mitre.org/data/definitions/757.html	-	Closed
32.	Call Center Solution Web Application	The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.open**.	CWE-757	NA	NA	NA	Low	The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.	https://cwe.mitre.org/data/definitions/757.html	New	Closed
33.	Call Center Solution Web Application	OTP masking is not implemented in the application.	CWE-549	NA	NA	NA	Low	OTP should be masked and should not be viewable in clear text to end user or an option should be provided to unmask, if needed.	https://cwe.mitre.org/data/definitions/549.html	New	Closed
34.	Call Center Solution Web Application	Cleartext submission of password	CWE-549	NA	NA	NA	Low	OTP should be masked and should not be viewable in clear text to end user or an option should be provided to unmask, if needed.	https://cwe.mitre.org/data/definitions/549.html	New	Closed
35.	Call Center Solution	The application does not maintain audit	CWE-778	NA	NA	NA	Observation	An Audit trail should be incorporated in the application admin	https://cwe.mitre.org/data/de	-	Closed

	Web Application	trail properly where all user activities must be logged. In case a malicious user tries to attack the application; the application will not be able to trace the attacker.						module, where all user activities must be logged.	finitions/778.html		

# Applicable in case of compliance Audits such as ISO/IEC 27001 Audit, PCI DSS audit, audit as per regulatory requirements / directions or any other such audit which checks compliance against standards/guidelines/directions mandated/recommended by a regulator or government agency.

Detailed Observations

Finding No. 1

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Unrestricted Upload of File with Dangerous Type.

iii) Detailed observation / Vulnerable point: It is possible to upload malicious files in the application.

iv) CVE/CWE: CWE-434

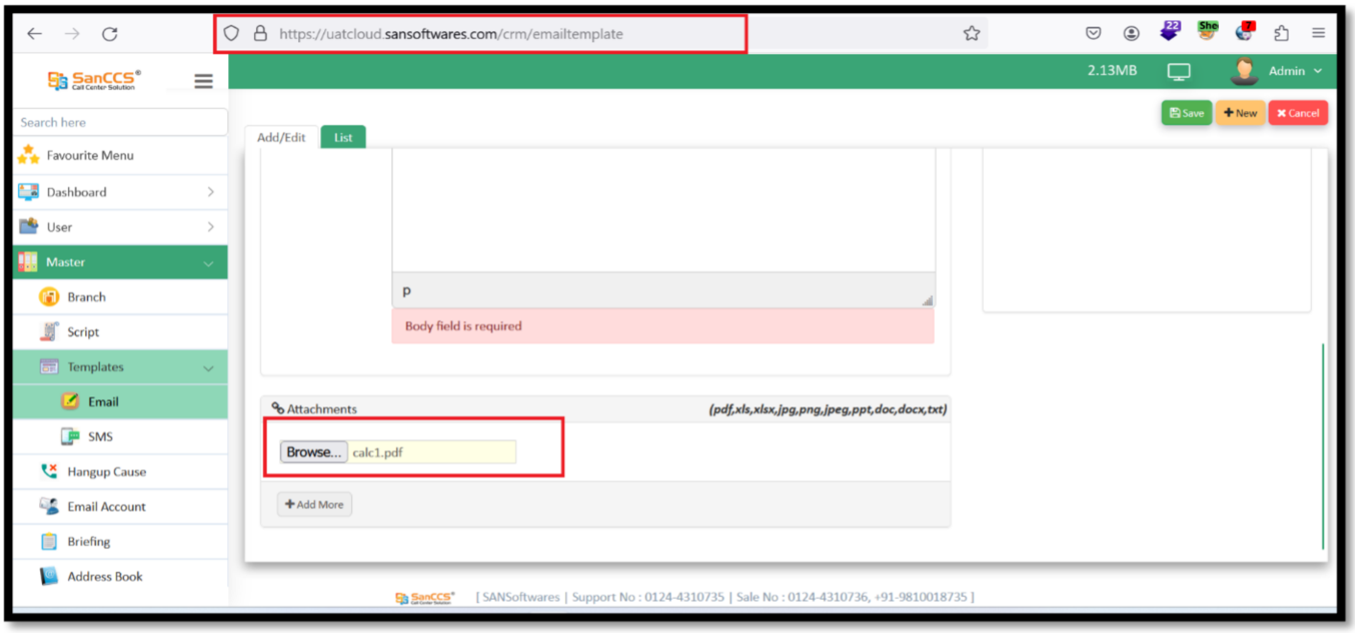
v) Severity: Critical

vi) Recommendation: Following things should be implemented in file upload module:
- Inspect the content of uploaded files, and enforce a white list of accepted, non-executable content types. Additionally, enforce a blacklist of common executable formats, to hinder hybrid file attacks.
- Enforce a white list of accepted, non-executable file extensions.
- If uploaded files are downloaded by users, supply an accurate non-generic Content-type header, and also a Content-disposition header which specifies that browsers should handle the file as an attachment.
- Enforce a size limit on uploaded files (max 8-10 MB); this can be implemented both within application code and in the web server's configuration.
- Reject attempts to upload archive formats such as ZIP.
- Multiple file extension like test.pdf.txt.php.jif.jpg should not be allowed for upload.
- Proper checks to be put on Content type and MIME type as well. Validation at the server end must be mandatory.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/434.html,
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

ix) References to evidences / Proof of Concept:
Step#1: After login an application and upload a calc1.pdf (malicious file) in application.



https://uatcloud.sansoftwares.com/crm/emailtemplate

p

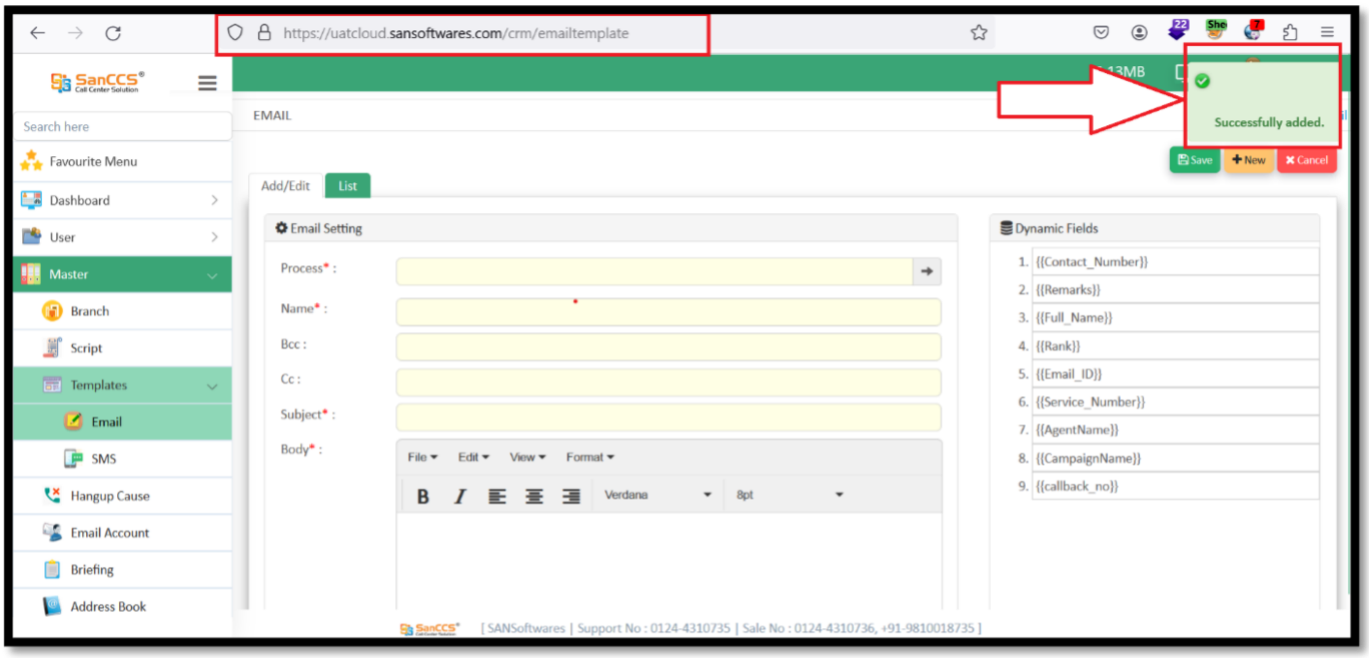
Body field is required

Attachments (pdf,xls,xlsx,jpg,png,jpeg,ppt,doc,docx,txt)

Browse... calc1.pdf

[SANSoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

Step#2: We can see it is uploaded successfully.



Successfully added.

EMAIL

Email Setting

Process* :

Name* :

Bcc :

Cc :

Subject* :

Body* :

Dynamic Fields

1. {{Contact_Number}}
2. {{Remarks}}
3. {{Full_Name}}
4. {{Rank}}
5. {{Email_ID}}
6. {{Service_Number}}
7. {{AgentName}}
8. {{CampaignName}}
9. {{callback_no}}

Finding No. 2

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Improper Neutralization of Input During Web Page Generation.

iii) **Detailed observation / Vulnerable point**: Cross Site scripting attack (XSS) is possible in the application.

iv) **CVE/CWE:** CWE-79

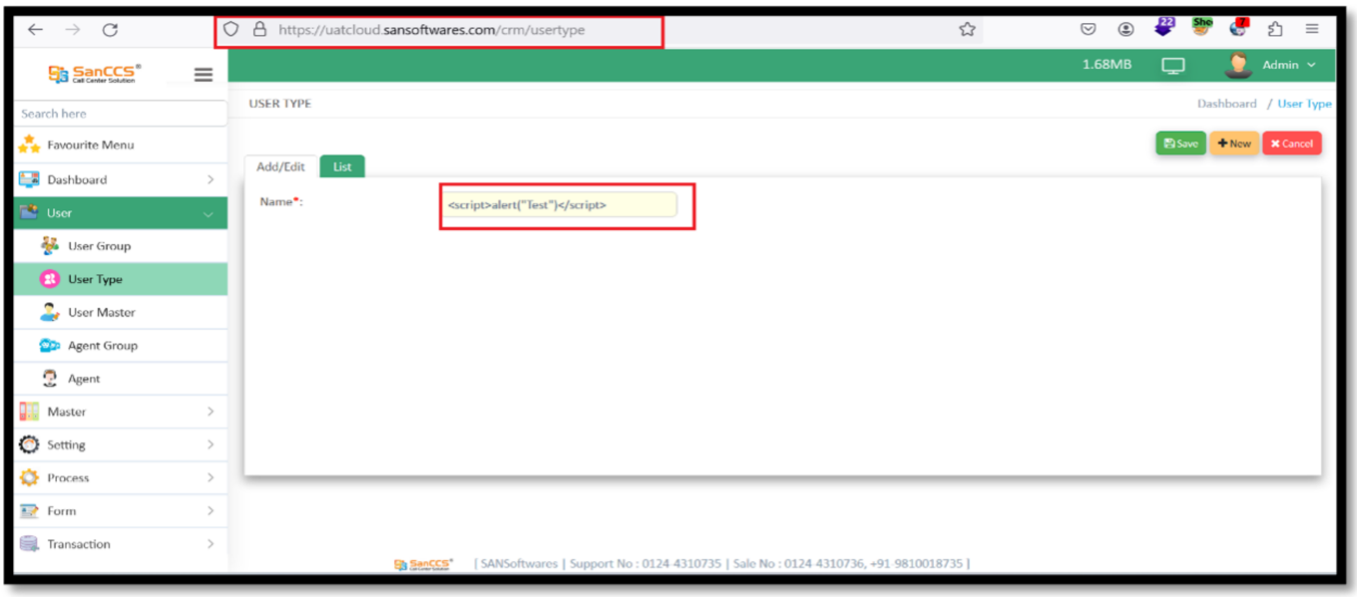
v) **Severity:** High

vi) **Recommendation:** Implement whitelisting and html encoding for every input field present in the application. Also, output encoding should be implemented. The input data should be validated for special characters both in value fields and in URL. Application should not save scripts in the database. Validation at the server end is mandatory.

vii) **Current Status:** Closed

viii) **Reference:**
https://cwe.mitre.org/data/definitions/79.html,https://www.acunetix.com/websitesecurity/cross-site-scripting/

ix) **References to evidences / Proof of Concept:**
Step#1: Go to an application and enter data in input field.



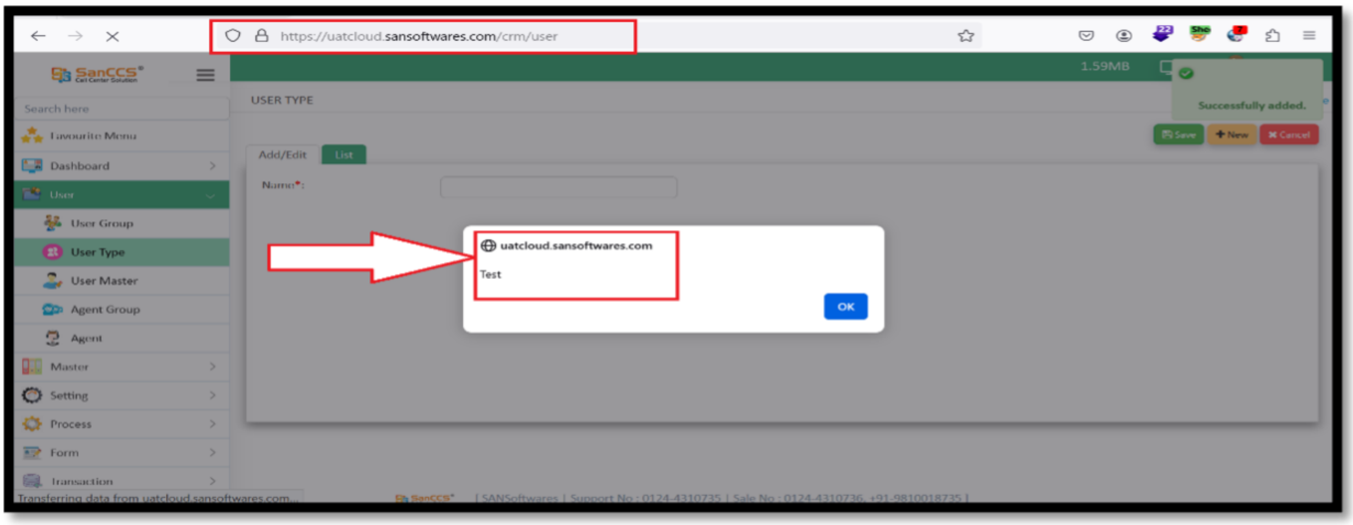
https://uatcloud.sansoftwares.com/crm/usertype

USER TYPE

Name*: <script>alert("Test")</script>

[SANSoftwares | Support No : 0124 4310735 | Sale No : 0124 4310736, +91 9810018735]

Step#2: And we can see the XSS is possible in this application**.**



https://uatcloud.sansoftwares.com/crm/user

uatcloud.sansoftwares.com

Test

Successfully added.

Transferring data from uatcloud.sansoftwares.com...

[SANSoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

Finding No. 3

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Improper Neutralization of Script-Related HTML Tags in a Web Page.

iii) Detailed observation /vulnerable point: HTML injection attack is possible in the application.

iv) CVE/CWE: CWE-80

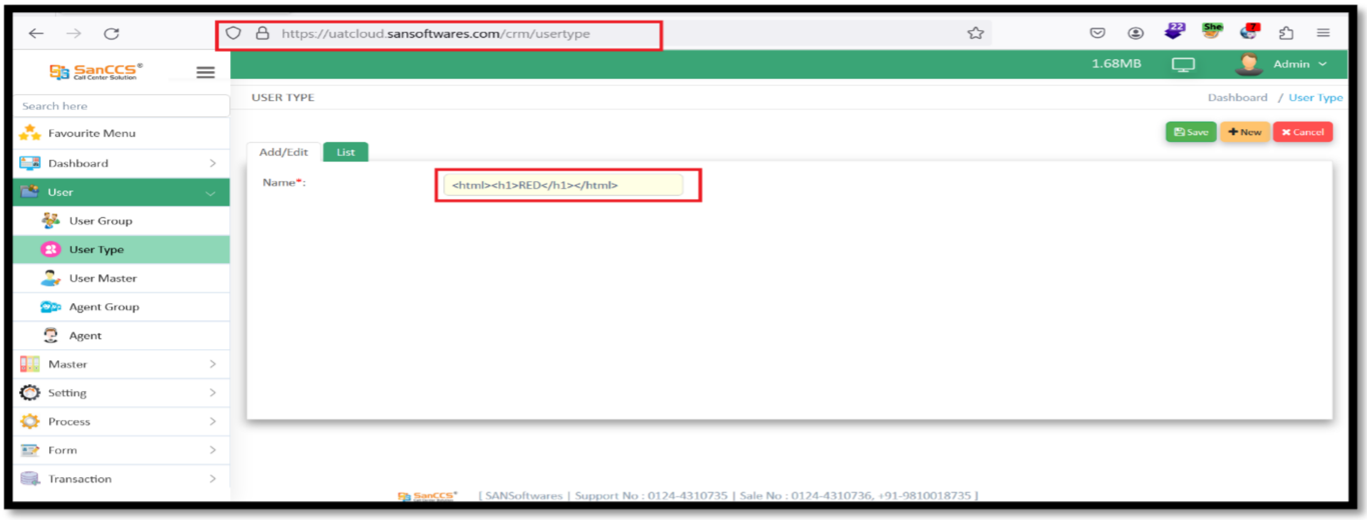
v) Severity: High

vi) Recommendation: Implement whitelisting and html encoding for every input field present in the application. Also, output encoding should be implemented. The input data should be validated for special characters both in value fields and in URL. Application should not save scripts in the database. Validation at the server end is mandatory.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/80.html, https://www.invicti.com/learn/html-injection/

ix) References to evidences / Proof of Concept:
Step#1: Go to an application and enter data in document input field.

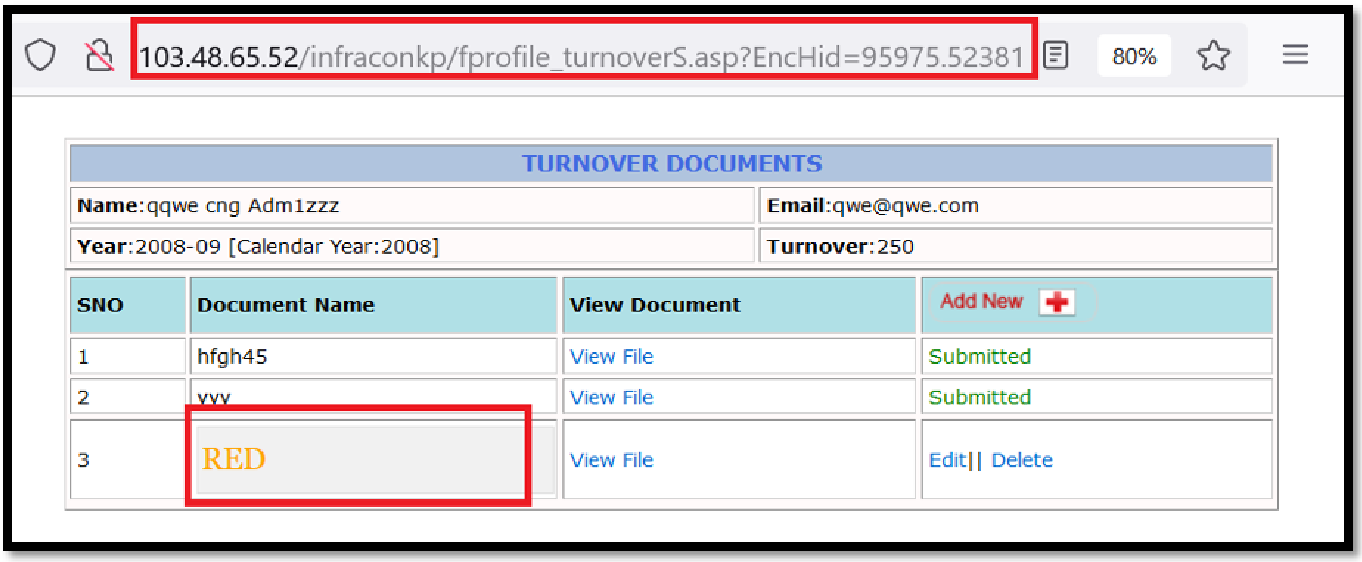


https://uatcloud.sansoftwares.com/crm/usertype

USER TYPE

Name*: <html><h1>RED</h1></html>

Step#2: And we can see that HTML injection is possible in this application.



103.48.65.52/infraconkp/fprofile_turnoverS.asp?EncHid=95975.52381

TURNOVER DOCUMENTS

Name:qqwe cng Adm1zzz	**Email**:qwe@qwe.com
Year:2008-09 [Calendar Year:2008]	**Turnover**:250

SNO	Document Name	View Document	Add New ✚
1	hfgh45	View File	Submitted
2	yyy	View File	Submitted
3	RED	View File	Edit|| Delete

Finding No. 4

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Improper Restriction of Rendered UI Layers or Frames

iii) Detailed observation /vulnerable point: I-Frame injection attack is possible in the application.

iv) CVE/CWE: CWE-1021

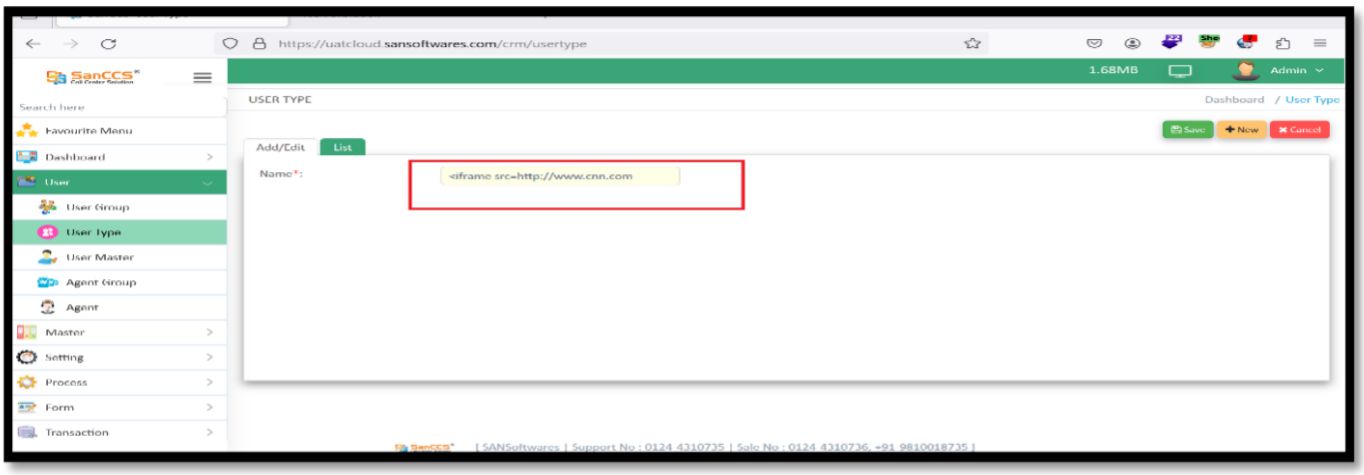
v) Severity: High

vi) Recommendation: Implement whitelisting and html encoding for every input field present in the application. Also, output encoding should be implemented. The input data should be validated for special characters both in value fields and in URL. Application should not save scripts in the database. Validation at the server end is mandatory.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/1021.html, https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/frame-injection/

ix) References to evidences / Proof of Concept:
Step#1: Go to an application and enter data in document input field and capture the request.

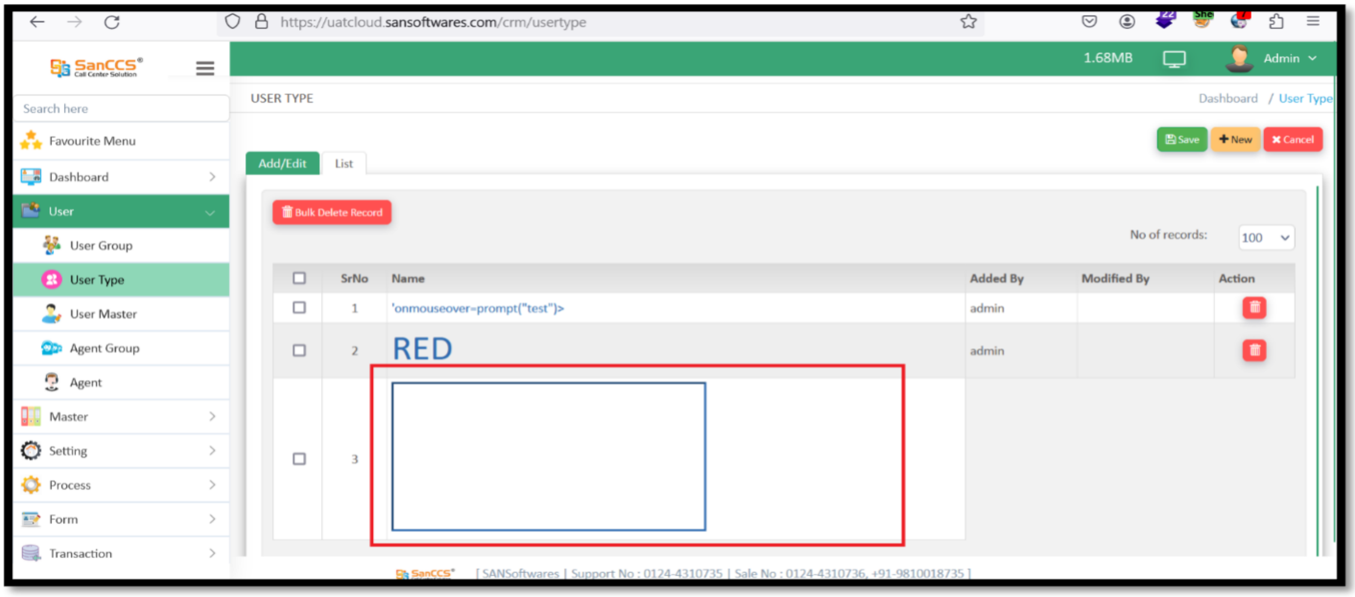


https://uatcloud.sansoftwares.com/crm/usertype

USER TYPE

Name*: <iframe src=http://www.cnn.com

Step#2: As we can see the result in given, I Frame Injection is possible in this application.



https://uatcloud.sansoftwares.com/crm/usertype

USER TYPE

No of records: 100

☐	SrNo	Name	Added By	Modified By	Action
☐	1	'onmouseover=prompt("test")>	admin		🗑
☐	2	RED	admin		🗑
☐	3				

Finding No. 5

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Use of Password Hash Instead of Password for Authentication.

iii) Detailed observation / Vulnerable point: Pass the hash (Password Replay) attack is possible in the application.

iv) CVE/CWE: CWE-836

v) Severity: High

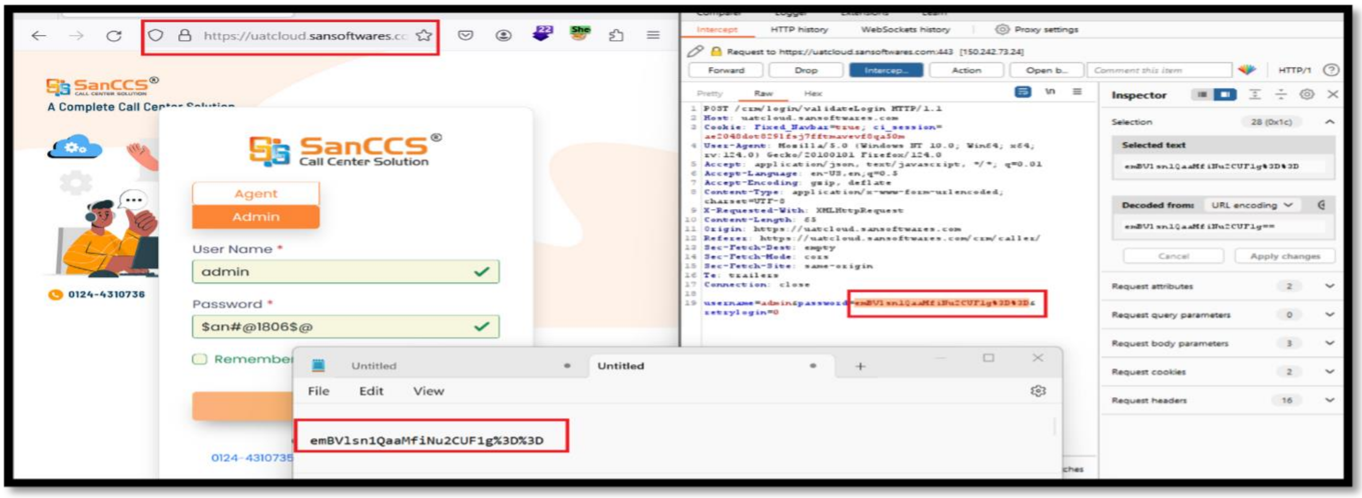
vi) Recommendation: SHA-256 Salted Hashing technique in "authentication or login module" should be implemented. The pre-requisite to this is that the backend database stores a SHA-256 or hash of the password. (SHA-256 hash is a cryptographic technique in which the actual value can never be recovered). Here is how the salted hash technique works: When a client requests for the login page, the server generates a random number, the salt, and sends it to the client along with the page. A JavaScript code on the client computes the (SHA-256) hash of the password entered by the user. It then concatenates the salt to the hash and re-computes the (SHA-256) hash. This result is then sent to the server. The server picks the hash of the password from its database, concatenates the salt and computes the (SHA-256) hash. If the user entered the correct password these two hashes should match. The server compares the two and if they match, the user is authenticated. Please note that every time a new "salt" value must be generated at the call of login page at the server end. As this "salt" is used it should be expired & deleted at the server end. If it is not used for login for more than a standard time (say 5 minutes), the "salt" value again should be expired & deleted. The SALT value should be properly implemented such that it meets the following conditions: • SALT value should not be visible in the POST request. • SALT value should be alphanumeric and minimum of 16 characters. • SALT value should not be generated on the client side but always on the server side.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/836.html, https://www.bleepingcomputer.com/news/security/pass-the-hash-attacks-and-how-to-prevent-them-in-windows-domains/

ix) References to evidences / Proof of Concept:

Step#1: Login in Web Application with correct User ID and Password and Capture the login request in Burp Suite, copy the password hash, and paste it into a notepad. Afterwards, disable the proxy and logout an application.



Request to https://uatcloud.sansoftwares.com:443 [150.242.73.24]

User Name * admin

Password * $an#@1806$@

```
POST /crm/login/validateLogin HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=
ae2040dot0291fsj7fftmavevf0qa50m
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:124.0) Gecko/20100101 Firefox/124.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 65
Origin: https://uatcloud.sansoftwares.com
Referer: https://uatcloud.sansoftwares.com/crm/caller/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

username=admin&password=emBVlsn1QaaMfiNu2CUF1g%3D%3D&
retrylogin=0
```

Selection 28 (0x1c)

Selected text: emBVlsn1QaaMfiNu2CUF1g%3D%3D

Decoded from: URL encoding

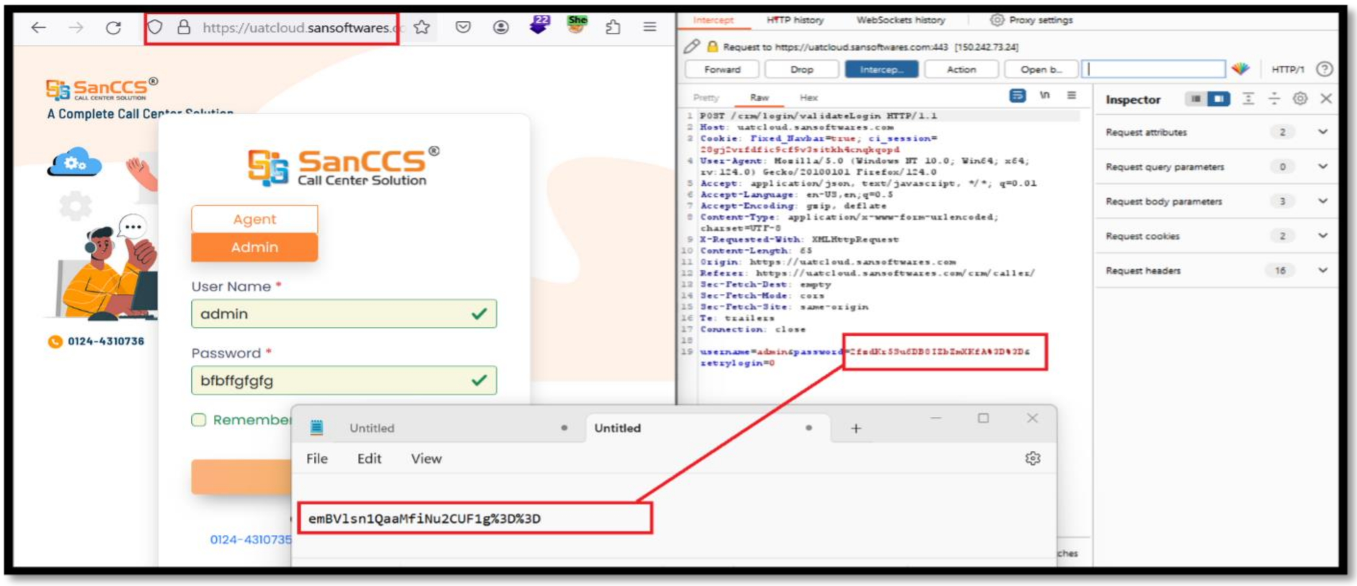
emBVlsn1QaaMfiNu2CUF1g==

Cancel | Apply changes

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	2
Request headers	16

```
emBVlsn1QaaMfiNu2CUF1g%3D%3D
```

Step#2: Attempt to log in with an incorrect password and capture the corresponding request using a proxy and, In the request, paste the previously copied request from Notepad into the password hash field, and forward the request.



Request to https://uatcloud.sansoftwares.com:443 [150.242.73.24]

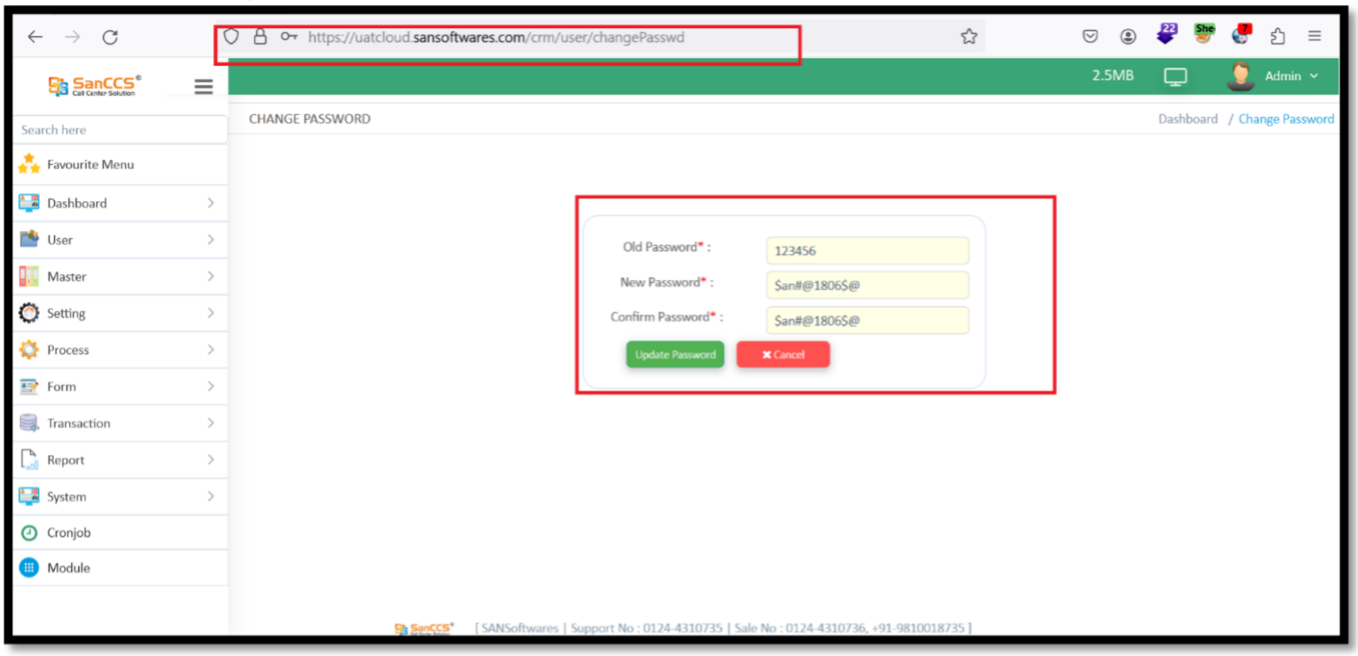
```
POST /crm/login/validateLogin HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=
28gj2vrfdfic9cf9v3sitkh4cnqkqopd
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:124.0) Gecko/20100101 Firefox/124.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 65
Origin: https://uatcloud.sansoftwares.com
Referer: https://uatcloud.sansoftwares.com/crm/caller/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

username=admin&password=ZfadKr5SuADB0IZbZmXKfA%3D%3D&
retrylogin=0
```

User Name *: admin

Password *: bfbffgfgfg

```
emBVlsn1QaaMfiNu2CUF1g%3D%3D
```

Step#3: In the request, paste the previously copied request from Notepad into the password hash field, and forward the request.



https://uatcloud.sansoftwares.com/crm/user/changePasswd

CHANGE PASSWORD

Old Password* : 123456

New Password* : San#@1806$@

Confirm Password* : San#@1806$@

SanCCS Call Center Solution
2.5MB
Admin
Dashboard / Change Password
Search here
Favourite Menu
Dashboard
User
Master
Setting
Process
Form
Transaction
Report
System
Cronjob
Module
Update Password
Cancel
SanCCS [SANSoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

Finding No. 6

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application

ii) **Observation/ Vulnerability title:** Exposure of Sensitive Information to an Unauthorized Actor.

iii) **Detailed observation /vulnerable point:** Session Hijacking is possible in the application due to the cookie settings being misconfigured in the application

iv) **CVE/CWE:** CAPEC-593, CWE-384

v) **Severity:** High

vi) **Recommendation:** 1. Add a new cookie that randomly changes for each login attempt. Generate different session id before and after authentication. Also, every request after the successful authentication should be associated with an extra auth cookie: It is possible to view the sensitive information by fetching the page from the cache option of the browser. session identifier cookie which also randomly changes and expires when user logs out from the application or closes the browser. For example,
Cookie: AUTHCookie=69BK7F0D8KL; ASP.NET_SessionId= JNHG7H0LKJ57CF4;
Cookie: AUTHCookie=5A0KN5F9ER5; ASP.NET_SessionId= JNHG7H0LKJ57CF4;
Cookie: AUTHCookie=CG4K8L3T5H; ASP.NET_SessionId= JNHG7H0LKJ57CF4;
Cookie: AUTHCookie=L6D3G0JA3S; ASP.NET_SessionId= JNHG7H0LKJ57CF4.
2. SSL should be implemented.

vii) **Current Status:** Closed

viii) **Reference:** https://capec.mitre.org/data/definitions/593.html,
https://owasp.org/www-community/attacks/Session_hijacking_attack,
https://www.malcare.com/blog/session-hijacking/

ix) **References to evidences / Proof of Concept: N/A**

Finding No. 7

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Exposure of Sensitive Information to an Unauthorized Actor.

iii) Detailed observation /vulnerable point: Cross Site Request Forgery (CSRF) attack is possible which forces a logged-on victim's browser to send a request to a vulnerable web application, which then performs the chosen action on behalf of the victim.

iv) CVE/CWE: CWE-352

v) Severity: High

vi) Recommendation: Here the problem is - sharing of Cookie values across different instances of the same browser for the same host page. The application should implement the following techniques to prevent the CSRF attack: Insert custom random tokens into every form (page)

- Such that to validate each request a random token is generated for that request on the server side with the server response to the previous request.
- These tokens will not be shared across different instances of the same browser accessing the same host page. Thus, these tokens will not be automatically submitted by the browser.
- Validate the submitted token at the server end.
- If the request doesn't contain the token or if the submitted token is incorrect then don't address the request.
- Token value should change on each and every request.
- Token value should be implemented on Page body.
- Token value should be alphanumeric and minimum 32 characters.
- Token should also be implemented on logout button.

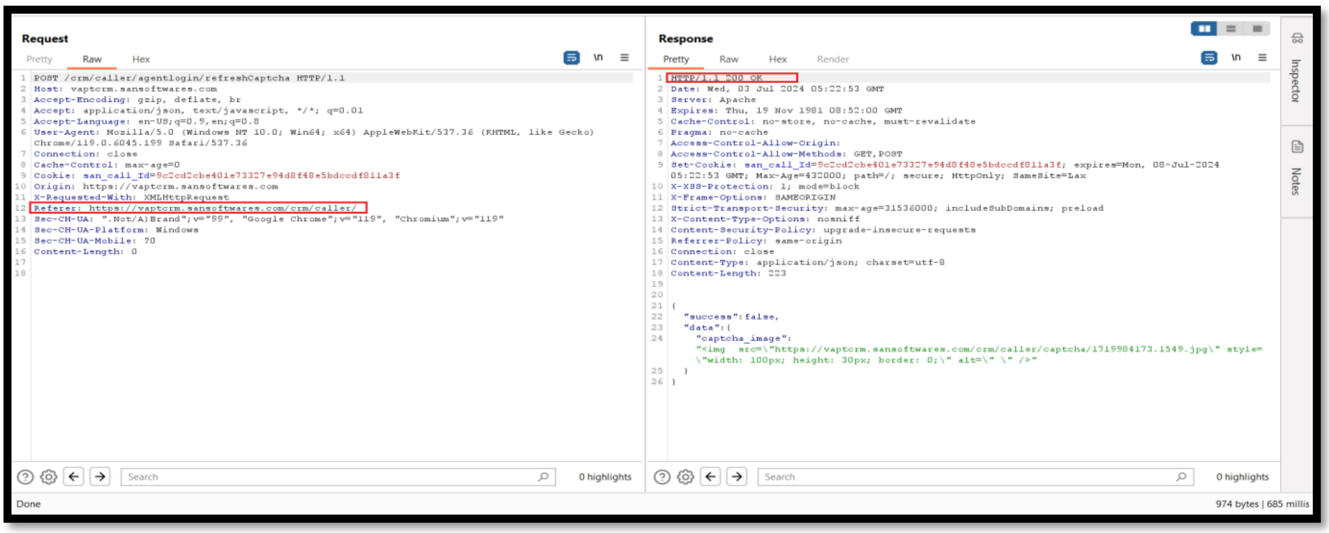
For example: It is recommended the token value should change at each page load event and should be validated on the server side before addressing the request. Also, make sure that server does not address the request if the CSRF token contains previously used values.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/352.html,
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

ix) References to evidences / Proof of Concept:

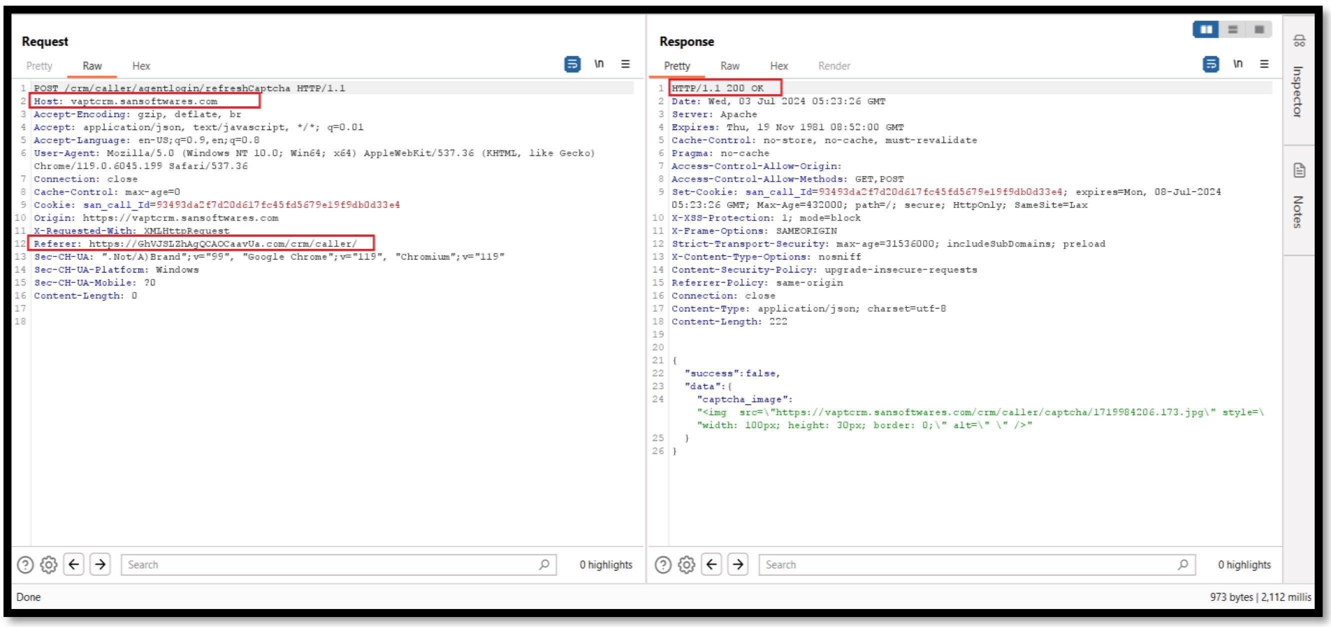
Step#1: Open the URL, login with valid credentials of user, and capture the request on Burp Suite.
Step#2: Change the Referrer



```
POST /crm/caller/agentlogin/refreshCaptcha HTTP/1.1
Host: vaptcrm.sansoftwares.com
Accept-Encoding: gzip, deflate, br
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.199 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: san_call_Id=9c2cd2cbe401e73327e94d8f48e5bdccdf811a3f
Origin: https://vaptcrm.sansoftwares.com
X-Requested-With: XMLHttpRequest
Referer: https://vaptcrm.sansoftwares.com/crm/caller/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="119", "Chromium";v="119"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Wed, 03 Jul 2024 05:22:53 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: GET,POST
Set-Cookie: san_call_Id=9c2cd2cbe401e73327e94d8f48e5bdccdf811a3f; expires=Mon, 08-Jul-2024
05:22:53 GMT; Max-Age=432000; path=/; secure; HttpOnly; SameSite=Lax
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Content-Security-Policy: upgrade-insecure-requests
Referrer-Policy: same-origin
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 223


{
  "success":false,
  "data":{
    "captcha_image":
    "<img  src=\"https://vaptcrm.sansoftwares.com/crm/caller/captcha/1719984173.1549.jpg\" style=
    \"width: 100px; height: 30px; border: 0;\" alt=\" \" />"
  }
}
```

Step#3: observe from the screenshot below, request is 200 OK, CSRF is possible.



```
POST /crm/caller/agentlogin/refreshCaptcha HTTP/1.1
Host: vaptcrm.sansoftwares.com
Accept-Encoding: gzip, deflate, br
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.199 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: san_call_Id=93493da2f7d20d617fc45fd5679e19f9db0d33e4
Origin: https://vaptcrm.sansoftwares.com
X-Requested-With: XMLHttpRequest
Referer: https://GhVJSLZhAgQCAOCaavUa.com/crm/caller/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="119", "Chromium";v="119"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Wed, 03 Jul 2024 05:23:26 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: GET,POST
Set-Cookie: san_call_Id=93493da2f7d20d617fc45fd5679e19f9db0d33e4; expires=Mon, 08-Jul-2024
05:23:26 GMT; Max-Age=432000; path=/; secure; HttpOnly; SameSite=Lax
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Content-Security-Policy: upgrade-insecure-requests
Referrer-Policy: same-origin
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 222


{
  "success":false,
  "data":{
    "captcha_image":
    "<img  src=\"https://vaptcrm.sansoftwares.com/crm/caller/captcha/1719984206.173.jpg\" style=\
    "width: 100px; height: 30px; border: 0;\" alt=\" \" />"
  }
}
```

Finding No. 8

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Improper Neutralization of Special Elements.

iii) Detailed observation /vulnerable point: SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

iv) CVE/CWE: CWE-89

v) Severity: Medium

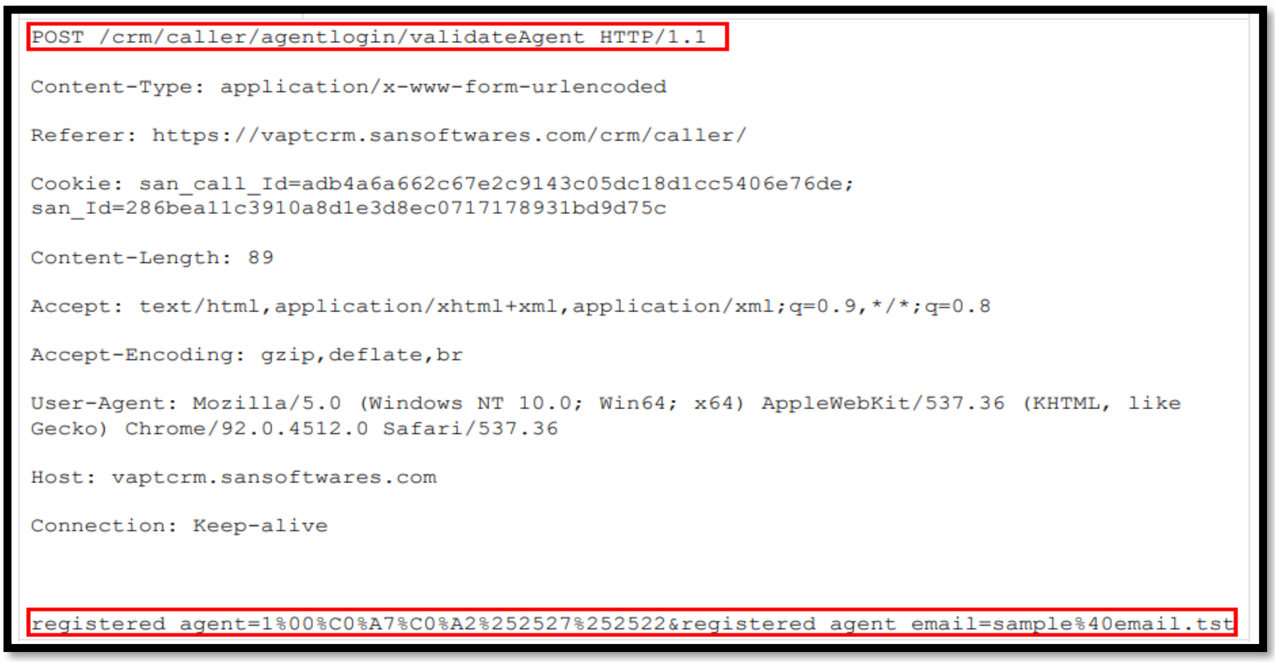
vi) Recommendation: Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/256.html,
https://www.securecodewarrior.com/article/coders-conquer-security-infrastructure-as-codesensitive-data-storage-plaintext-storage-of-passwords

ix) References to evidences / Proof of Concept:

Step#1: Observed from the screenshot below, URL encoded POST input registered_agent was set to 1À§À¢%2527%2522.



```
POST /crm/caller/agentlogin/validateAgent HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: https://vaptcrm.sansoftwares.com/crm/caller/

Cookie: san_call_Id=adb4a6a662c67e2c9143c05dc18d1cc5406e76de;
san_Id=286bea11c3910a8d1e3d8ec0717178931bd9d75c

Content-Length: 89

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: vaptcrm.sansoftwares.com

Connection: Keep-alive


registered_agent=1%00%C0%A7%C0%A2%252527%252522&registered_agent_email=sample%40email.tst
```

Finding No. 9

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Exposure of Sensitive Information to an Unauthorized Actor.

iii) Detailed observation /vulnerable point: The sensitive information is shown in Clear Text to the end user.

iv) CVE/CWE: CWE-256

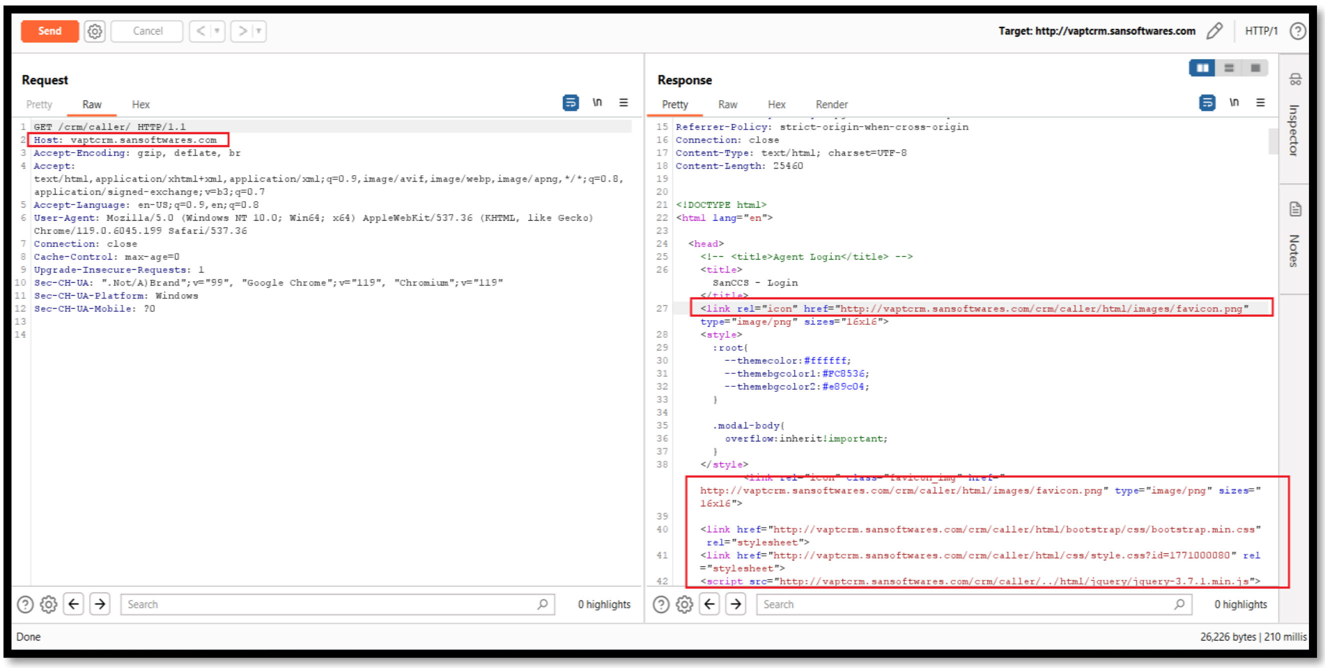
v) Severity: Medium

vi) Recommendation: It is recommended that data should not be displayed in cleartext to end users by default and should be masked when being displayed with an option to temporarily remove the masking when needed.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/256.html, https://www.securecodewarrior.com/article/coders-conquer-security-infrastructure-as-codesensitive-data-storage-plaintext-storage-of-passwords

ix) References to evidences / Proof of Concept:
Step#1: Observed from the screenshot below, Sensitive information displayed in the application in the clear text.



```
GET /crm/caller/ HTTP/1.1
Host: vaptcrm.sansoftwares.com
Accept-Encoding: gzip, deflate, br
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.199 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="119", "Chromium";v="119"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

```
Referrer-Policy: strict-origin-when-cross-origin
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 25460


<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="http://vaptcrm.sansoftwares.com/crm/caller/html/images/favicon.png"
    type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
            <link rel="icon" class="favicon_img" href="
    http://vaptcrm.sansoftwares.com/crm/caller/html/images/favicon.png" type="image/png" sizes="
    16x16">

    <link href="http://vaptcrm.sansoftwares.com/crm/caller/html/bootstrap/css/bootstrap.min.css"
     rel="stylesheet">
    <link href="http://vaptcrm.sansoftwares.com/crm/caller/html/css/style.css?id=1771000080" rel
    ="stylesheet">
    <script src="http://vaptcrm.sansoftwares.com/crm/caller/../html/jquery/jquery-3.7.1.min.js">
```

Finding No. 10

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application

ii) **Observation/ Vulnerability title:** Exposure of Sensitive Information to an Unauthorized Actor.

iii) **Detailed observation /vulnerable point:** Sensitive File disclosure is occurring in the application.

iv) **CVE/CWE:** CWE-200

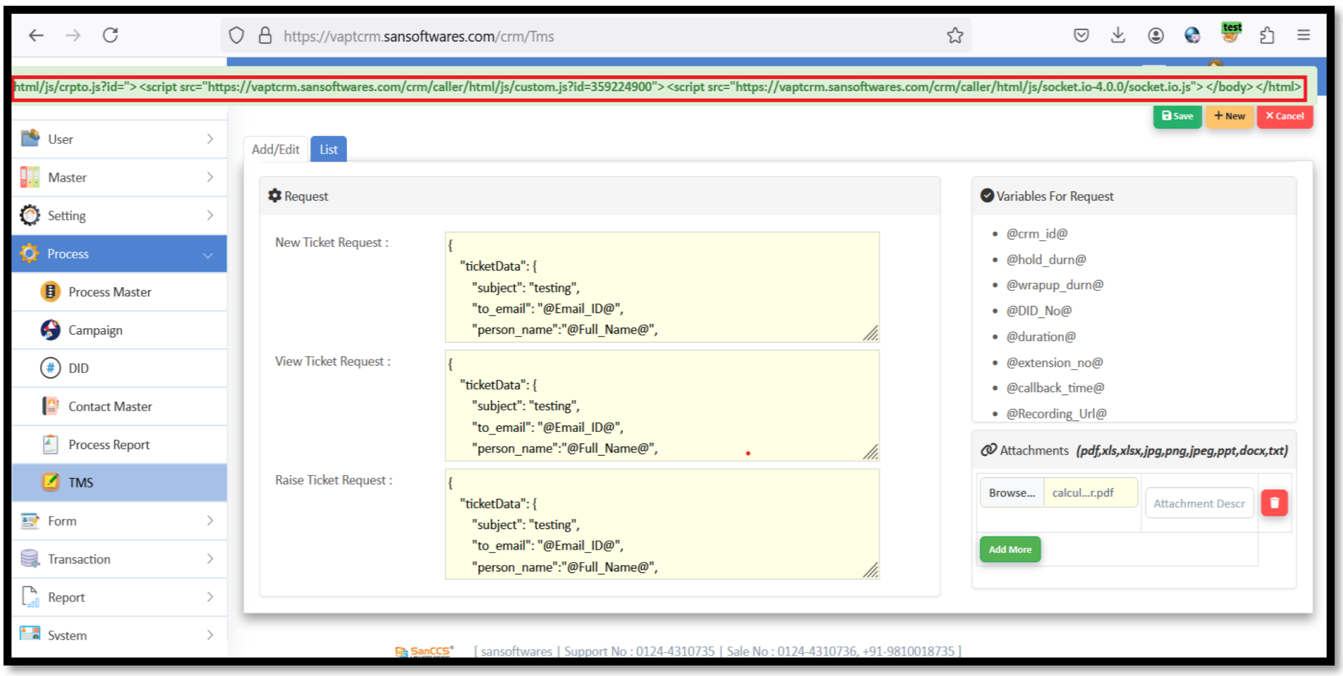
v) **Severity:** Medium

vi) **Recommendation:** Access should be restricted to sensitive files in the application. Only authorized personnel should be able to access sensitive files and proper access control should be maintained/configured to control that.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/200.html

ix) **References to evidences / Proof of Concept:**
Step#1: Observed from the screenshot below, Sensitive file disclosure is occurring in the application.



https://vaptcrm.sansoftwares.com/crm/Tms

```
html/js/crpto.js?id="> <script src="https://vaptcrm.sansoftwares.com/crm/caller/html/js/custom.js?id=359224900"> <script src="https://vaptcrm.sansoftwares.com/crm/caller/html/js/socket.io-4.0.0/socket.io.js"> </body> </html>
```

Request

New Ticket Request :

```
{
  "ticketData": {
    "subject": "testing",
    "to_email": "@Email_ID@",
    "person_name":"@Full_Name@",
```

View Ticket Request :

```
{
  "ticketData": {
    "subject": "testing",
    "to_email": "@Email_ID@",
    "person_name":"@Full_Name@",
```

Raise Ticket Request :

```
{
  "ticketData": {
    "subject": "testing",
    "to_email": "@Email_ID@",
    "person_name":"@Full_Name@",
```

Variables For Request

- @crm_id@
- @hold_durn@
- @wrapup_durn@
- @DID_No@
- @duration@
- @extension_no@
- @callback_time@
- @Recording_Url@

Attachments *(pdf,xls,xlsx,jpg,png,jpeg,ppt,docx,txt)*

Browse... calcul...r.pdf

Attachment Descr

SanCCS [sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

Finding No. 11

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application

ii) **Observation/ Vulnerability title:** Exposure of Sensitive Information to an Unauthorized Actor.

iii) **Detailed observation /vulnerable point:** One or more configuration files are publicly accessible in this application.

iv) **CVE/CWE:** CWE-200

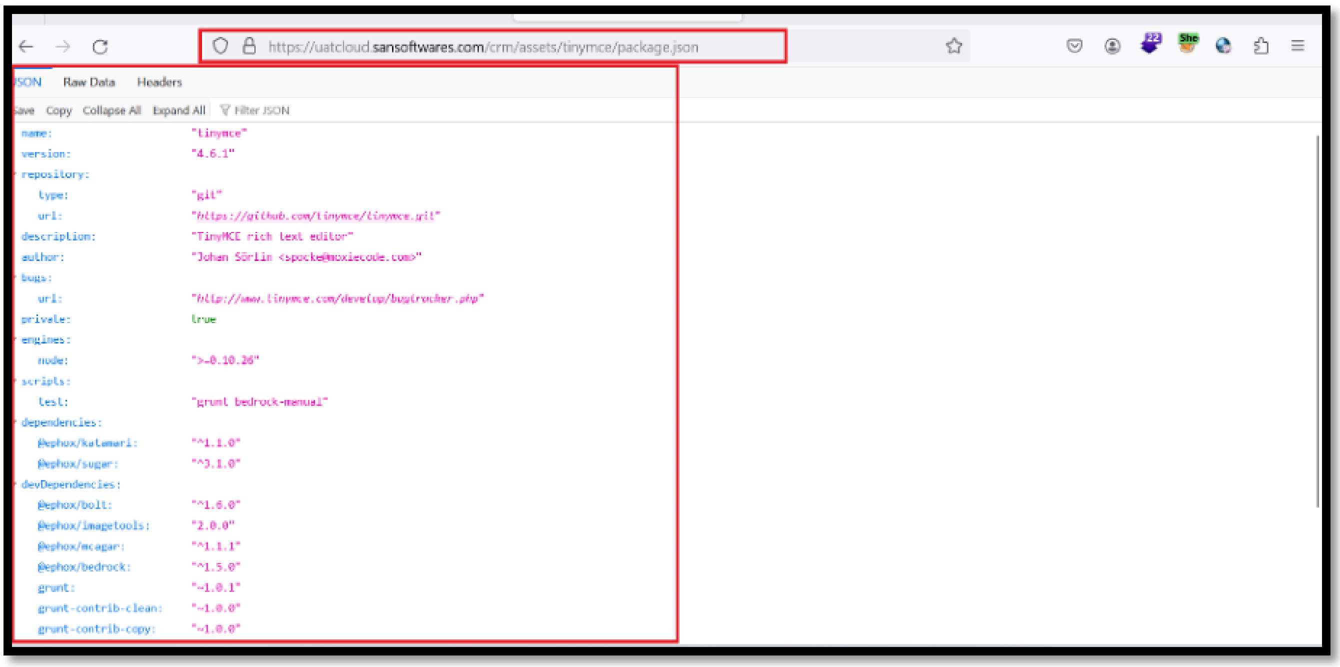
v) **Severity:** Medium

vi) **Recommendation:** Remove or restrict access to all configuration files accessible from internet.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/200.html

ix) **References to evidences / Proof of Concept:**
Step#1: we can see given below package.json file disclosed publicly in this application.


https://uatcloud.sansoftwares.com/crm/assets/tinymce/package.json
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
name:                 "tinymce"
version:              "4.6.1"
repository:
  type:               "git"
  url:                "https://github.com/tinymce/tinymce.git"
description:          "TinyMCE rich text editor"
author:               "Johan Sörlin <spocke@moxiecode.com>"
bugs:
  url:                "http://www.tinymce.com/develop/bugtracker.php"
private:              true
engines:
  node:               ">=0.10.26"
scripts:
  test:               "grunt bedrock-manual"
dependencies:
  @ephox/katamari:    "^1.1.0"
  @ephox/sugar:       "^3.1.0"
devDependencies:
  @ephox/bolt:        "^1.6.0"
  @ephox/imagetools:  "2.0.0"
  @ephox/mcagar:      "^1.1.1"
  @ephox/bedrock:     "^1.5.0"
  grunt:              "~1.0.1"
  grunt-contrib-clean: "~1.0.0"
  grunt-contrib-copy: "~1.0.0"
```

Finding No. 12

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application

ii) **Observation/ Vulnerability title:** Improper Restriction of Rendered UI Layers or Frames

iii) **Detailed observation /vulnerable point:** Clickjacking attack is possible in application.

iv) **CVE/CWE:** CWE-1021

v) **Severity:** Medium

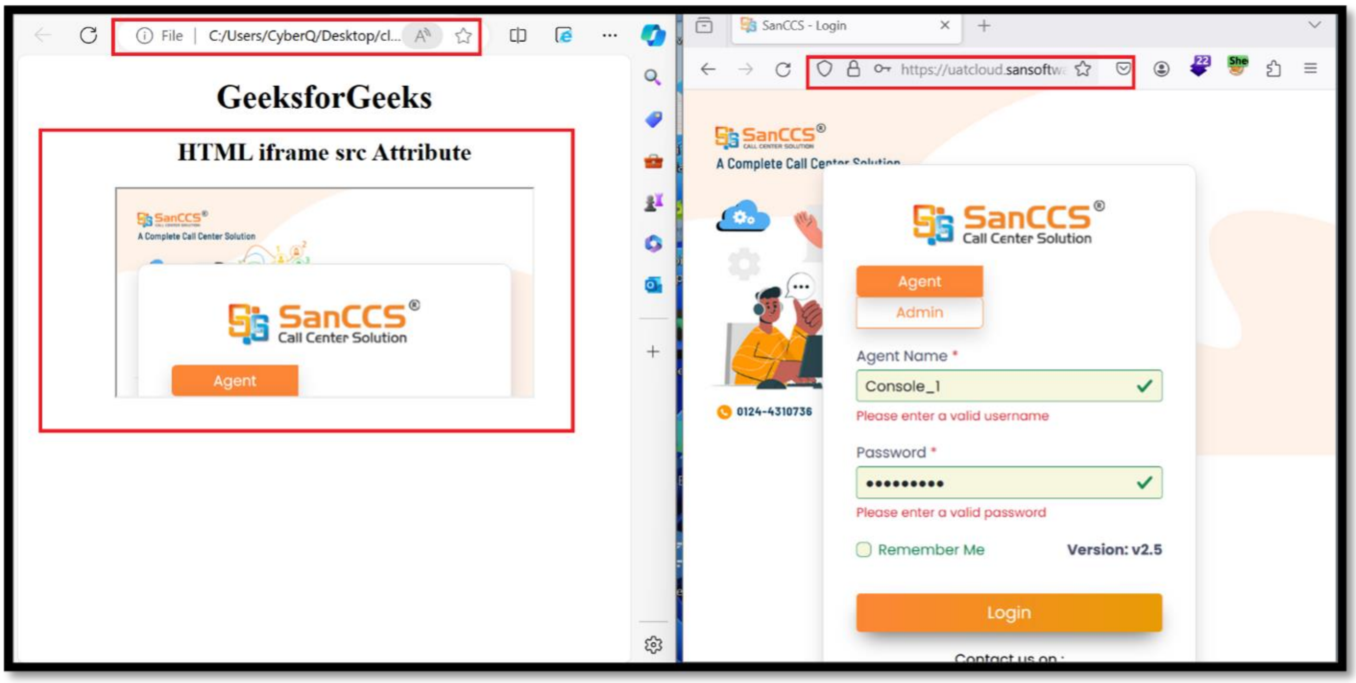
vi) **Recommendation:** The server-side header “X-frame Options” can permit or forbid displaying the page inside a frame. Thus, the application will not be able to open in any third-party application.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/1021.html, https://www.pingidentity.com/en/resources/cybersecurity-fundamentals/threats/clickjacking.html

ix) **References to evidences / Proof of Concept:**

Step#1: We can see in below screenshot; application is open in a frame. So, clickjacking possible in this application.



File | C:/Users/CyberQ/Desktop/cl...
GeeksforGeeks
HTML iframe src Attribute
SanCCS
A Complete Call Center Solution
SanCCS Call Center Solution
Agent
SanCCS - Login
https://uatcloud.sansoftw
SanCCS
A Complete Call Center Solution
0124-4310736
SanCCS Call Center Solution
Agent
Admin
Agent Name *
Console_1
Please enter a valid username
Password *
•••••••••
Please enter a valid password
Remember Me
Version: v2.5
Login
Contact us on :

Finding No. 13

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Exposure of Sensitive Information to an Unauthorized Actor.

iii) Detailed observation /vulnerable point: Banner grabbing (application is displaying Server name/version and web technology name/version which may help attacker to learn more about his target) is possible in the application.

iv) CVE/CWE: CWE-200

v) Severity: Medium

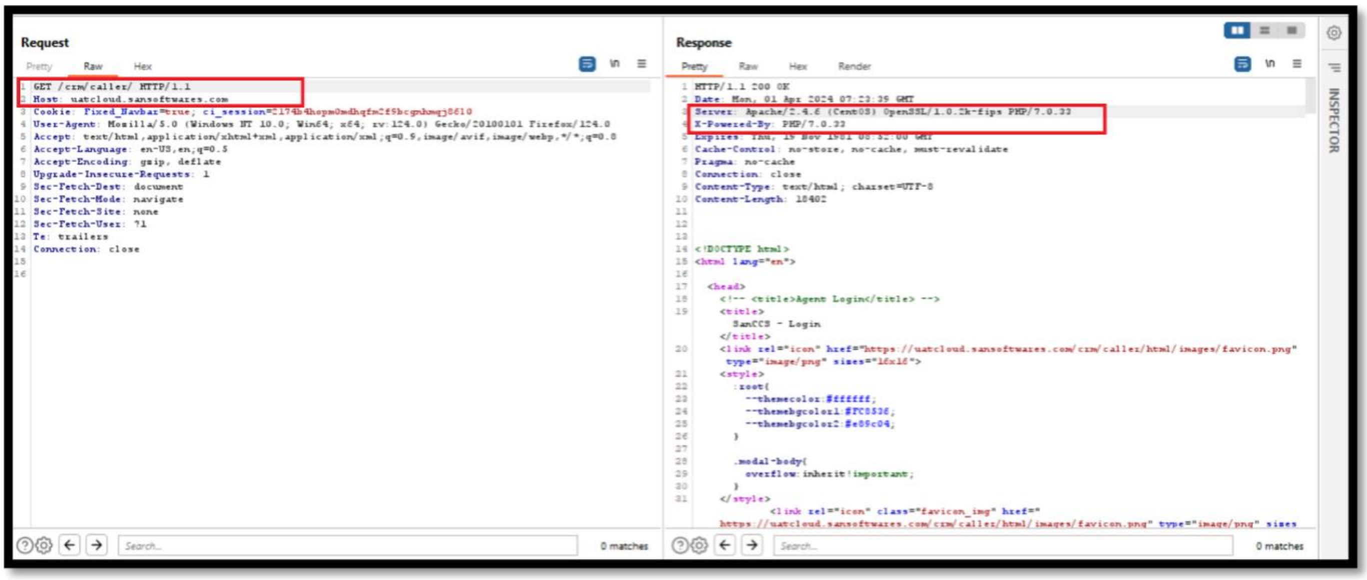
vi) Recommendation: Server and Web technology version should not be displayed to the end user.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/200.html, https://support.smarten.com/support/solutions/articles/9000203049-banner-grabbing-vulnerabilities-and-solutions

ix) References to evidences / Proof of Concept:

Step#1: Using Burp Suite, we capture the request of a webpage of the application and we can see in below snapshot that Server and version information's are easily visible in this application.



```
GET /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:23:39 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18402



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8526;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
            <link rel="icon" class="favicon_img" href="
    https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png" type="image/png" sizes
```

Finding No. 14

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Protection Mechanism Failure

iii) Detailed observation /vulnerable point: All HTTP Security Headers are missing at some pages in the application.

iv) CVE/CWE: CWE-693

v) Severity: Medium

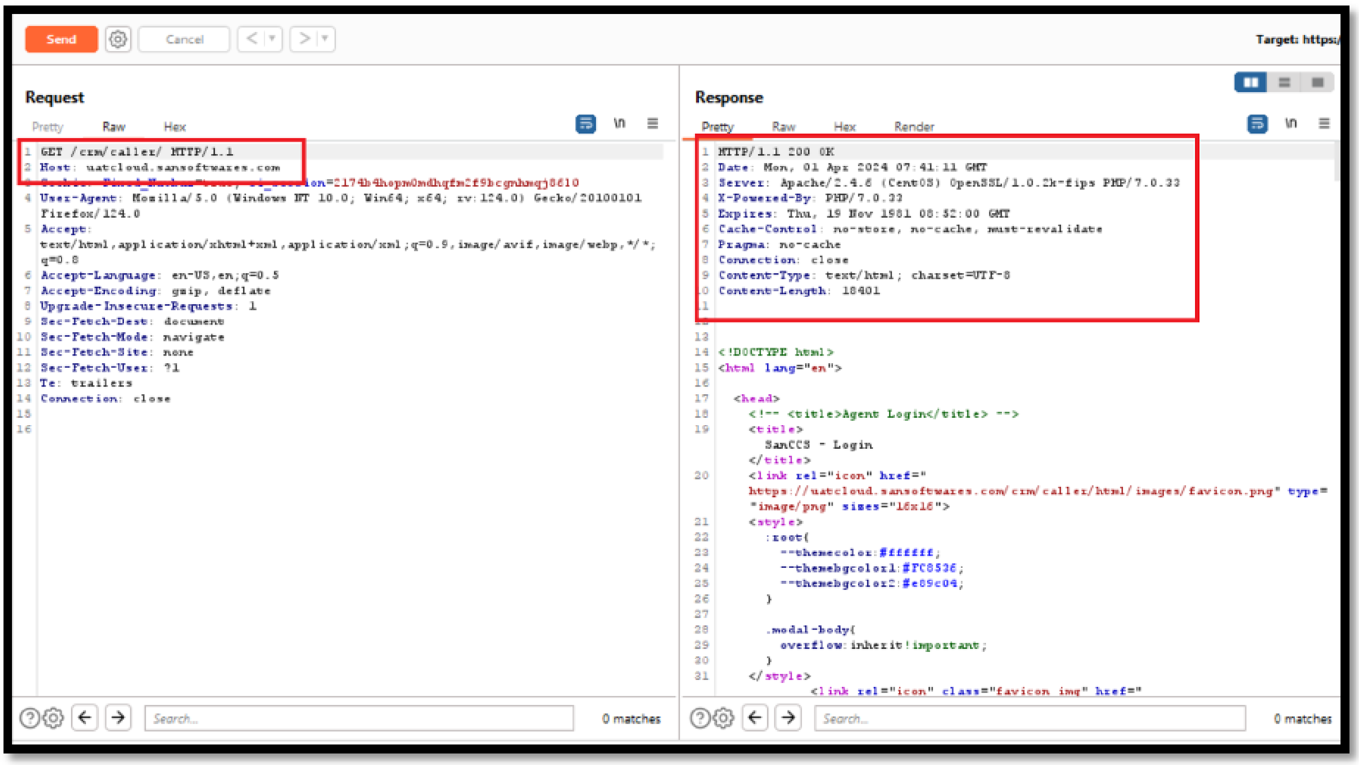
vi) Recommendation: HTTP security headers are a fundamental part of website security. Upon implementation, they protect you against the types of attacks that your site is most likely to come across. These headers protect against XSS, code injection, click jacking, etc. The following headers should be implemented. • Cross Site Scripting Protection (X-XSS) • Content Security Policy (CSP) • HTTP Strict Transport Security (HSTS) • X-Frame-Option • X-Content-Type-Options.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/693.html, https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

ix) References to evidences / Proof of Concept:

Step#1: We can see in this application here are all header missing.



Request

```
GET /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Header=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101
Firefox/124.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:41:11 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18401



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="
    https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png" type=
    "image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
          <link rel="icon" class="favicon img" href="
```

Finding No. 15

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Improper Restriction of Excessive Authentication Attempts

iii) **Detailed observation / Vulnerable point**: There is no limit on number of incorrect passwords retries while trying to login. This may lead to Brute force attack.

iv) **CVE/CWE:** CWE-307

v) **Severity:** Medium

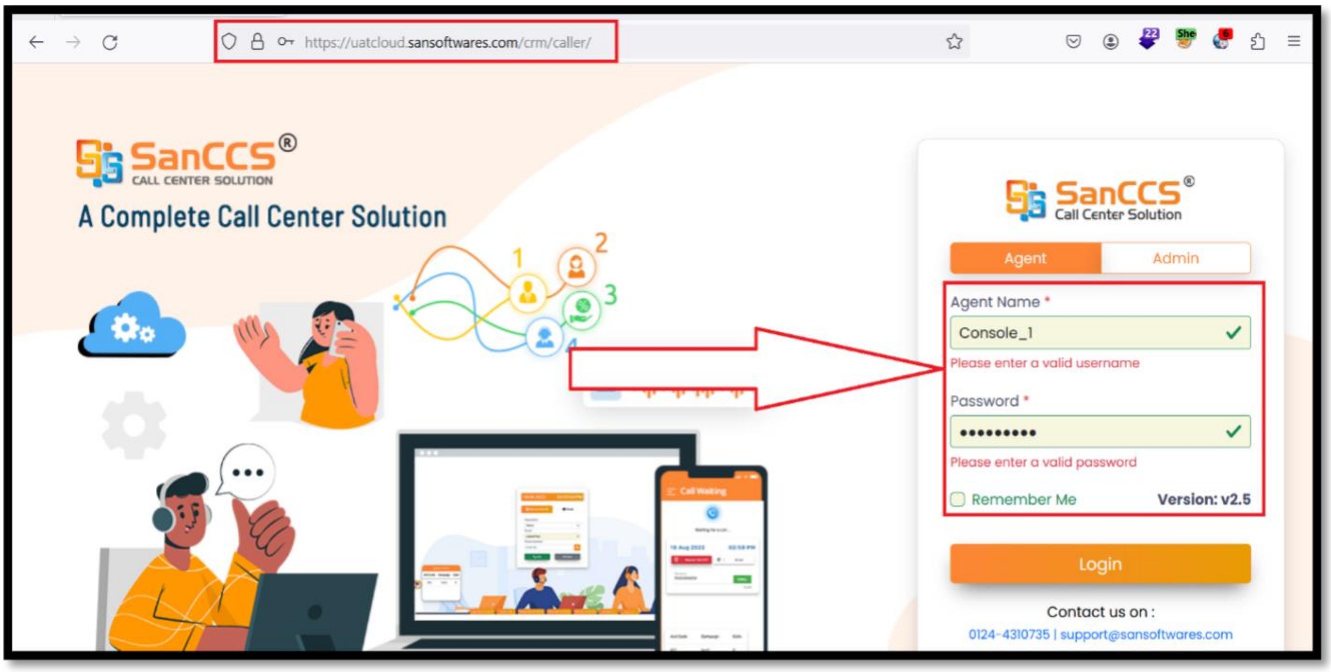
vi) **Recommendation:** Users should be restricted to a defined number of login attempts per unit of time. After that defined number of login attempt, application should block that user account or CAPTCHA can be implemented at login page. This way automated attempt to login can be checked and brute force attacks can be prevented. CAPTCHA should follow the following condition: a) The combination of alphanumeric value. b) Combination of Upper case and lower-case letters. c) Case-Sensitive d) Its length should be minimum 6 characters. e) Should not be a third-party CAPTCHA: f) Should be Random and not follow a pattern. g) Example: Ab73jy, PT34h8, Hos3t3, nic23n etc.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/757.html,
https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

ix) **References to evidences / Proof of Concept:**

Step#1: We can see there is not set any limit or CAPTCHA implemented.



https://uatcloud.sansoftwares.com/crm/caller/

Agent Name * Console_1 ✓

Please enter a valid username

Password * ••••••••• ✓

Please enter a valid password

□ Remember Me Version: v2.5

Contact us on :
0124-4310735 | support@sansoftwares.com

Finding No. 16

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application

ii) **Observation/ Vulnerability title:** Trusting HTTP Permission Methods on the Server Side

iii) **Detailed observation /vulnerable point:** HTTP Methods are enabled in the application.

iv) **CVE/CWE:** CWE-650

v) **Severity:** Medium

vi) **Recommendation:** HTTP methods should be disabled in the application which may prevent the application from security breach. Only GET and POST method should be enabled in the application.

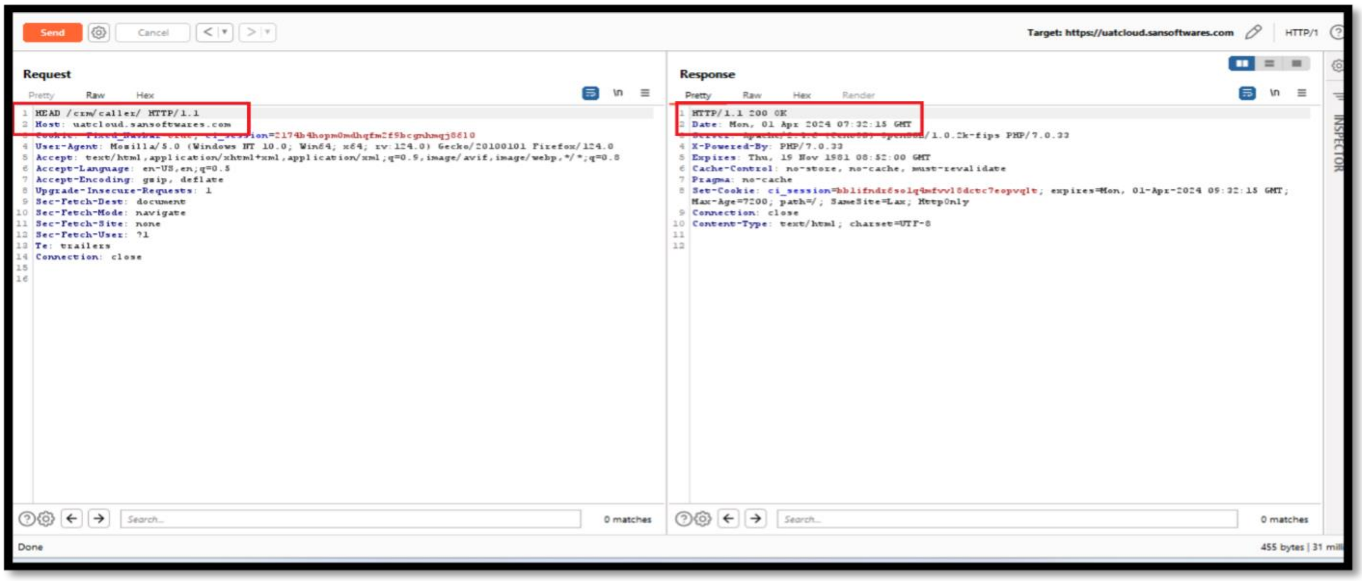
vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/650.html

ix) **References to evidences / Proof of Concept:**

Case#1: HEAD Method Enabled

Step#1: We can see Head method enable in this application.

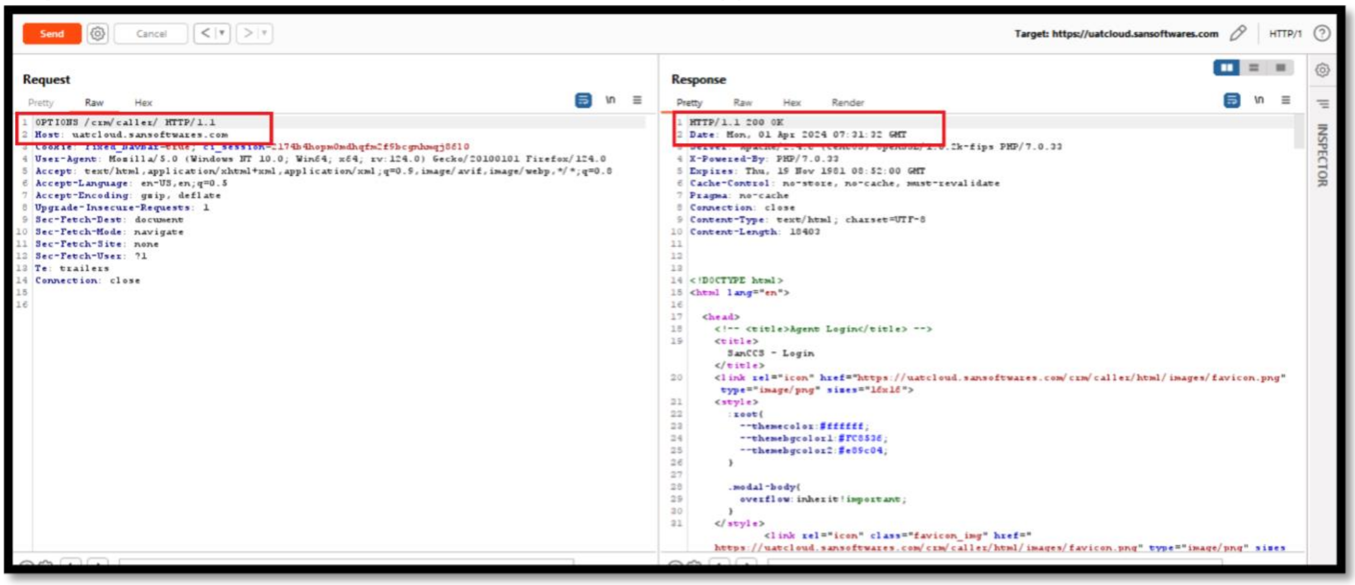


```
HEAD /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:32:15 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: ci_session=bblifndr6solq4mfvvl8dctc7eopvqlt; expires=Mon, 01-Apr-2024 09:32:15 GMT;
Max-Age=7200; path=/; SameSite=Lax; HttpOnly
Connection: close
Content-Type: text/html; charset=UTF-8
```

Case#2: OPTIONS Method Enabled

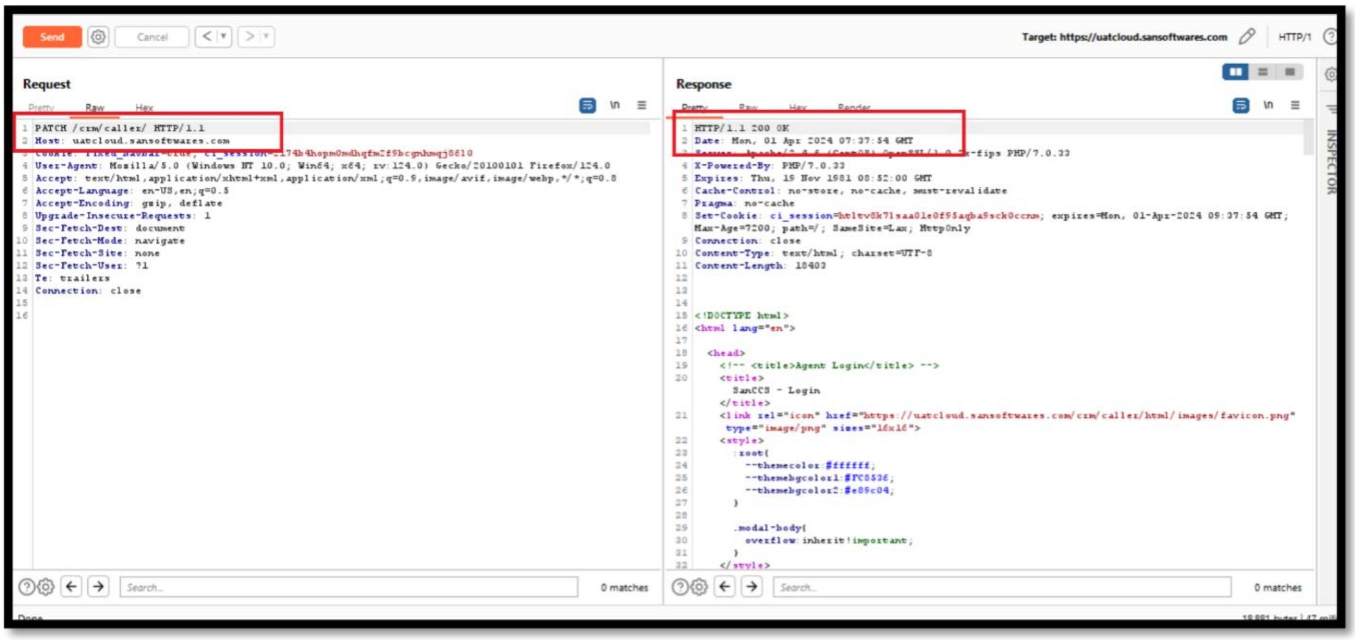
Step#1: We can see OPTIONS method enable in this application.



```
OPTIONS /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:31:32 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18403



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e09c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
            <link rel="icon" class="favicon_img" href="
    https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png" type="image/png" sizes
```

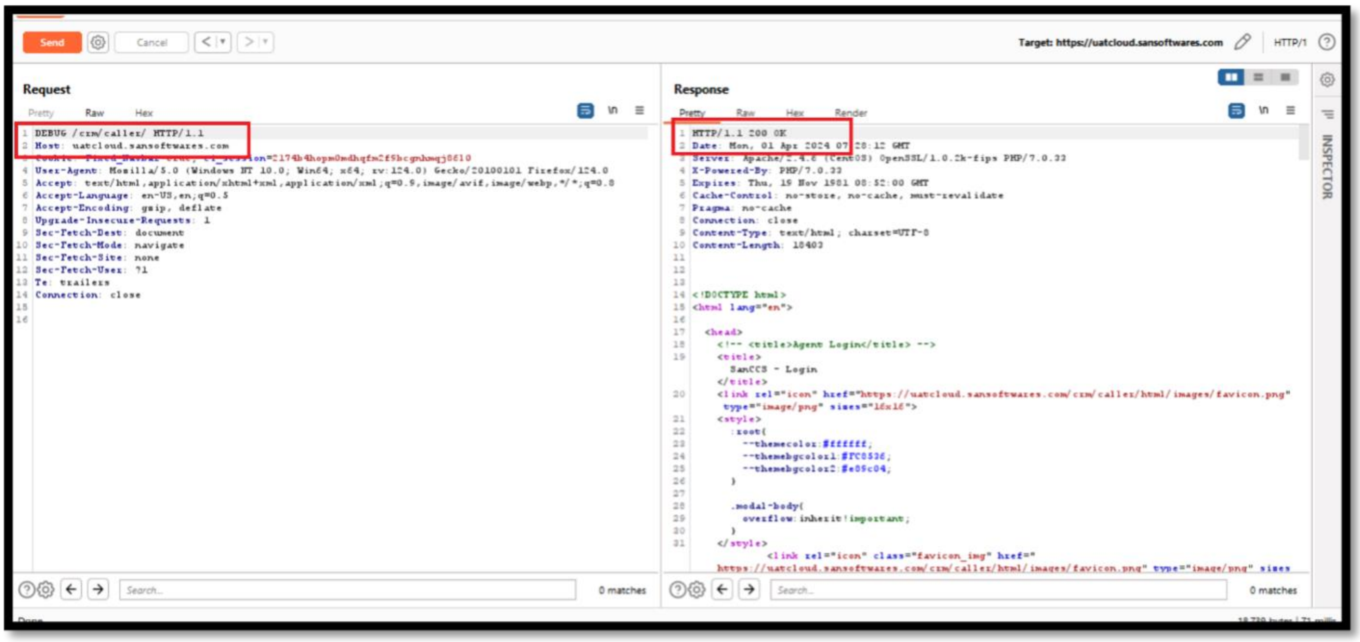
Case#3: Patch Method Enabled
Step#1: We can see Patch method enable in this application.



```
PATCH /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:37:54 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: ci_session=htltv8k71saa0le0f95aqba9sck0ccnm; expires=Mon, 01-Apr-2024 09:37:54 GMT;
Max-Age=7200; path=/; SameSite=Lax; HttpOnly
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18403



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
```

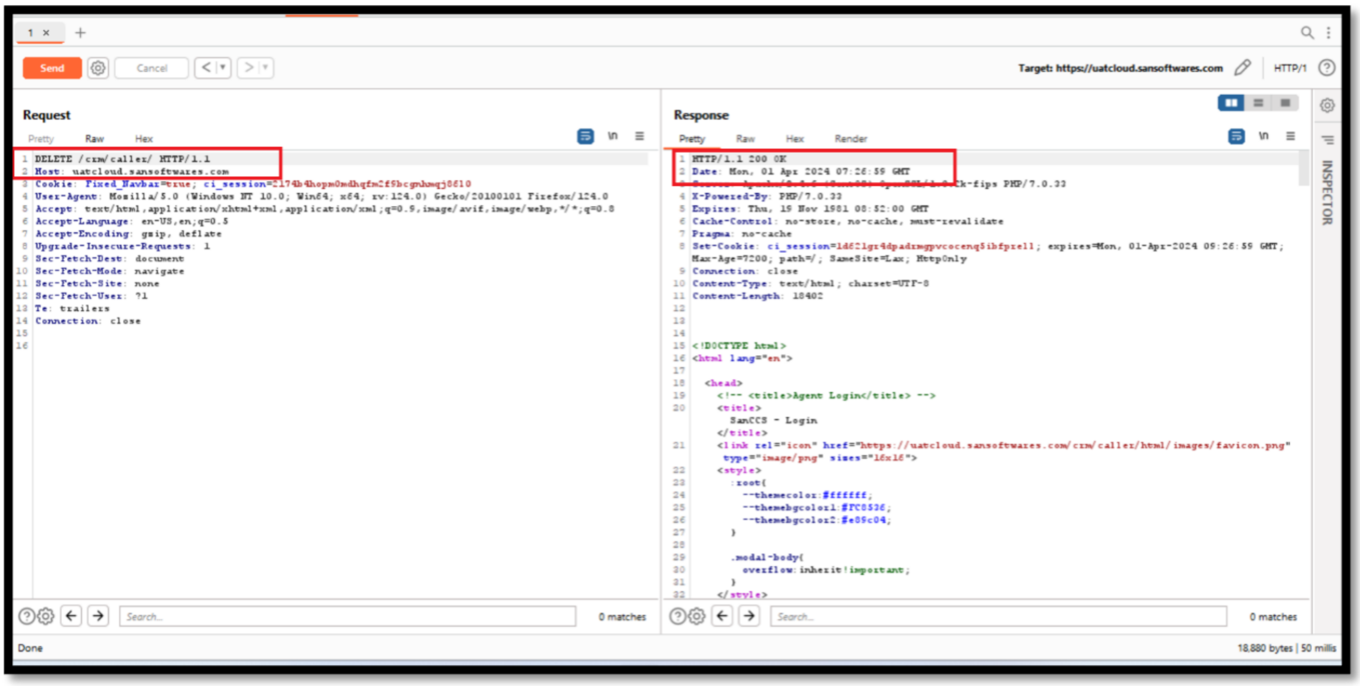
Case#4: DEBUG Method Enabled
Step#1: We can see Debug method enable in this application.



```
DEBUG /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:28:12 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18403



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
            <link rel="icon" class="favicon_img" href="
https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png" type="image/png" sizes
```

Case#5: Delete Method Enabled
Step#1: We can see Delete method enable in this application.

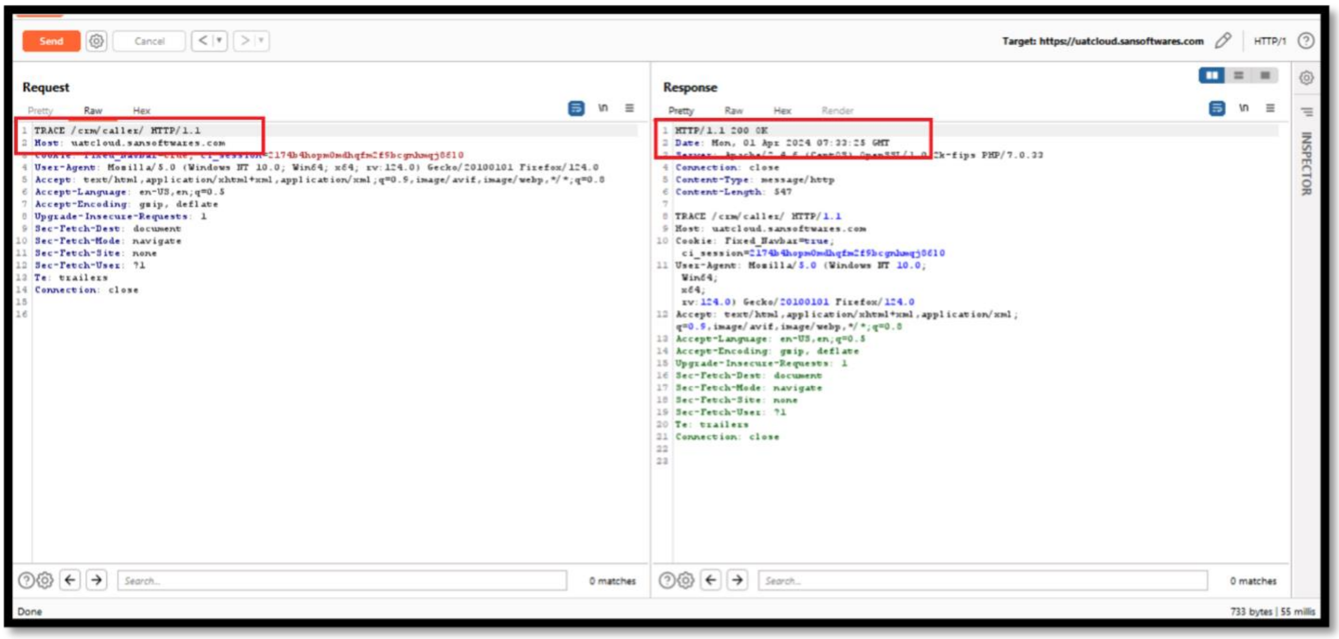


```
DELETE /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:26:59 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: ci_session=1d621gr4dpadrmgpvcocenq5ibfprell; expires=Mon, 01-Apr-2024 09:26:59 GMT;
Max-Age=7200; path=/; SameSite=Lax; HttpOnly
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18402



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
```

Case#6: TRACE Method Enabled

Step#1: We can see Trace method enable in this application.



Target: https://uatcloud.sansoftwares.com

Request:

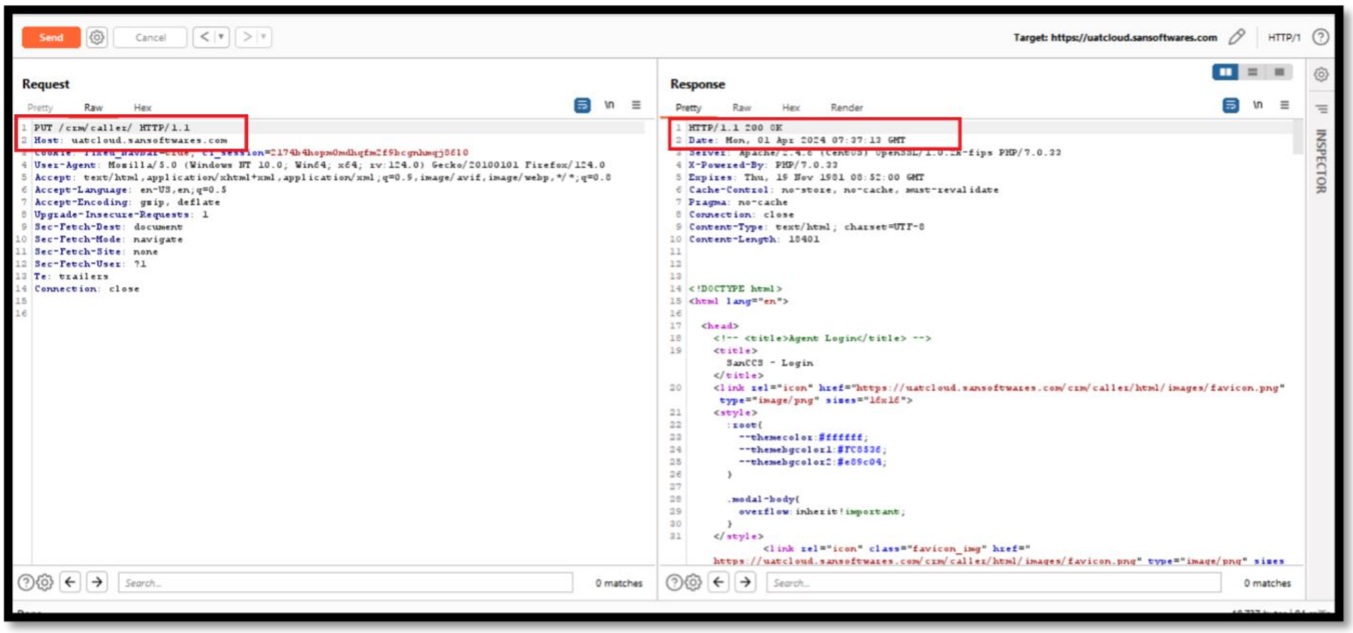
```
TRACE /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:33:25 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
Connection: close
Content-Type: message/http
Content-Length: 547

TRACE /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true;
 ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0;
 Win64;
 x64;
 rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;
q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

Case#7: PUT Method Enabled

Step#1: We can see Put method enable in this application.



Target: https://uatcloud.sansoftwares.com

Request:

```
PUT /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close


```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:37:13 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18401



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
            <link rel="icon" class="favicon_img" href="
    https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png" type="image/png" sizes
```

Finding No. 17

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Use of Unmaintained Third-Party Components

iii) Detailed observation / Vulnerable point: Old and vulnerable version of libraries and environment are still being used in the application.

iv) CVE/CWE: CWE-1104

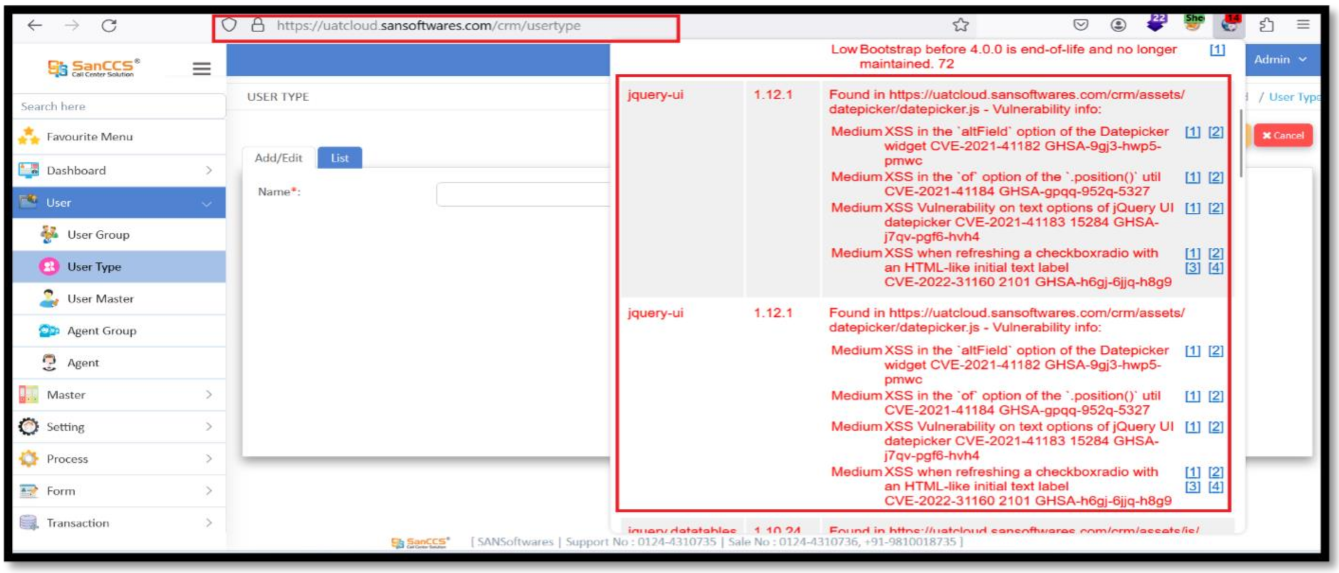
v) Severity: Medium

vi) Recommendation: It is recommended to use latest and stable version for more secured application.

vii) Current Status: Closed

viii) Reference https://cwe.mitre.org/data/definitions/1104.html

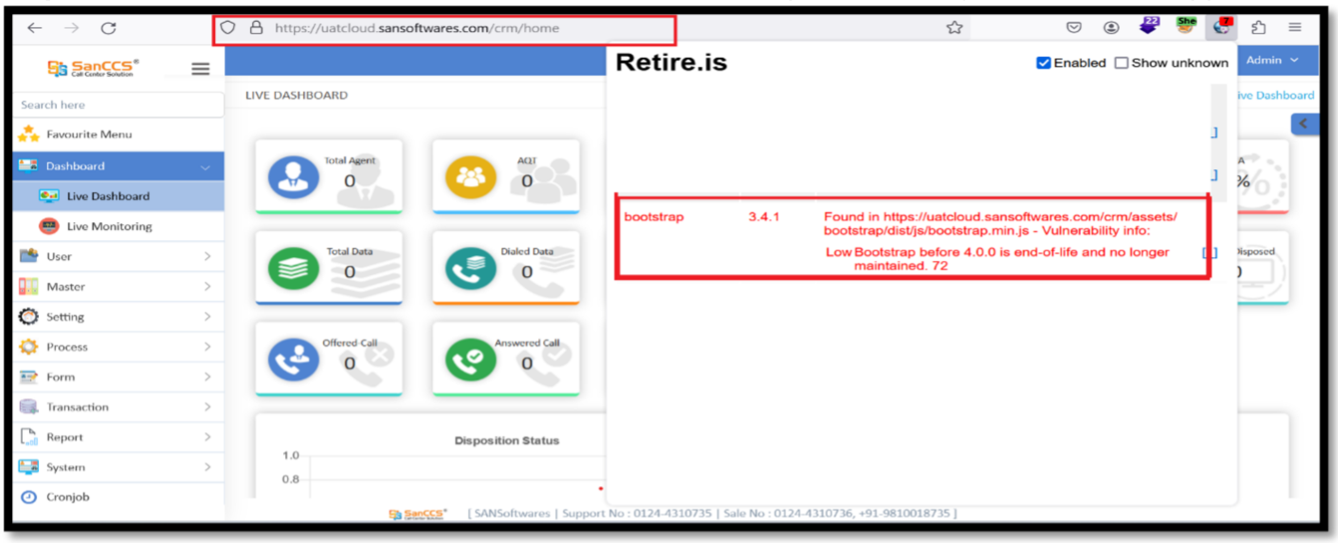
ix) References to evidences / Proof of Concept:
Case#1: Old and vulnerable jQuery-UI
Step#1: Old and vulnerable version of jQuery-UI is being used in application.



https://uatcloud.sansoftwares.com/crm/usertype

```
Low    Bootstrap before 4.0.0 is end-of-life and no longer             [1]
       maintained. 72

jquery-ui   1.12.1   Found in https://uatcloud.sansoftwares.com/crm/assets/
                     datepicker/datepicker.js - Vulnerability info:
                     Medium XSS in the `altField` option of the Datepicker   [1] [2]
                            widget CVE-2021-41182 GHSA-9gj3-hwp5-
                            pmwc
                     Medium XSS in the `of` option of the `.position()` util [1] [2]
                            CVE-2021-41184 GHSA-gpqq-952q-5327
                     Medium XSS Vulnerability on text options of jQuery UI  [1] [2]
                            datepicker CVE-2021-41183 15284 GHSA-
                            j7qv-pgf6-hvh4
                     Medium XSS when refreshing a checkboxradio with        [1] [2]
                            an HTML-like initial text label                 [3] [4]
                            CVE-2022-31160 2101 GHSA-h6gj-6jjq-h8g9

jquery-ui   1.12.1   Found in https://uatcloud.sansoftwares.com/crm/assets/
                     datepicker/datepicker.js - Vulnerability info:
                     Medium XSS in the `altField` option of the Datepicker   [1] [2]
                            widget CVE-2021-41182 GHSA-9gj3-hwp5-
                            pmwc
                     Medium XSS in the `of` option of the `.position()` util [1] [2]
                            CVE-2021-41184 GHSA-gpqq-952q-5327
                     Medium XSS Vulnerability on text options of jQuery UI  [1] [2]
                            datepicker CVE-2021-41183 15284 GHSA-
                            j7qv-pgf6-hvh4
                     Medium XSS when refreshing a checkboxradio with        [1] [2]
                            an HTML-like initial text label                 [3] [4]
                            CVE-2022-31160 2101 GHSA-h6gj-6jjq-h8g9
```

Case#2: Old and vulnerable bootstrap
Step#1: Old and vulnerable version of bootstrap is being used in application.



https://uatcloud.sansoftwares.com/crm/home

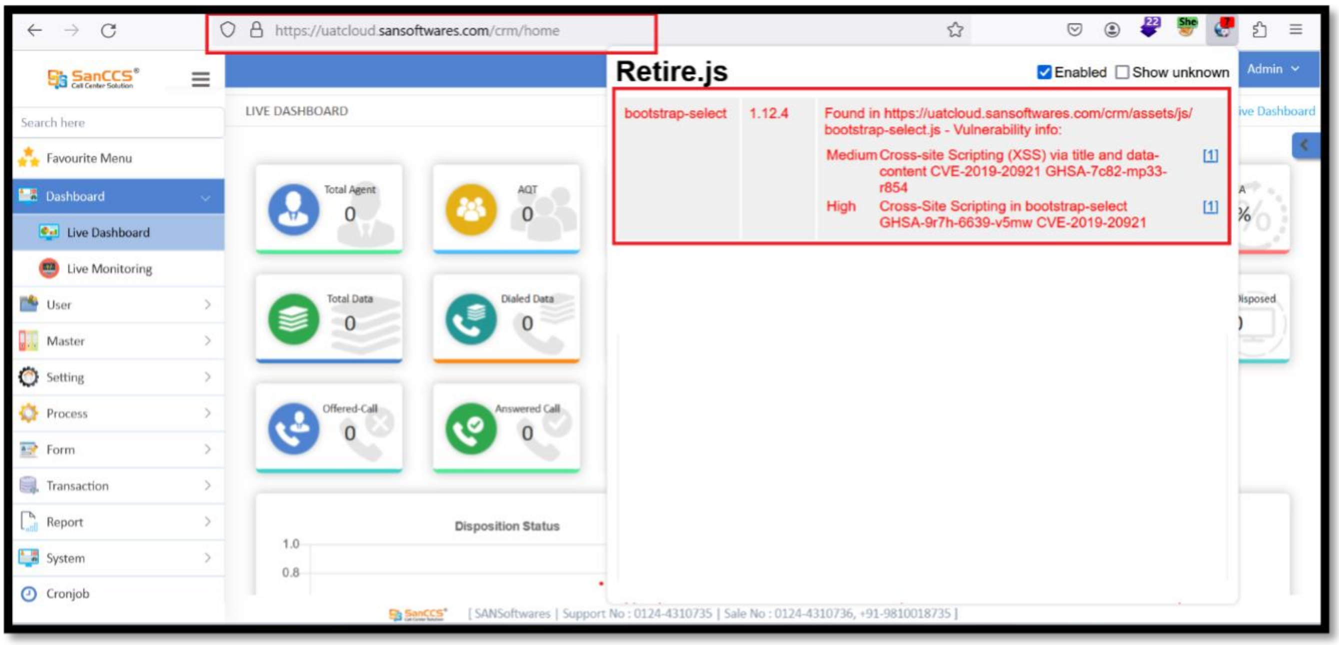
Retire.js

☑ Enabled ☐ Show unknown

```
bootstrap   3.4.1   Found in https://uatcloud.sansoftwares.com/crm/assets/
                    bootstrap/dist/js/bootstrap.min.js - Vulnerability info:
                    Low  Bootstrap before 4.0.0 is end-of-life and no longer   [ ]
                         maintained. 72
```

Case#3: Old and vulnerable bootstrap-select

Step#1: Old and vulnerable version of bootstrap-select is being used in application.

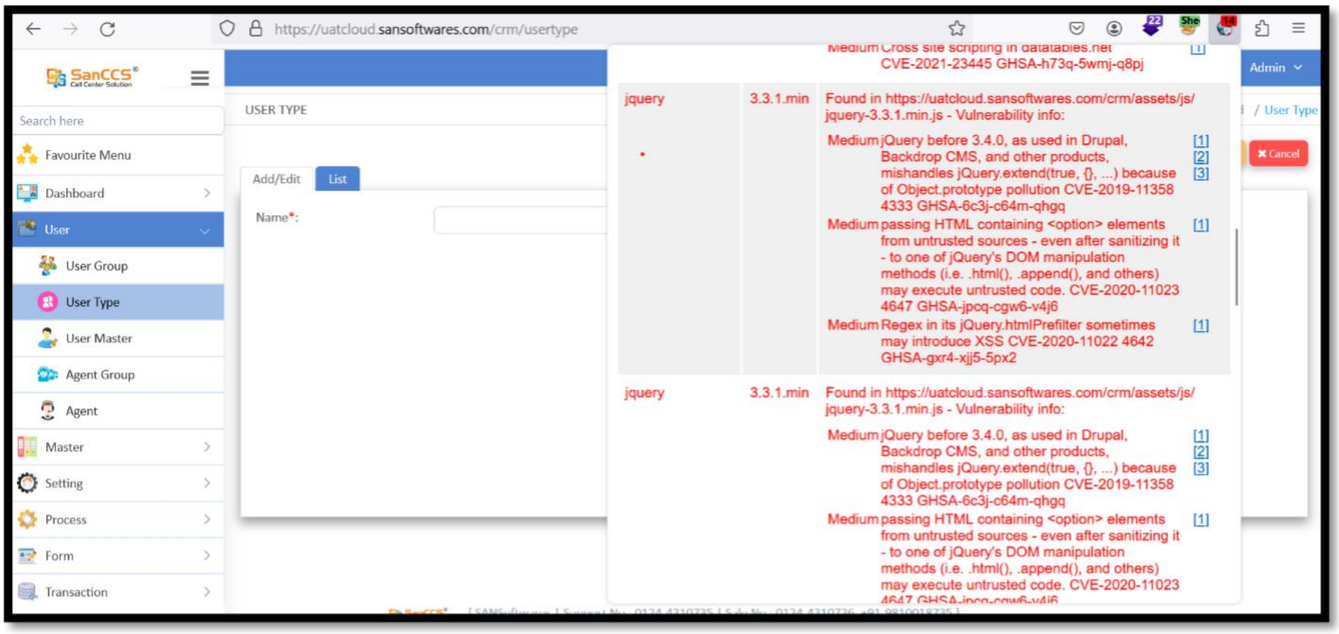


Retire.js ☑ Enabled □ Show unknown

bootstrap-select	1.12.4	Found in https://uatcloud.sansoftwares.com/crm/assets/js/bootstrap-select.js - Vulnerability info: Medium Cross-site Scripting (XSS) via title and data-content CVE-2019-20921 GHSA-7c82-mp33-r854 [1] High Cross-Site Scripting in bootstrap-select GHSA-9r7h-6639-v5mw CVE-2019-20921 [1]

Case#4: Old and vulnerable jQuery

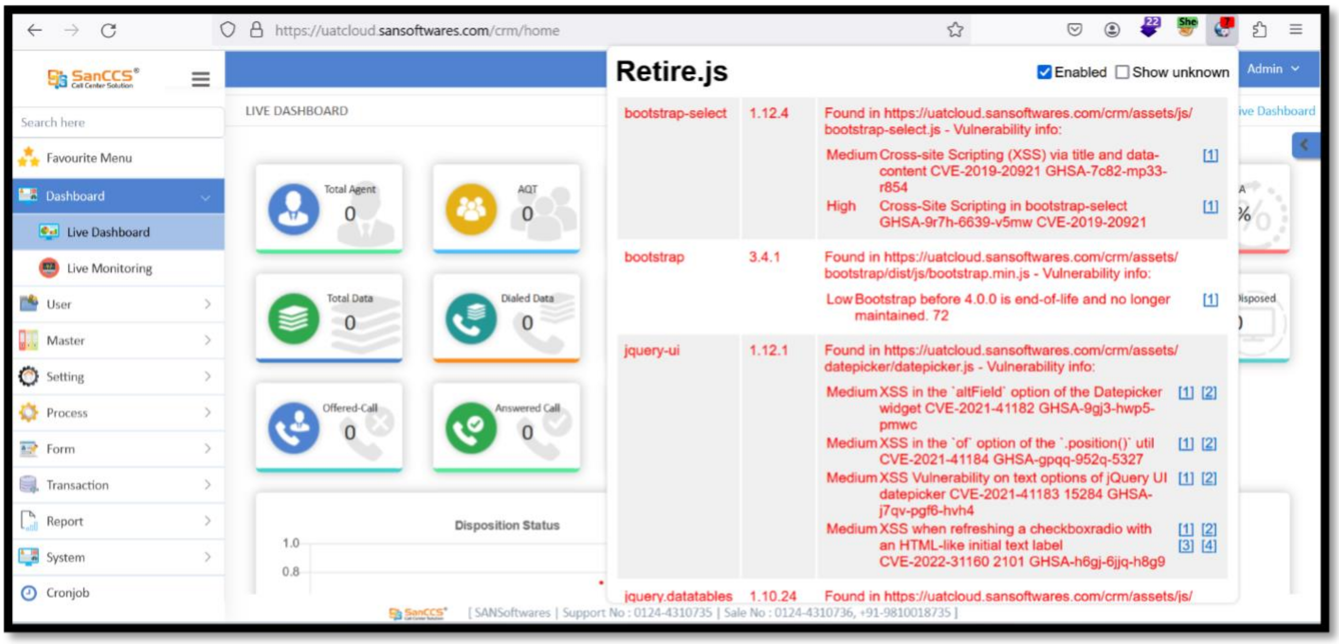
Step#1: Old and vulnerable version of jQuery is being used in application.



		Medium Cross site scripting in datatables.net CVE-2021-23445 GHSA-h73q-5wmj-q8pj [1]
jquery	3.3.1.min	Found in https://uatcloud.sansoftwares.com/crm/assets/js/jquery-3.3.1.min.js - Vulnerability info: Medium jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution CVE-2019-11358 4333 GHSA-6c3j-c64m-qhgq [1] [2] [3] Medium passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6 [1] Medium Regex in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gxr4-xjj5-5px2 [1]
jquery	3.3.1.min	Found in https://uatcloud.sansoftwares.com/crm/assets/js/jquery-3.3.1.min.js - Vulnerability info: Medium jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution CVE-2019-11358 4333 GHSA-6c3j-c64m-qhgq [1] [2] [3] Medium passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6 [1]

Case#5: Old and vulnerable jquery-datatables

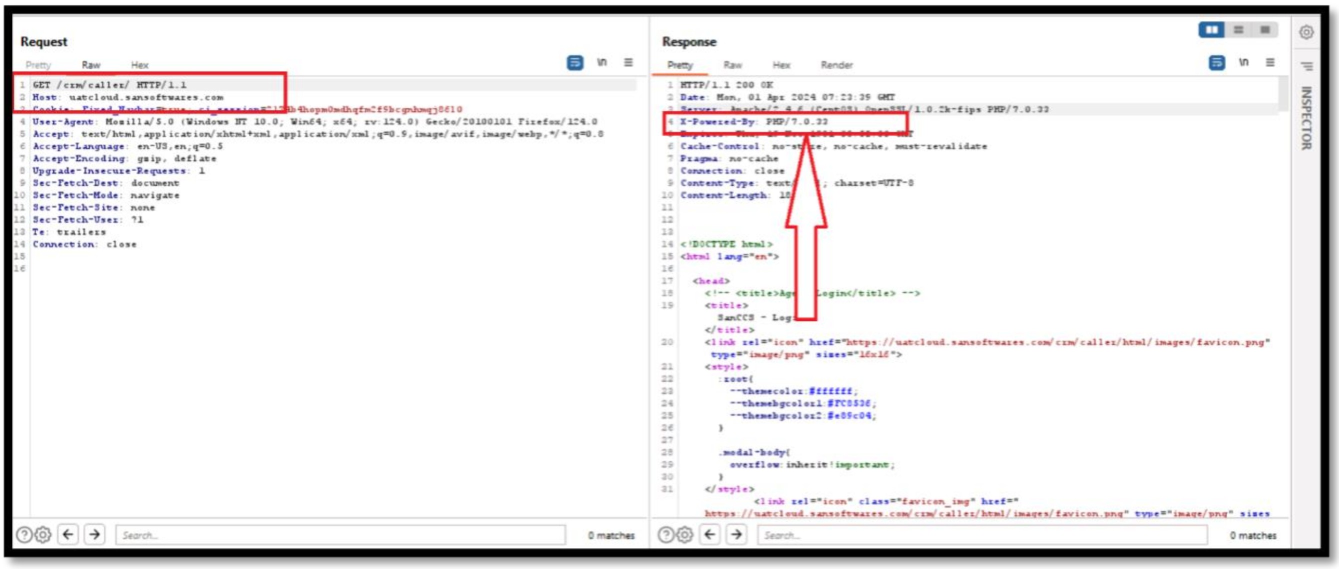
Step#1: Old and vulnerable version of jQuery-datatables is being used in application.



Retire.js ☑ Enabled □ Show unknown

bootstrap-select	1.12.4	Found in https://uatcloud.sansoftwares.com/crm/assets/js/bootstrap-select.js - Vulnerability info: Medium Cross-site Scripting (XSS) via title and data-content CVE-2019-20921 GHSA-7c82-mp33-r854 [1] High Cross-Site Scripting in bootstrap-select GHSA-9r7h-6639-v5mw CVE-2019-20921 [1]
bootstrap	3.4.1	Found in https://uatcloud.sansoftwares.com/crm/assets/bootstrap/dist/js/bootstrap.min.js - Vulnerability info: Low Bootstrap before 4.0.0 is end-of-life and no longer maintained. 72 [1]
jquery-ui	1.12.1	Found in https://uatcloud.sansoftwares.com/crm/assets/datepicker/datepicker.js - Vulnerability info: Medium XSS in the `altField` option of the Datepicker widget CVE-2021-41182 GHSA-9gj3-hwp5-pmwc [1] [2] Medium XSS in the `of` option of the `.position()` util CVE-2021-41184 GHSA-gpqq-952q-5327 [1] [2] Medium XSS Vulnerability on text options of jQuery UI datepicker CVE-2021-41183 15284 GHSA-j7qv-pgf6-hvh4 [1] [2] Medium XSS when refreshing a checkboxradio with an HTML-like initial text label CVE-2022-31160 2101 GHSA-h6gj-6jjq-h8g9 [1] [2] [3] [4]
jquery.datatables	1.10.24	Found in https://uatcloud.sansoftwares.com/crm/assets/js/

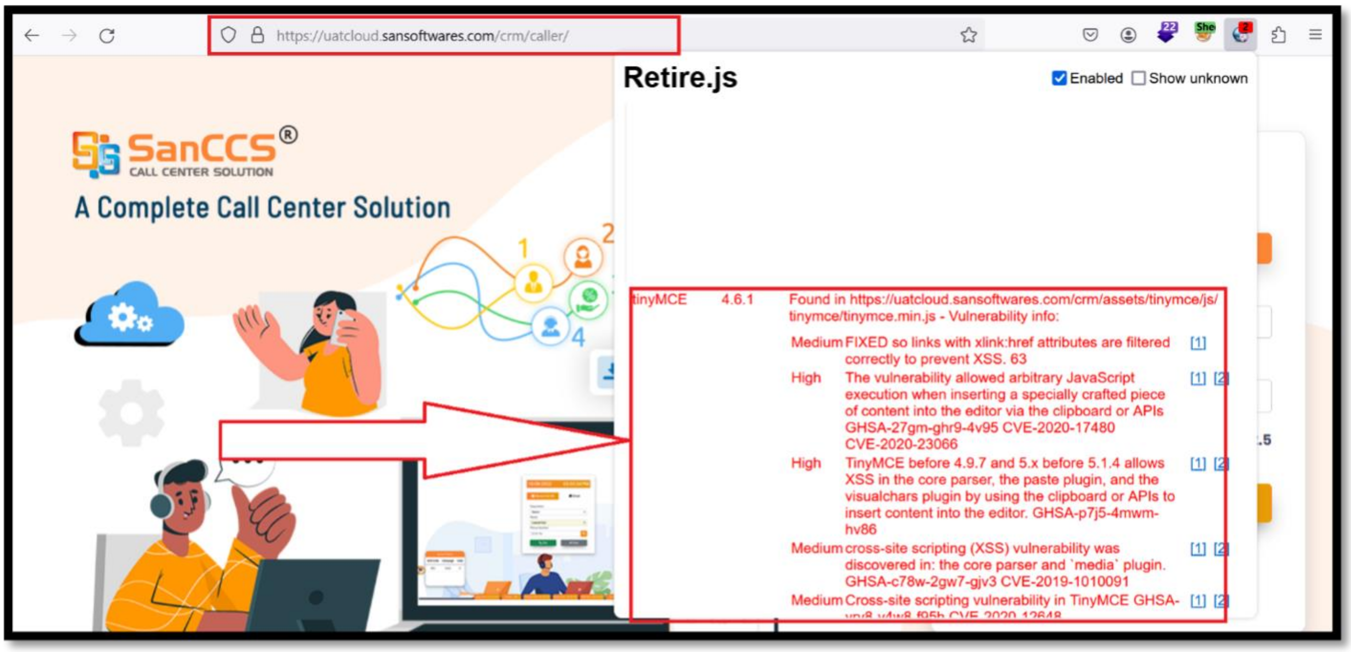
Case#6: Old and vulnerable PHP
Step#1: Old and vulnerable version of php is being used in application.



```
GET /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:23:39 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18402



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
            <link rel="icon" class="favicon_img" href="
    https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png" type="image/png" sizes
```

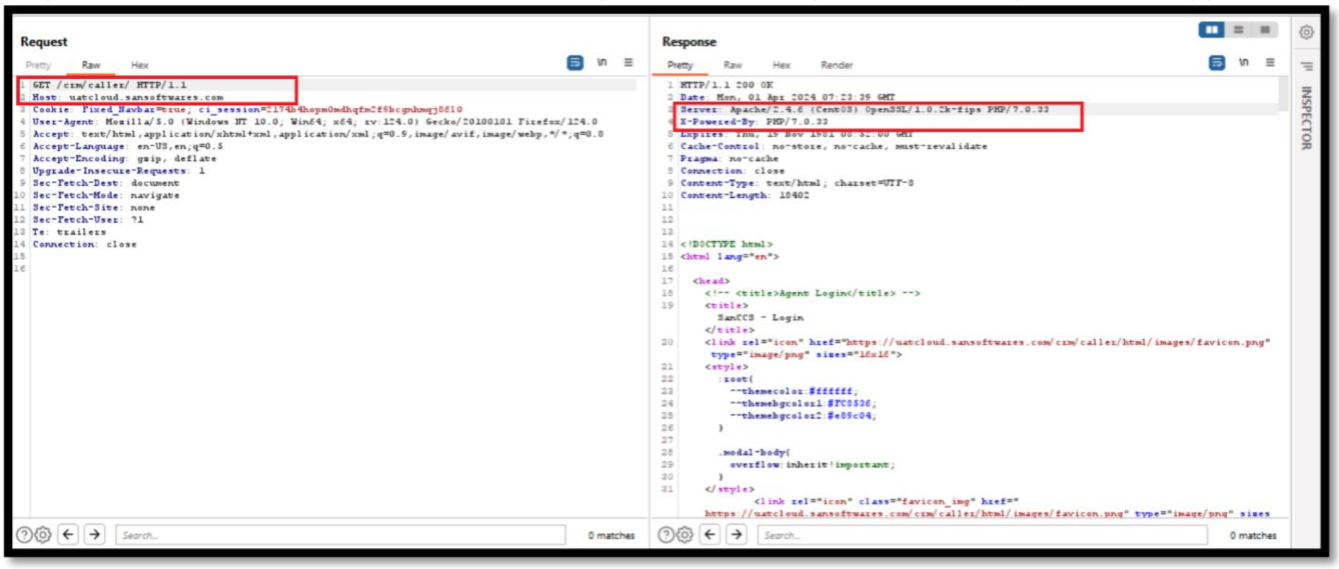
Case#7: Old and vulnerable tinyMCE
Step#1: Old and vulnerable version of tinyMCE is being used in application.


https://uatcloud.sansoftwares.com/crm/caller/
SanCCS®
CALL CENTER SOLUTION
A Complete Call Center Solution
1
2
4
Retire.js
☑ Enabled ☐ Show unknown

tinyMCE 4.6.1 Found in https://uatcloud.sansoftwares.com/crm/assets/tinymce/js/tinymce/tinymce.min.js - Vulnerability info:

Medium	FIXED so links with xlink:href attributes are filtered correctly to prevent XSS. 63	[1]
High	The vulnerability allowed arbitrary JavaScript execution when inserting a specially crafted piece of content into the editor via the clipboard or APIs GHSA-27gm-ghr9-4v95 CVE-2020-17480 CVE-2020-23066	[1] [2]
High	TinyMCE before 4.9.7 and 5.x before 5.1.4 allows XSS in the core parser, the paste plugin, and the visualchars plugin by using the clipboard or APIs to insert content into the editor. GHSA-p7j5-4mwm-hv86	[1] [2]
Medium	cross-site scripting (XSS) vulnerability was discovered in: the core parser and `media` plugin. GHSA-c78w-2gw7-gjv3 CVE-2019-1010091	[1] [2]
Medium	Cross-site scripting vulnerability in TinyMCE GHSA-vrv8-v4w8-f95h CVE-2020-12648	[1] [2]

Case#8: Old and vulnerable OpenSSL and Apache
Step#1: Old and vulnerable version of OpenSSL and Apache is being used in application.



```
GET /crm/caller/ HTTP/1.1
Host: uatcloud.sansoftwares.com
Cookie: Fixed_Navbar=true; ci_session=2174b4hopm0mdhqfm2f9bcgnhmqj8610
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 01 Apr 2024 07:23:39 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
X-Powered-By: PHP/7.0.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18402



<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png"
     type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
        overflow:inherit!important;
      }
    </style>
            <link rel="icon" class="favicon_img" href="
    https://uatcloud.sansoftwares.com/crm/caller/html/images/favicon.png" type="image/png" sizes
```

Finding No. 18

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling').

iii) Detailed observation / Vulnerable point: Client-side desync (CSD) vulnerabilities occur when a web server fails to correctly process the Content-Length of POST requests. By exploiting this behavior, an attacker can force a victim's browser to desynchronize its connection with the website, typically leading to XSS.

iv) CVE/CWE: CWE-444

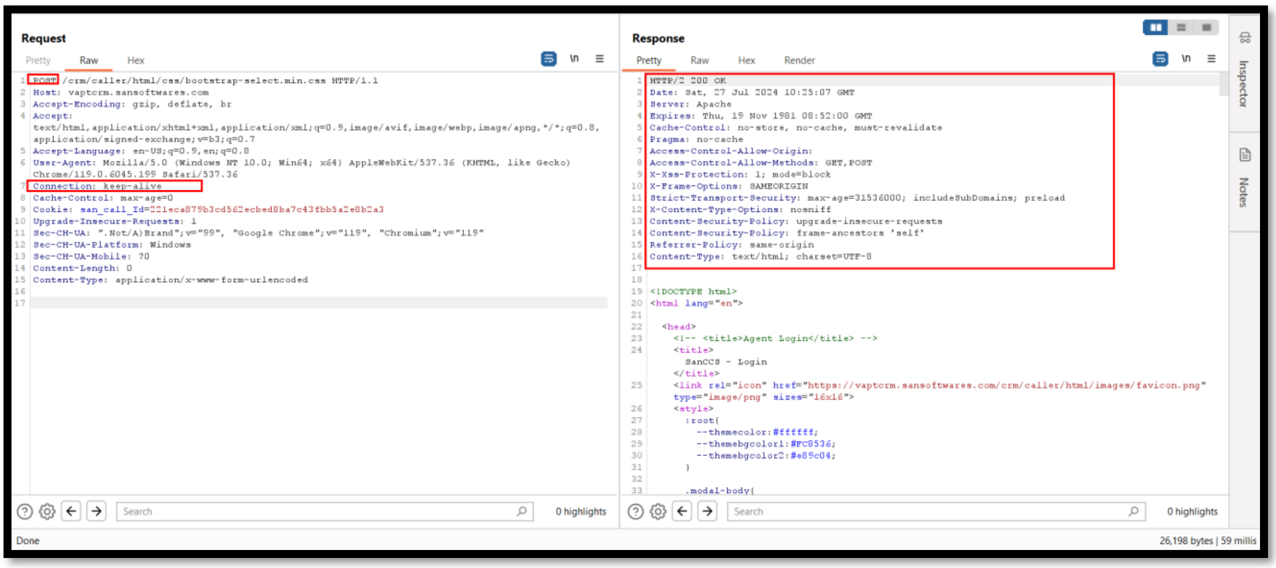
v) Severity: Medium

vi) Recommendation This vulnerability can be resolved by patching the server so that it either processes POST requests correctly or closes the connection after handling them. You could also disable connection reuse entirely, but this may reduce performance. You can also resolve this issue by enabling HTTP/2.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/444.html

ix) References to evidences / Proof of Concept:
Step#1: Send the request to repeater and send the request.
Step#2: Observed that the request is processed by the server successfully.



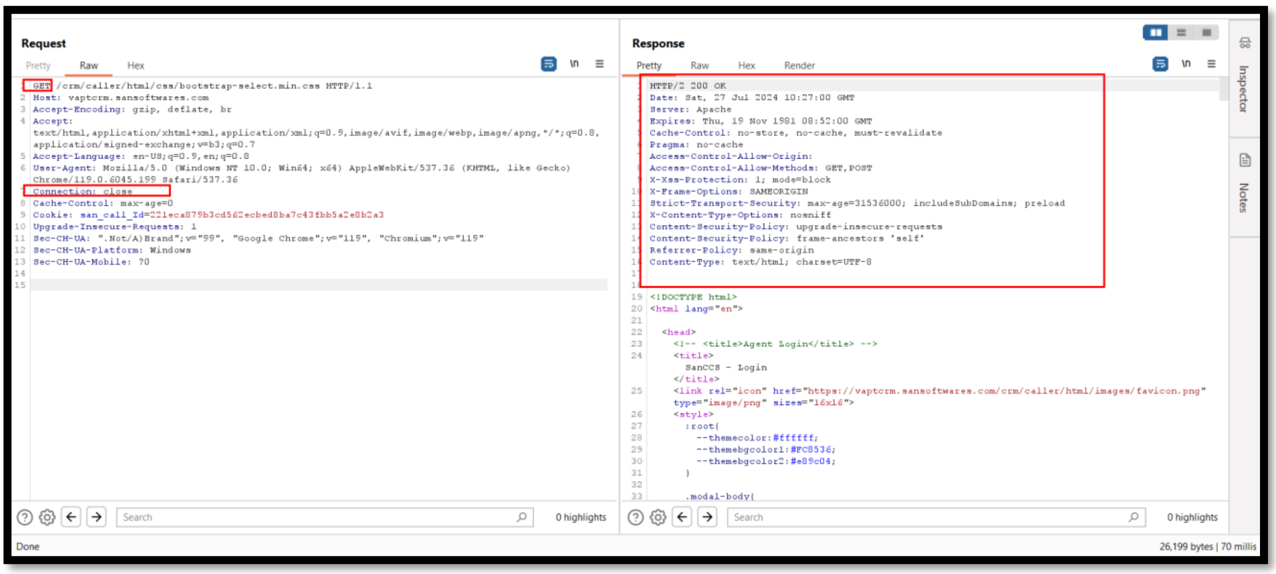
Request

```
POST /crm/caller/html/css/bootstrap-select.min.css HTTP/1.1
Host: vaptcrm.sansoftwares.com
Accept-Encoding: gzip, deflate, br
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.199 Safari/537.36
Connection: keep-alive
Cache-Control: max-age=0
Cookie: san_call_Id=221eca879b3cd562ecbed8ba7c43fbb5a2e8b2a3
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="119", "Chromium";v="119"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
```

Response

```
HTTP/2 200 OK
Date: Sat, 27 Jul 2024 10:25:07 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: GET,POST
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Content-Security-Policy: upgrade-insecure-requests
Content-Security-Policy: frame-ancestors 'self'
Referrer-Policy: same-origin
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://vaptcrm.sansoftwares.com/crm/caller/html/images/favicon.png"
    type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
```

Step#3: Now we add a second request to the end of the first request (HTTP smuggling) and send the request.
Step#4: Observe that the request is processed by the server again.



Request

```
GET /crm/caller/html/css/bootstrap-select.min.css HTTP/1.1
Host: vaptcrm.sansoftwares.com
Accept-Encoding: gzip, deflate, br
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.199 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: san_call_Id=221eca879b3cd562ecbed8ba7c43fbb5a2e8b2a3
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="119", "Chromium";v="119"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/2 200 OK
Date: Sat, 27 Jul 2024 10:27:00 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: GET,POST
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Content-Security-Policy: upgrade-insecure-requests
Content-Security-Policy: frame-ancestors 'self'
Referrer-Policy: same-origin
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

  <head>
    <!-- <title>Agent Login</title> -->
    <title>
      SanCCS - Login
    </title>
    <link rel="icon" href="https://vaptcrm.sansoftwares.com/crm/caller/html/images/favicon.png"
    type="image/png" sizes="16x16">
    <style>
      :root{
        --themecolor:#ffffff;
        --themebgcolor1:#FC8536;
        --themebgcolor2:#e89c04;
      }

      .modal-body{
```

Finding No. 19

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Not Using Password Aging.

iii) Detailed observation / Vulnerable point: Password History is not maintained in the application.

iv) CVE/CWE: CWE-262

v) Severity: Low

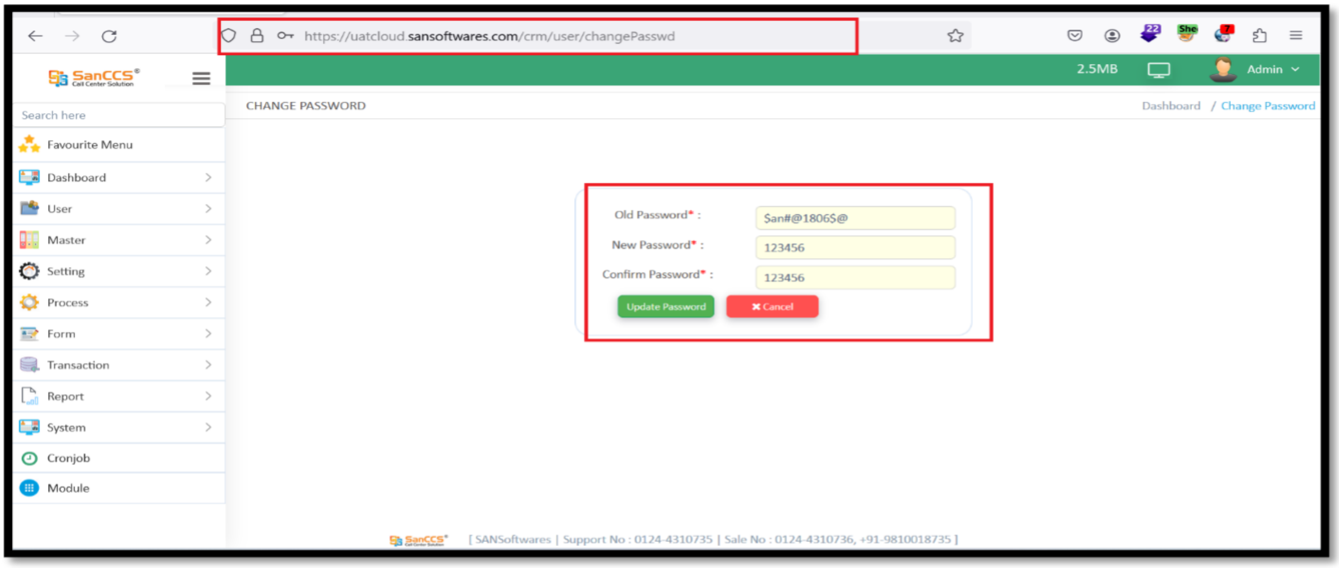
vi) Recommendation: Users should be prevented from reusing their current or previous 3 passwords. Password history should ideally be 3.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/262.html

ix) References to evidences / Proof of Concept:

Step#1: We are entering a detail for change the password of application according to given field. (Old pass: - $an#@1806$@ , new pass:- 123456 and con pass:- 123456).



https://uatcloud.sansoftwares.com/crm/user/changePasswd

CHANGE PASSWORD

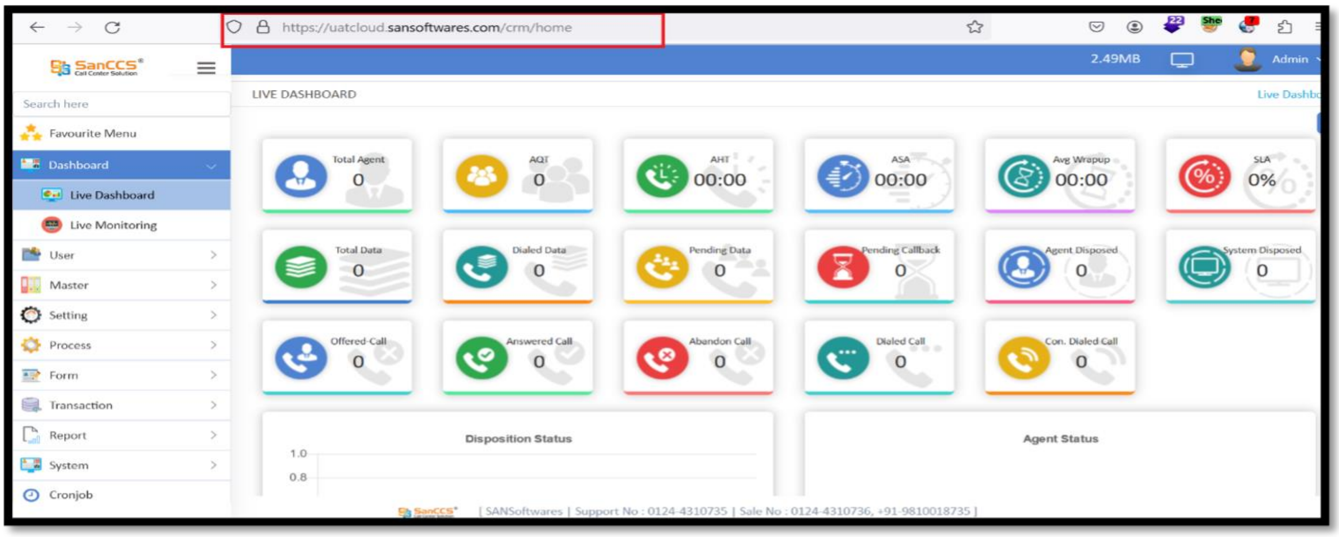
Old Password* : San#@1806$@

New Password* : 123456

Confirm Password* : 123456

SanCCS Call Center Solution
2.5MB
Admin
Dashboard / Change Password
Search here
Favourite Menu
Dashboard
User
Master
Setting
Process
Form
Transaction
Report
System
Cronjob
Module
Update Password
✖ Cancel
[SANSoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

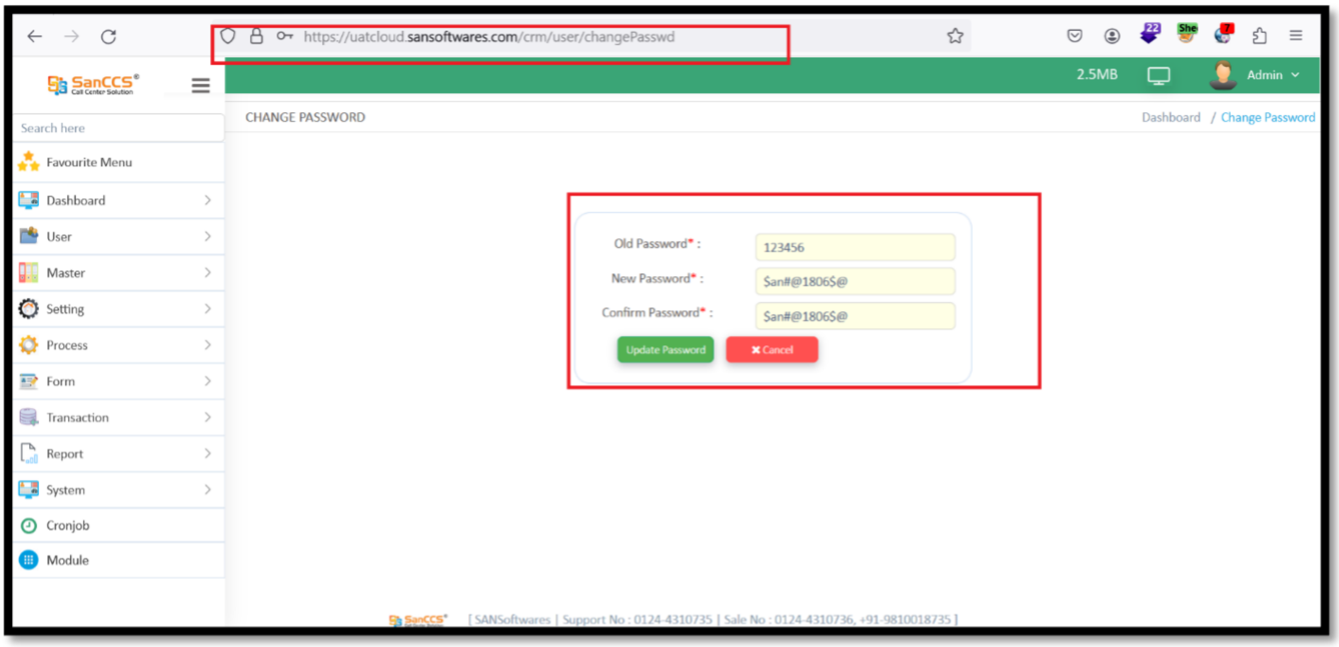
Step#2: We can see, password has been changed successfully.



https://uatcloud.sansoftwares.com/crm/home

LIVE DASHBOARD

Step#3: We are entering again detail for change the password of application according to given field. (Old pass: - 123456, new pass: - $an#@1806$@ and con pass: - $an#@1806$@).



https://uatcloud.sansoftwares.com/crm/user/changePasswd

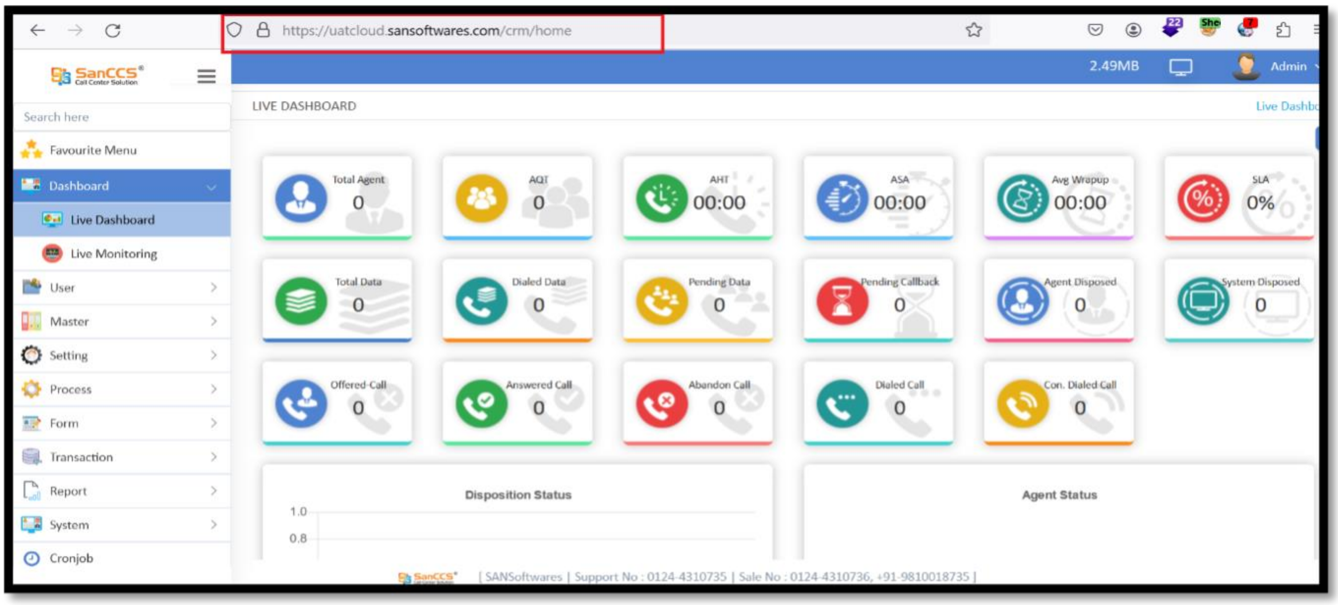
CHANGE PASSWORD

Old Password* : 123456

New Password* : San#@1806$@

Confirm Password* : San#@1806$@

Step#4: We can see, password has been changed successfully.



https://uatcloud.sansoftwares.com/crm/home

LIVE DASHBOARD

Total Agent 0	AQT 0	AHT 00:00	ASA 00:00	Avg Wrapup 00:00	SLA 0%
Total Data 0	Dialed Data 0	Pending Data 0	Pending Callback 0	Agent Disposed 0	System Disposed 0
Offered Call 0	Answered Call 0	Abandon Call 0	Dialed Call 0	Con. Dialed Call 0	

Finding No. 20

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Weak Password Requirements

iii) Detailed observation / Vulnerability point: Password Complexity is not implemented properly in the application.

iv) CVE/CWE: CWE-521

v) Severity: Low

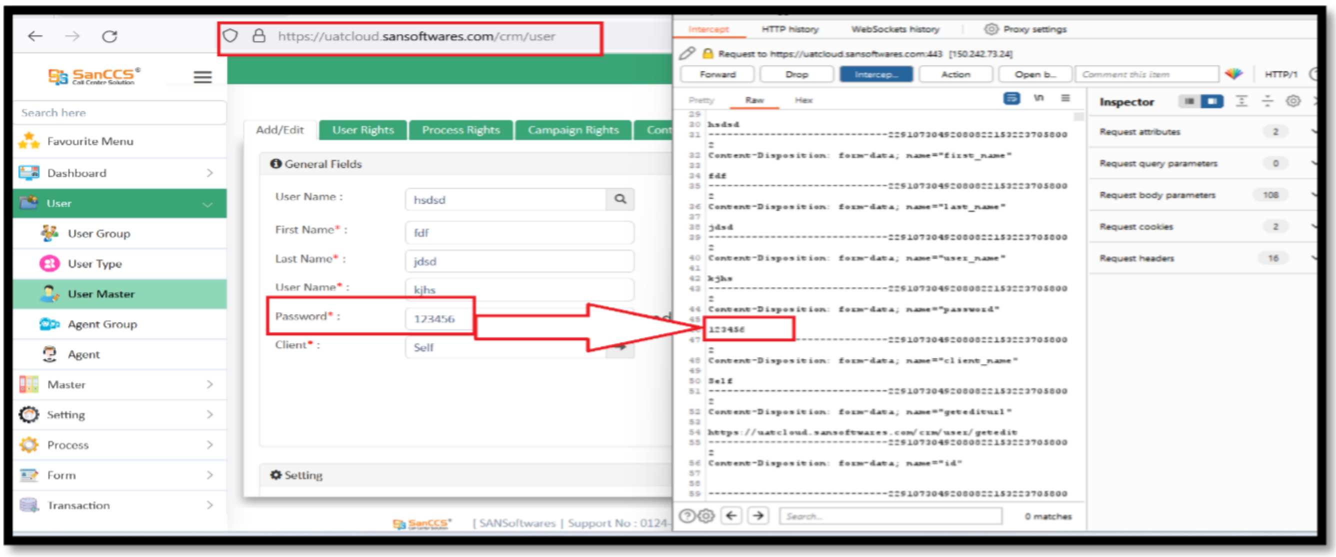
vi) Recommendation Password should be complex.

vii) Current Status: Closed

viii) Reference https://cwe.mitre.org/data/definitions/521.html

ix) References to evidences / Proof of Concept:

Step#1: Login an application and fill the required details and then capture the request, we can see the password complexity is not used.



https://uatcloud.sansoftwares.com/crm/user

Request to https://uatcloud.sansoftwares.com:443 [150.242.73.24]

User Name : hsdsd

First Name* : fdf

Last Name* : jdsd

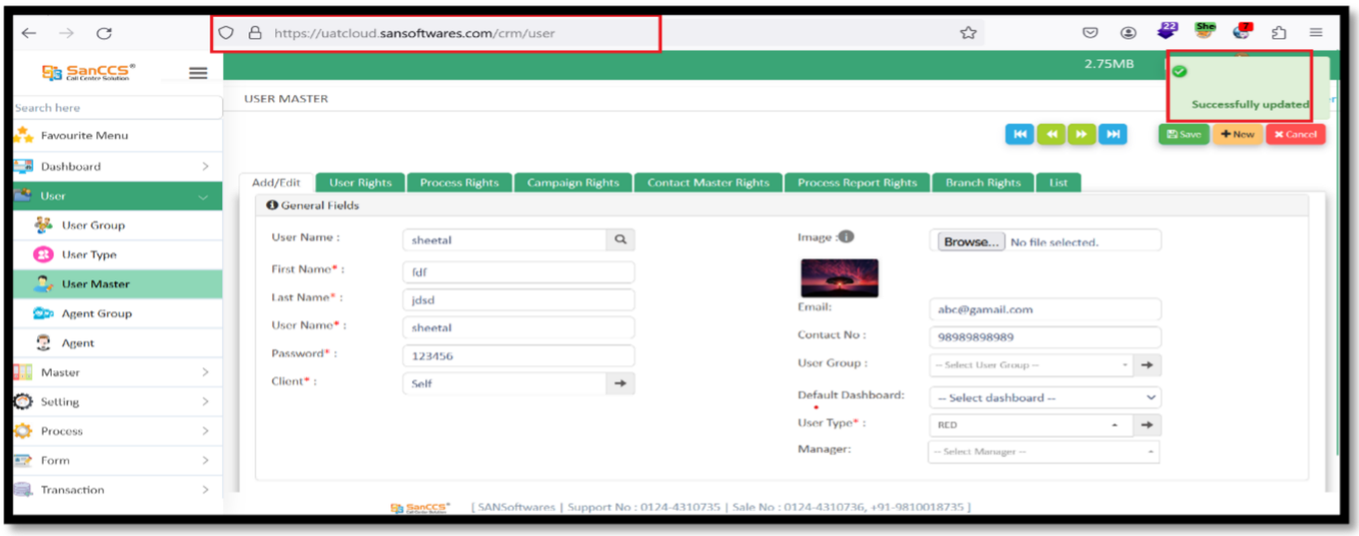
User Name* : kjhs

Password* : 123456

Client* : Self

```
hsdsd
-----------------------------225107304520808221532237058002
Content-Disposition: form-data; name="first_name"

fdf
-----------------------------225107304520808221532237058002
Content-Disposition: form-data; name="last_name"

jdsd
-----------------------------225107304520808221532237058002
Content-Disposition: form-data; name="user_name"

kjhs
-----------------------------225107304520808221532237058002
Content-Disposition: form-data; name="password"

123456
-----------------------------225107304520808221532237058002
Content-Disposition: form-data; name="client_name"

Self
-----------------------------225107304520808221532237058002
Content-Disposition: form-data; name="getediturl"

https://uatcloud.sansoftwares.com/crm/user/getedit
-----------------------------225107304520808221532237058002
Content-Disposition: form-data; name="id"


-----------------------------225107304520808221532237058002
```

Step#2: As we can, we are using simple password and it is updated successfully. So, password complexity is not maintaining in this application.



https://uatcloud.sansoftwares.com/crm/user

Successfully updated

USER MASTER

User Name : sheetal

First Name* : fdf

Last Name* : jdsd

User Name* : sheetal

Password* : 123456

Client* : Self

Email: abc@gamail.com

Contact No : 98989898989

User Group : -- Select User Group --

Default Dashboard: -- Select dashboard --

User Type* : RED

Manager: -- Select Manager --

Image : Browse... No file selected.

Finding No. 21

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Excessive Attack Surface.

iii) **Detailed observation / Vulnerable point:** Multiple Ports are open in the application.

iv) **CVE/CWE:** CWE-1125

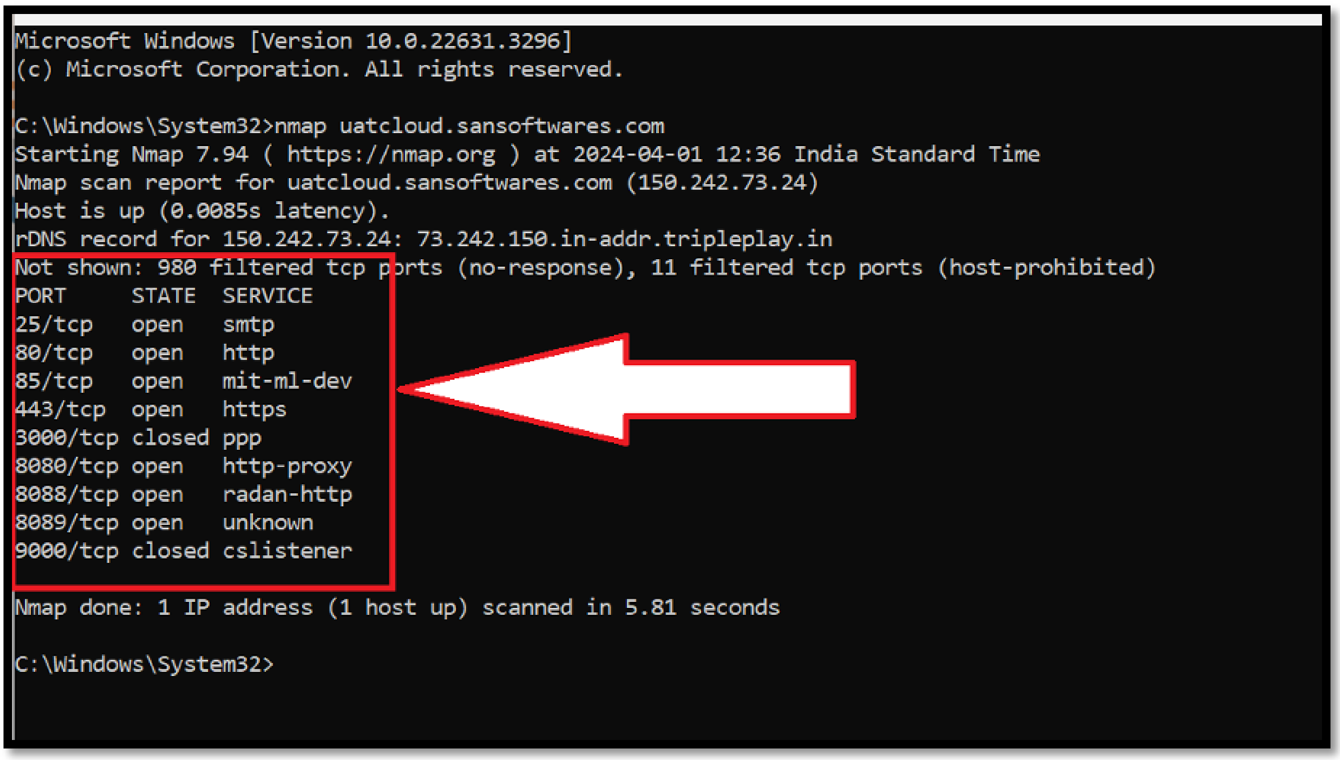
v) **Severity:** Low

vi) **Recommendation:** Only port 443 must be open in the application, all other remaining ports must be closed.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/1125.html,
https://blog.netwrix.com/2022/08/16/open-network-ports/

ix) **References to evidences / Proof of Concept:**
Step#1: Using Nmap and scanning the application host, we can gather information about the hosted IP as well as the ports open on it. Here we can see multiple ports open. This increases the attack surface area.



```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nmap uatcloud.sansoftwares.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-01 12:36 India Standard Time
Nmap scan report for uatcloud.sansoftwares.com (150.242.73.24)
Host is up (0.0085s latency).
rDNS record for 150.242.73.24: 73.242.150.in-addr.tripleplay.in
Not shown: 980 filtered tcp ports (no-response), 11 filtered tcp ports (host-prohibited)
PORT      STATE  SERVICE
25/tcp    open   smtp
80/tcp    open   http
85/tcp    open   mit-ml-dev
443/tcp   open   https
3000/tcp closed ppp
8080/tcp open   http-proxy
8088/tcp open   radan-http
8089/tcp open   unknown
9000/tcp closed cslistener

Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds

C:\Windows\System32>
```

Finding No. 22

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Improper Input Validation.

iii) Detailed observation / Vulnerable point: Input validations not implemented properly in the application.

iv) CVE/CWE: CWE-20

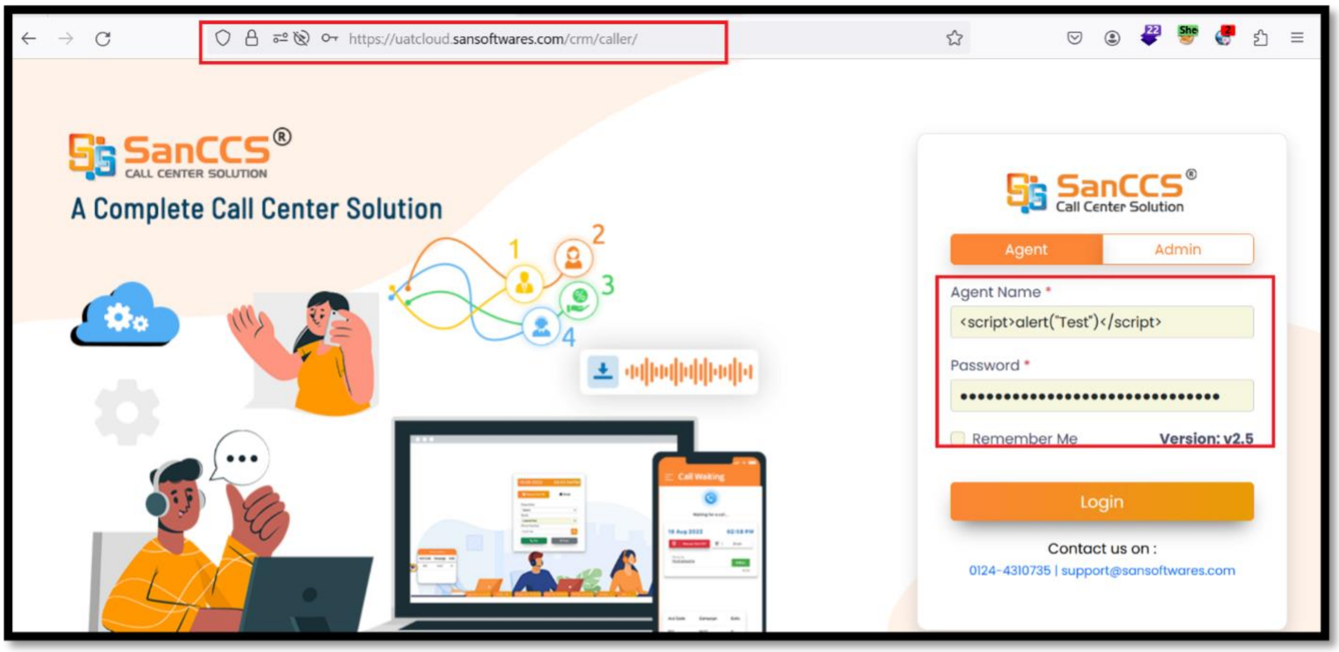
v) Severity: Low

vi) Recommendation: Input validations should be properly implemented in the application.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/20.html

ix) References to evidences / Proof of Concept:
Step#1: We can see in below screenshot, there is no input validation implemented.



https://uatcloud.sansoftwares.com/crm/caller/

Agent Name * <script>alert("Test")</script>

Password * ••••••••••••••••••••••••••••••••

Version: v2.5

Contact us on : 0124-4310735 | support@sansoftwares.com

Finding No. 23

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Improper Resolution of Path Equivalence

iii) Detailed observation / Vulnerable point: Path is set to default root i.e. '/'.

iv) CVE/CWE: CWE-41

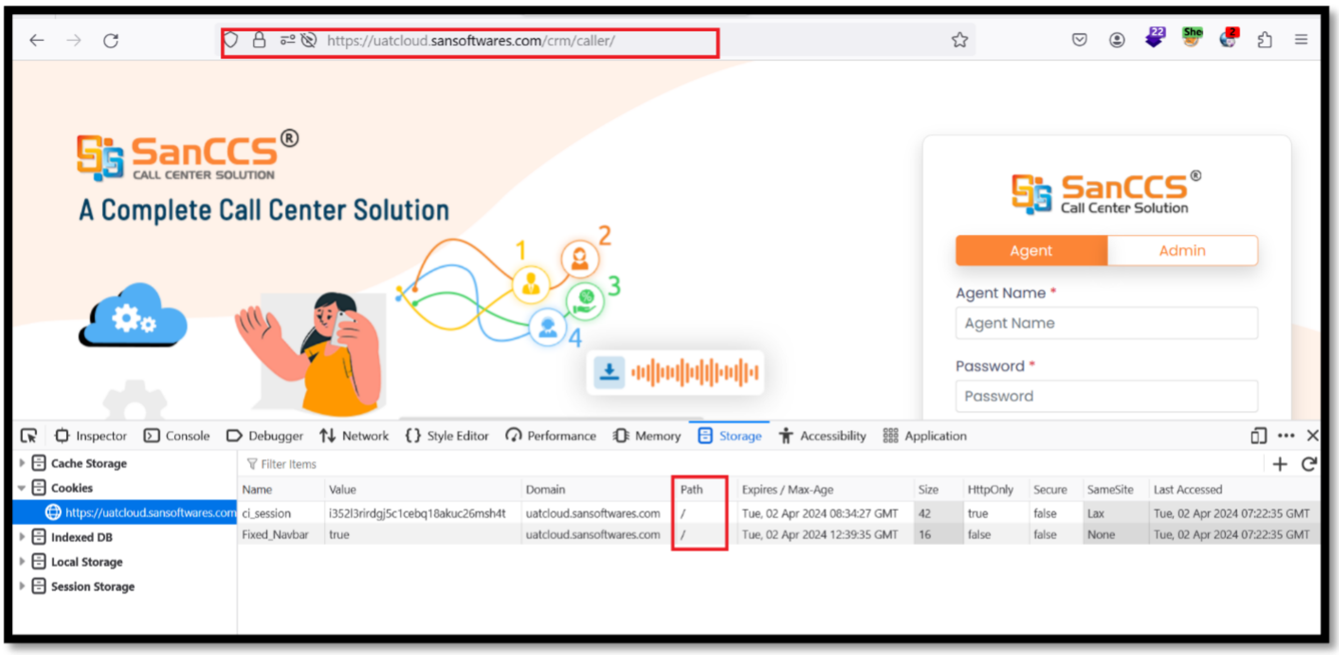
v) Severity: Low

vi) Recommendation: Verify that the path attribute, just as the Domain attribute, has not been set too loosely. Even if the Domain attribute has been configured as tight as possible, if the path is set to the root directory "/" then it can be vulnerable to less secure applications on the same server.

vii) Current Closed: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/41.html

ix) References to evidences / Proof of Concept:
Step#1: Using the inspect element and navigating to Storage > Cookies, we can easily see that the path for the cookies has been set to root.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ci_session	i352l3rirdgj5c1cebq18akuc26msh4t	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 08:34:27 GMT	42	true	false	Lax	Tue, 02 Apr 2024 07:22:35 GMT
Fixed_Navbar	true	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 12:39:35 GMT	16	false	false	None	Tue, 02 Apr 2024 07:22:35 GMT

Finding No. 24

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

iii) **Detailed observation / Vulnerable point**: Cookie is displaying without SECURE flag.

iv) **CVE/CWE:** CWE-614

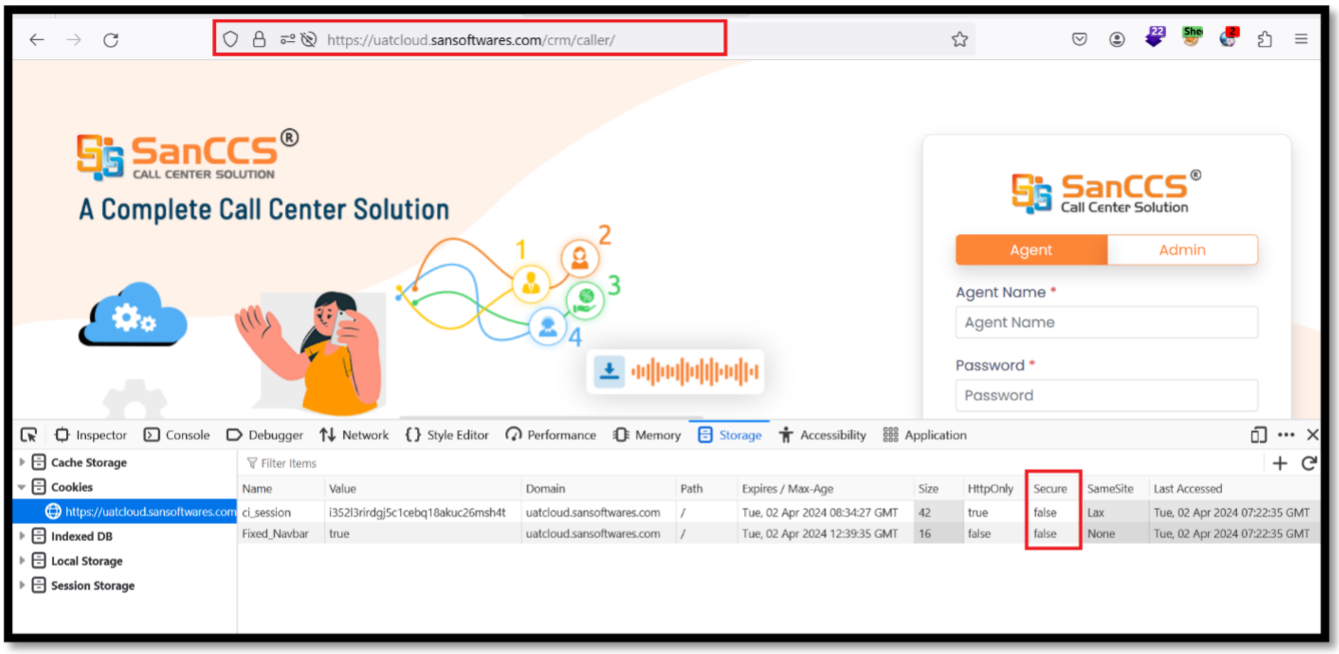
v) **Severity:** Low

vi) **Recommendation** Secure flag should be "True" in website's configuration file.

vii) **Current Status:** Closed

viii) **Reference** https://cwe.mitre.org/data/definitions/614.html

ix) **References to evidences / Proof of Concept:**
Step#1: We can see cookie is set to false for secure flag.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ci_session	i352l3rirdgj5c1cebq18akuc26msh4t	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 08:34:27 GMT	42	true	false	Lax	Tue, 02 Apr 2024 07:22:35 GMT
Fixed_Navbar	true	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 12:39:35 GMT	16	false	false	None	Tue, 02 Apr 2024 07:22:35 GMT

Finding No. 25

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Sensitive Cookie Without 'HTTPonly' Flag.

iii) Detailed observation / Vulnerable point: HTTPonly flag is not set properly in the application.

iv) CVE/CWE: CWE-1004

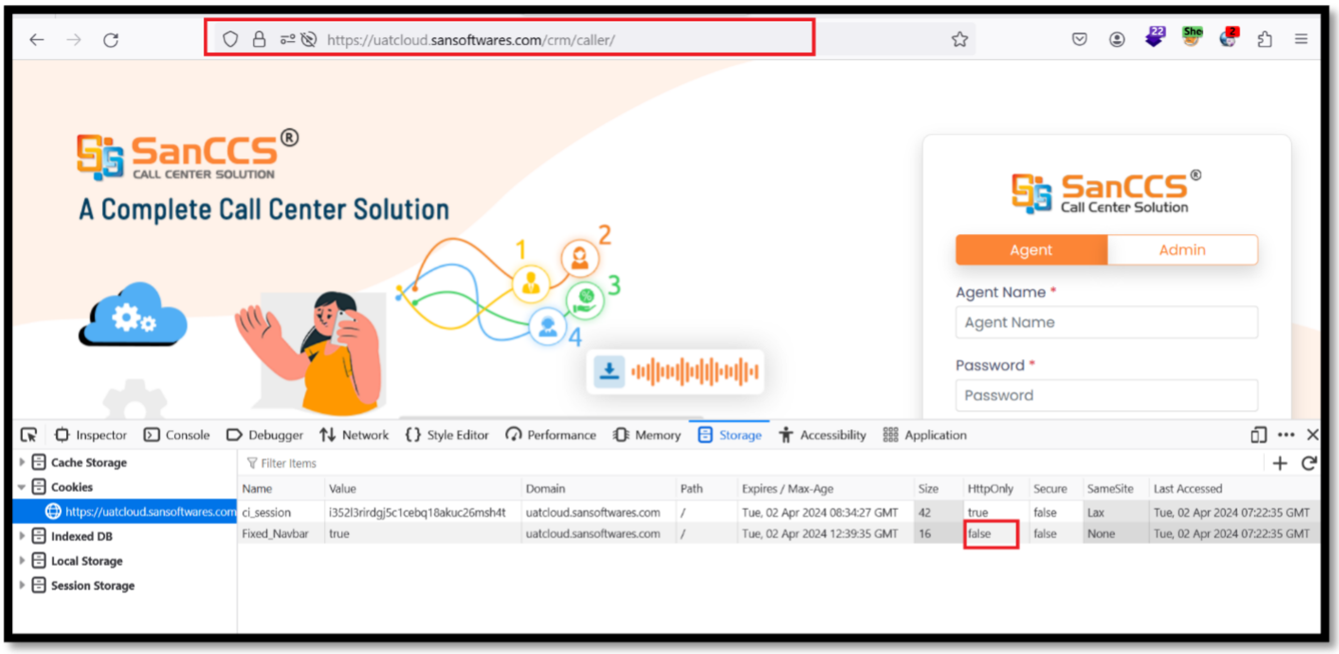
v) Severity: Low

vi) Recommendation: HTTPonly flag should be set to "True" in website's configuration file.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/1004.html.

ix) References to evidences / Proof of Concept:
Step#1: As we can see in given screenshot httponly flag is set to false in this application.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ci_session	i352l3rirdgj5c1cebq18akuc26msh4t	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 08:34:27 GMT	42	true	false	Lax	Tue, 02 Apr 2024 07:22:35 GMT
Fixed_Navbar	true	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 12:39:35 GMT	16	false	false	None	Tue, 02 Apr 2024 07:22:35 GMT

Finding No. 26

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Sensitive Cookie with Improper Same Site Attribute.

iii) Detailed observation / Vulnerable point: Same Site attribute set to none.

iv) CVE/CWE: CWE-1275

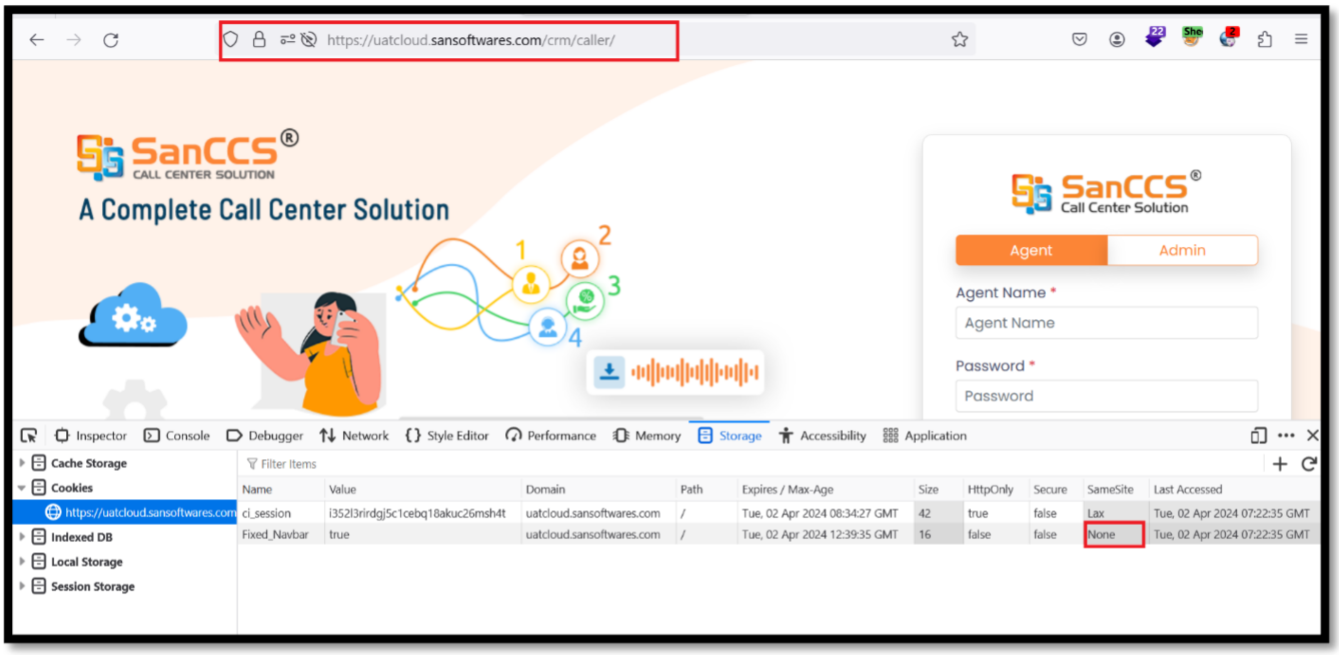
v) Severity: Low

vi) Recommendation: Same Site attribute should be set to “LAX or STRICT”.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/1275.html,
https://probely.com/vulnerabilities/cookie-with-samesite-attribute-set-to-none

ix) References to evidences / Proof of Concept:
Step#1: As we can see in given screenshot Same site attribute is not set in this applcation.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ci_session	i352l3rirdgj5c1cebq18akuc26msh4t	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 08:34:27 GMT	42	true	false	Lax	Tue, 02 Apr 2024 07:22:35 GMT
Fixed_Navbar	true	uatcloud.sansoftwares.com	/	Tue, 02 Apr 2024 12:39:35 GMT	16	false	false	None	Tue, 02 Apr 2024 07:22:35 GMT

Finding No. 27

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Unverified Password Change

iii) **Detailed observation / Vulnerable point:** There is no forgot password option available for the user.

iv) **CVE/CWE:** CWE-620

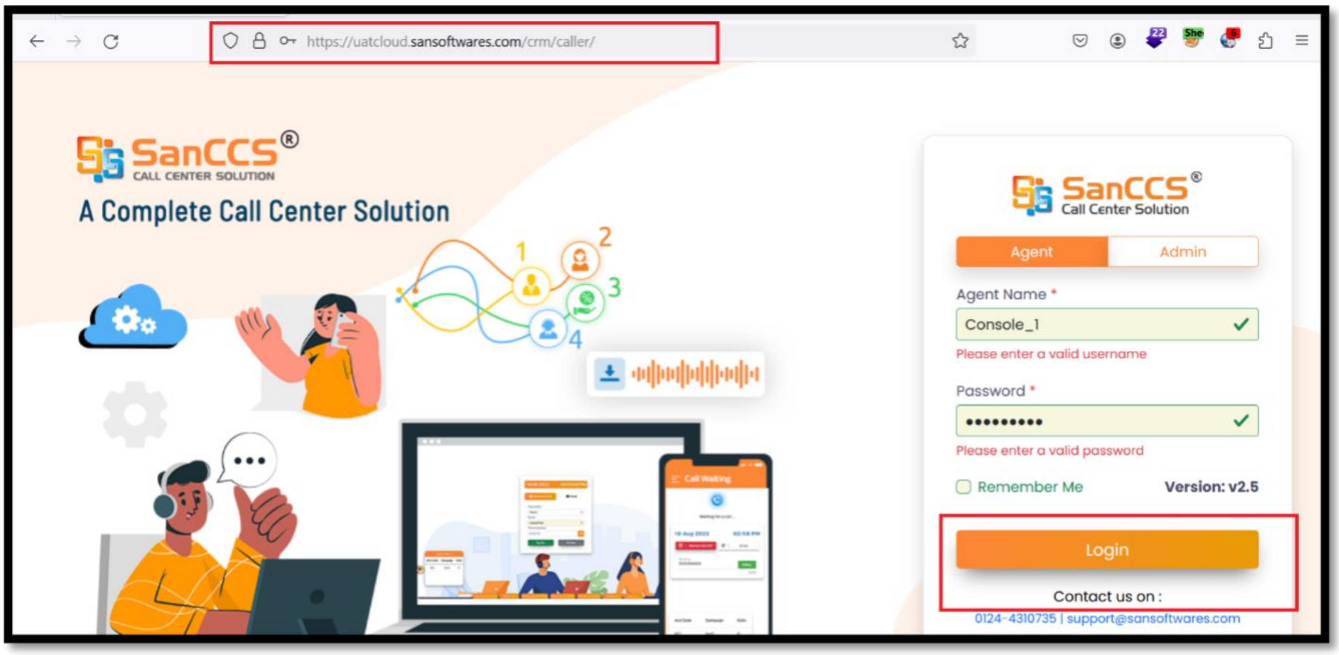
v) **Severity:** Low

vi) **Recommendation:** Users may be required to retrieve their password. Users should be provided with a “forgot password” option through which user will retrieve their password whenever required. Forgot password should be enabled with the users email address. There are following conditions that should be met in the forget password function:
1. A reset link should be sent to the user registered email address instead of password directly.
2. Reset Password link should expire in 24 hours.
3. Reset Password link should not be reused again once the link is used for resetting password.
4. In the Reset Password page, Mandatory fields i.e. new password, Confirm Password and CAPTCHA field must present and should be validated at the client end. Server end validations are also mandatory.
However, if the password retrieval is internal in the application, then it is recommended to implement a hyperlink on login page resulting to a static page containing a message. “Please contact your site administrator at mail_id[at]domain[dot]com”. Please note that the email address in the message should not be a hyperlink.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/620.html

ix) **References to evidences / Proof of Concept:**
Step#1: As we can see, Forgot password module is not available for change the password.



https://uatcloud.sansoftwares.com/crm/caller/

SanCCS® CALL CENTER SOLUTION

A Complete Call Center Solution

SanCCS® Call Center Solution

Agent | Admin

Agent Name *
Console_1
Please enter a valid username

Password *
•••••••••
Please enter a valid password

□ Remember Me Version: v2.5

Login

Contact us on :
0124-4310735 | support@sansoftwares.com

Finding No. 28

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application

ii) **Observation/ Vulnerability title:** Insufficient Session Expiration

iii) **Detailed observation /vulnerable point:** Session termination due to user inactivity is not properly configured in the application.

iv) **CVE/CWE:** CWE-613

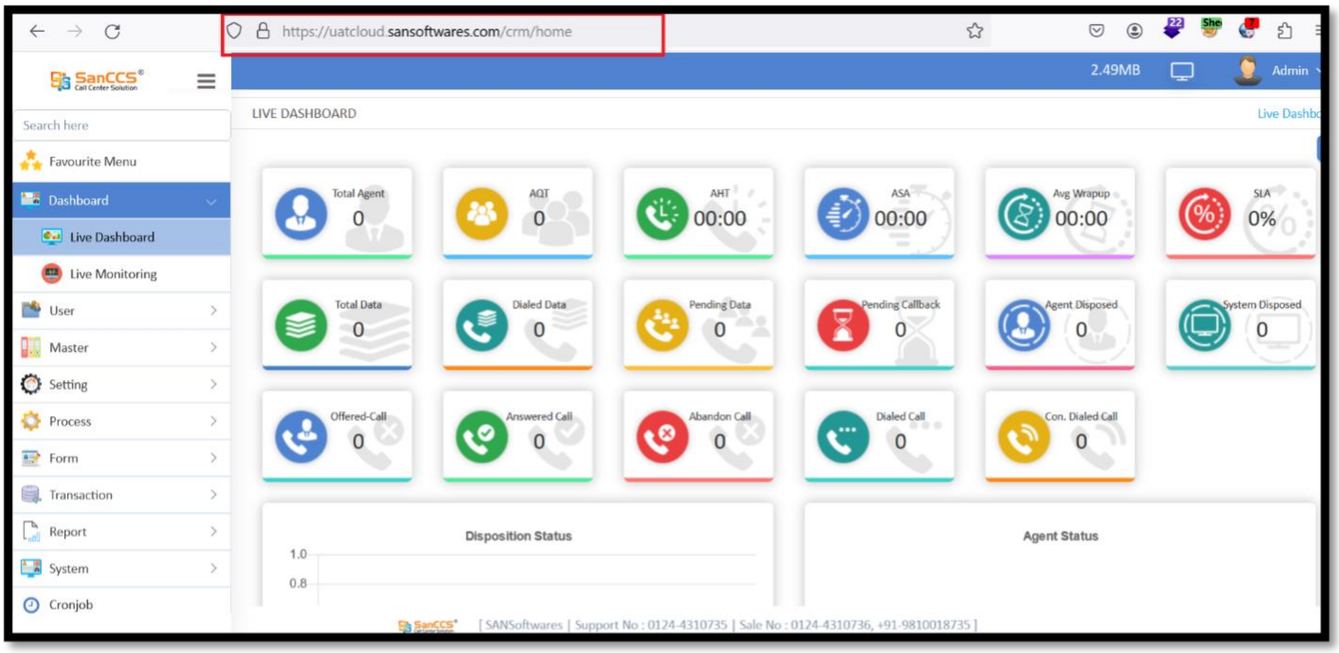
v) **Severity:** Low

vi) **Recommendation:** In case of session termination by the application due to inactivity of the user within his session for more than 15 minutes, application must terminate session completely and login page must be loaded in the main window instead of in a child frame of the window.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/613.html

ix) **References to evidences / Proof of Concept:**
Step#1: Application seesion is not terminated after 15 min. inactivity of application.



Finding No. 29

i) IP/URL/Application: CALL CENTER SOLUTION Web Application

ii) Observation/ Vulnerability title: Improper Control of Interaction Frequency.

iii) Detailed observation /vulnerable point: Email spamming is possible in the application.

iv) CVE/CWE: CWE-799

v) Severity: Low

vi) Recommendation: The application should properly customize the email addresses while posting on the website as:

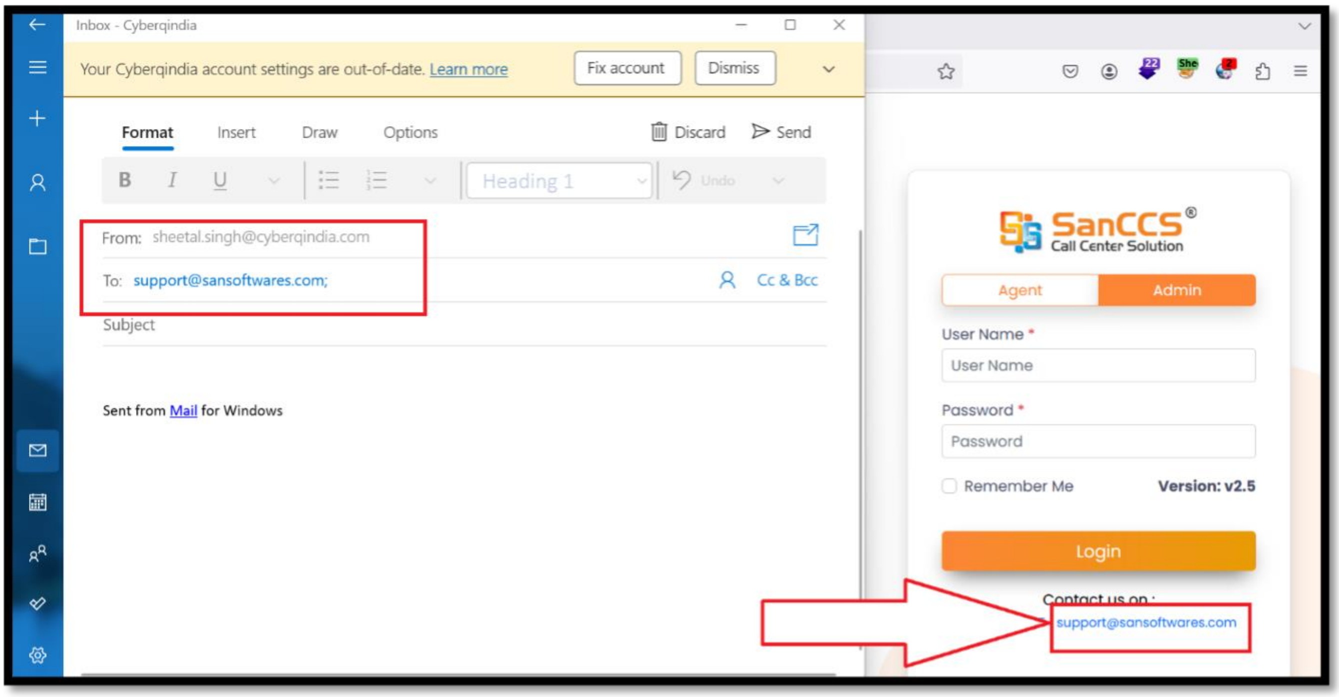
1. Email addresses should be posted as an image not as a hyperlink. Alternatively, instead of @symbol, [at] should be used. Similarly, the dot character (.) should be replaced by [dot]. So abc@nic.in should be written as abc[at]nic[dot]in.
2. High privilege email addresses should not be posted on the website.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/799.html

ix) References to evidences / Proof of Concept:

Step#1: Go to application and click on the hyperlinked mail then these are open in a mail box.



From: sheetal.singh@cyberqindia.com

To: support@sansoftwares.com;

Subject

Sent from Mail for Windows

Finding No. 30

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Exposure of Sensitive Information to an Unauthorized Actor.

iii) **Detailed observation / Vulnerable point**: Autofill is enabled in forms.

iv) **CVE/CWE:** CWE-200

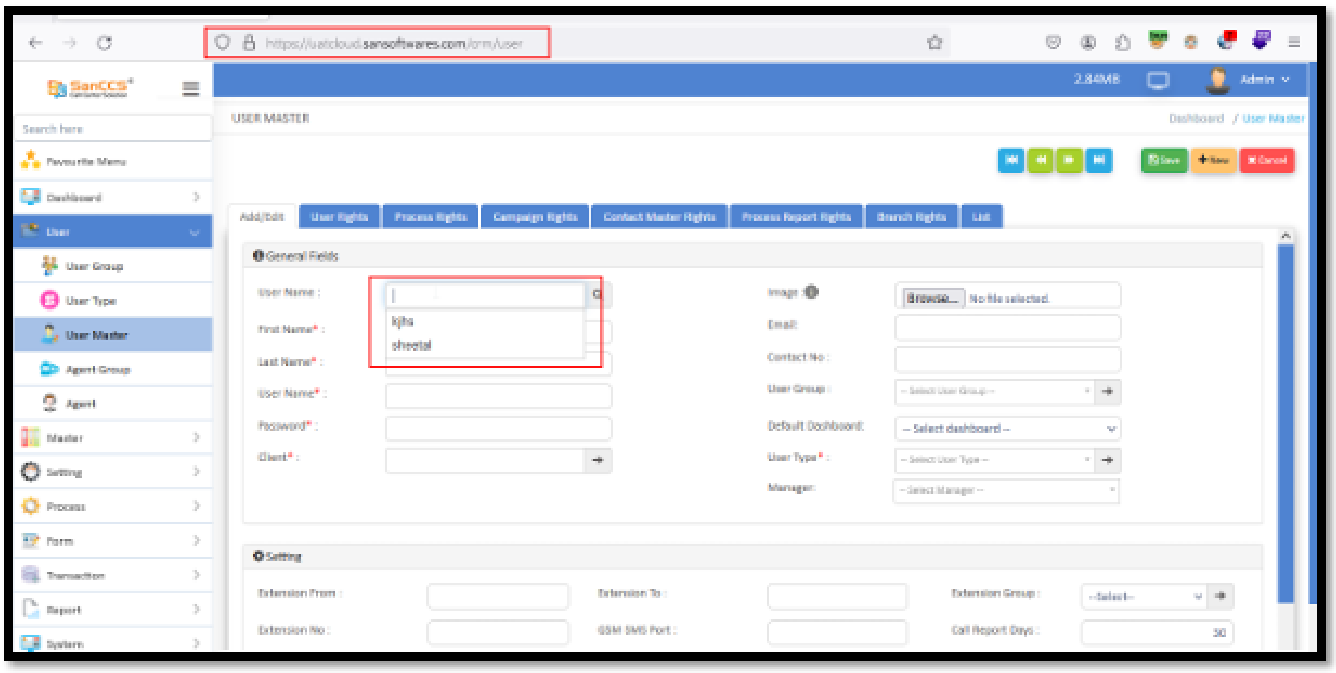
v) **Severity:** Low

vi) **Recommendation** Application should not have the option to remember information entered by the user as this may cause unavailability of services to valid users. AutoComplete option should be turned off by the application so as to override any settings by the user from the browser.

vii) **Current Status:** Closed

viii) **Reference:** https://portswigger.net/kb/issues/00500800_password-field-with-autocomplete-enabled
https://cwe.mitre.org/data/definitions/200.html

ix) **References to evidences / Proof of Concept:**
Step#1: We can see autocomplete is not defined properly.



https://uatcloud.sansoftwares.com/crm/user

USER MASTER

General Fields

User Name : |
kjhs
sheetal

First Name* :
Last Name* :
User Name* :
Password* :
Client* :
Image: Browse... No file selected.
Email:
Contact No :
User Group : -- Select User Group --
Default Dashboard: -- Select dashboard --
User Type* : -- Select User Type --
Manager: -- Select Manager --

Setting

Extension From :
Extension To :
Extension Group : --Select--
Extension No :
GSM SMS Port :
Call Report Days : 30

Finding No. 31

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: Selection of Less-Secure Algorithm During Negotiation.

iii) Detailed observation / Vulnerable point: Old TLS versions are still being used in the application.

iv) CVE/CWE: CWE-757

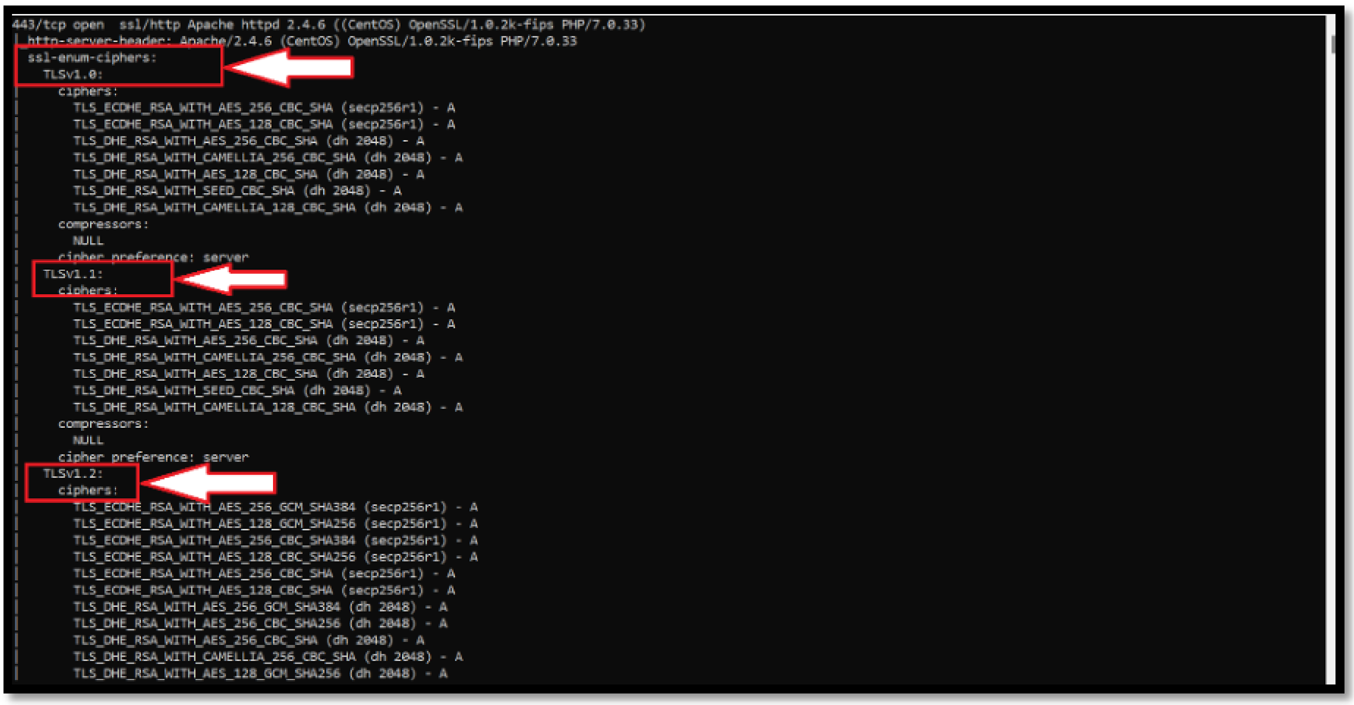
v) Severity: Low

vi) Recommendation TLS v1.2 or higher should be used. All other TLS versions should be removed.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/757.html

ix) References to evidences / Proof of Concept:
Step#1: Multiple TLS version is use in this application.



```
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
```

Finding No. 32

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Selection of Less-Secure Algorithm During Negotiation.

iii) **Detailed observation / Vulnerable point**: The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **xhr.open** application.

iv) **CVE/CWE:** CWE-601

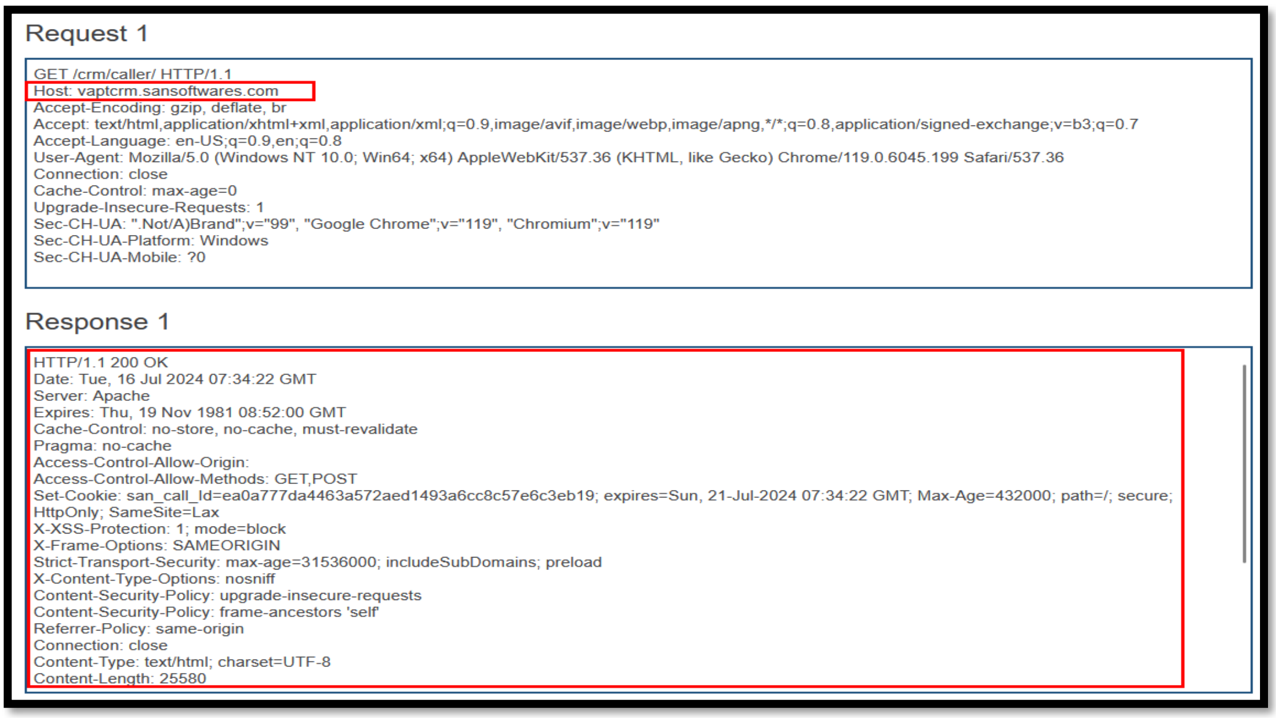
v) **Severity:** Low

vi) **Recommendation** The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.

vii) **Current Status:** Closed

viii) **Reference**: https://cwe.mitre.org/data/definitions/757.html

ix) **References to evidences / Proof of Concept:**
Step#1: We can see DOM-Based Open redirection is possible in the application.



Request 1

```
GET /crm/caller/ HTTP/1.1
Host: vaptcrm.sansoftwares.com
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="119", "Chromium";v="119"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Tue, 16 Jul 2024 07:34:22 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: GET,POST
Set-Cookie: san_call_Id=ea0a777da4463a572aed1493a6cc8c57e6c3eb19; expires=Sun, 21-Jul-2024 07:34:22 GMT; Max-Age=432000; path=/; secure;
HttpOnly; SameSite=Lax
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Content-Security-Policy: upgrade-insecure-requests
Content-Security-Policy: frame-ancestors 'self'
Referrer-Policy: same-origin
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 25580
```

Finding No. 33

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Missing Password Field Masking

iii) **Detailed observation / Vulnerable point:** OTP masking is not implemented in the application.

iv) **CVE/CWE:** CWE-549

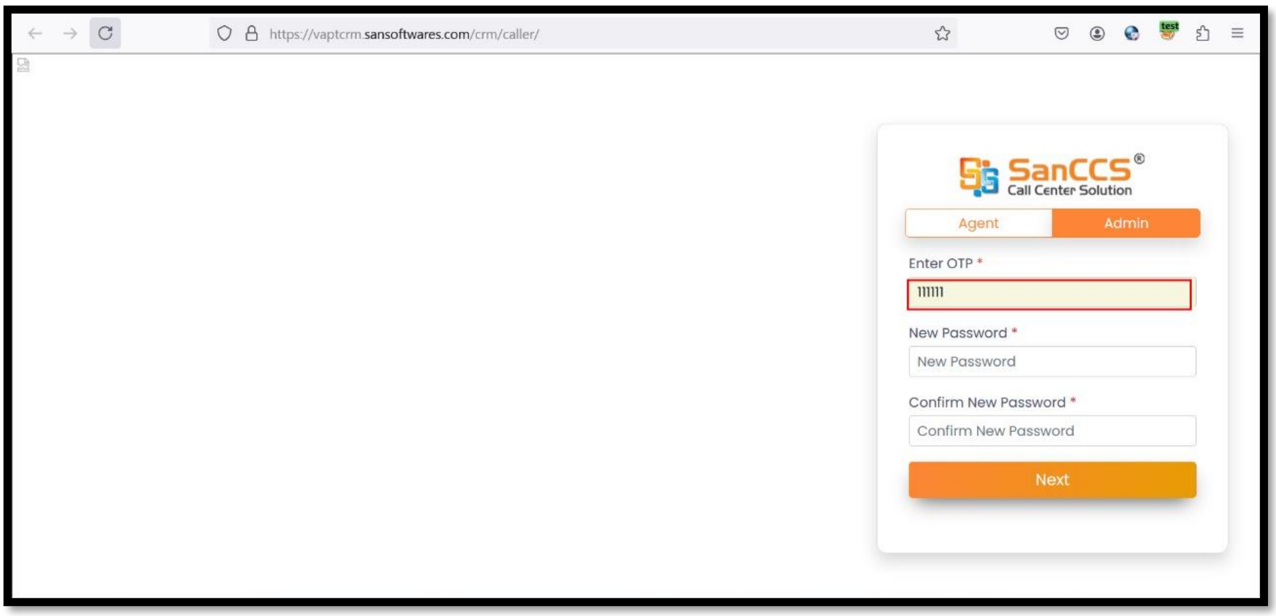
v) **Severity:** Low

vi) **Recommendation:** OTP should be masked and should not be viewable in clear text to end user or an option should be provided to unmask, if needed.

vii) **Current Status:** Closed

viii) **Reference:** https://cwe.mitre.org/data/definitions/549.html

ix) **References to evidences / Proof of Concept:**
Step#1: Open the URL https://vaptcrm.sansoftwares.com/crm/caller/ and fill in the otp.
Step#2: Enter the OTP and observe that the OTP is not masked.



https://vaptcrm.sansoftwares.com/crm/caller/

Enter OTP *: 111111

New Password *: New Password

Confirm New Password *: Confirm New Password

Finding No. 34

i) IP/URL/Application: CALL CENTER SOLUTION Web Application.

ii) Observation/ Vulnerability title: unencrypted connections

iii) Detailed observation / Vulnerable point: Cleartext submission of password.

iv) CVE/CWE: CWE-549

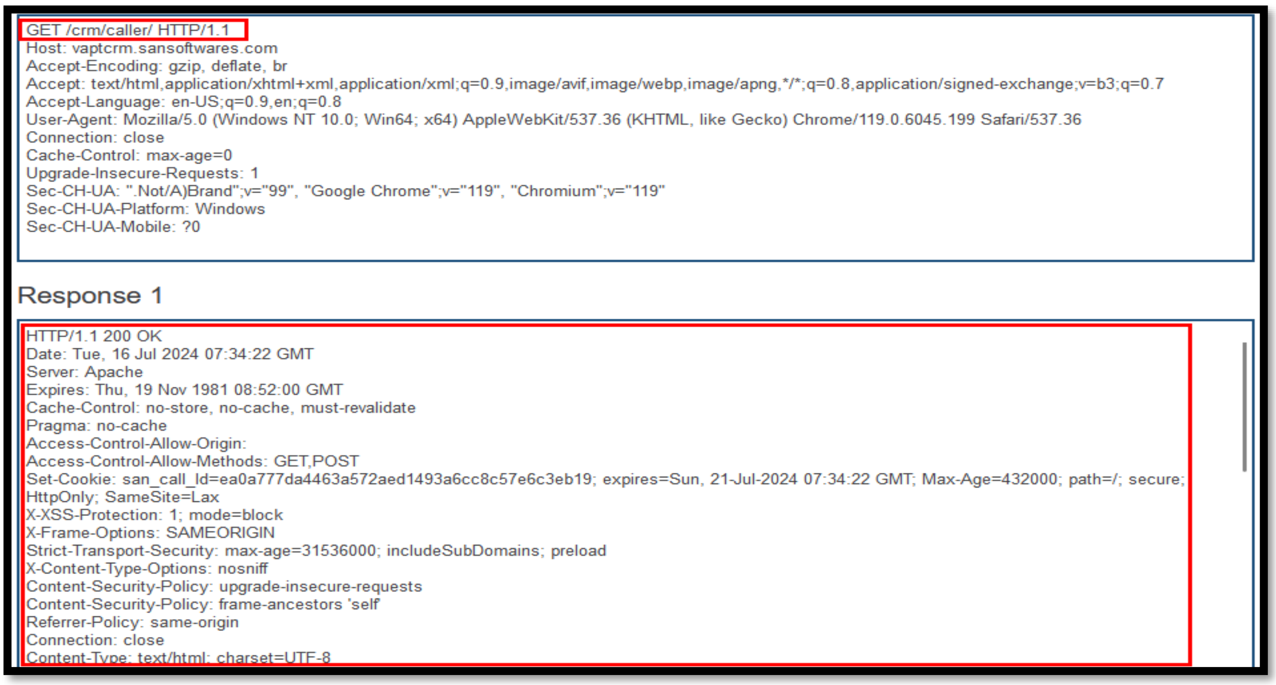
v) Severity: Low

vi) Recommendation: Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.

vii) Current Status: Closed

viii) Reference: https://cwe.mitre.org/data/definitions/549.html

ix) References to evidences / Proof of Concept:
Step#1: We can see that unencrypted connection over the network.



```
GET /crm/caller/ HTTP/1.1
Host: vaptcrm.sansoftwares.com
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="119", "Chromium";v="119"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Tue, 16 Jul 2024 07:34:22 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: GET,POST
Set-Cookie: san_call_Id=ea0a777da4463a572aed1493a6cc8c57e6c3eb19; expires=Sun, 21-Jul-2024 07:34:22 GMT; Max-Age=432000; path=/; secure;
HttpOnly; SameSite=Lax
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Content-Security-Policy: upgrade-insecure-requests
Content-Security-Policy: frame-ancestors 'self'
Referrer-Policy: same-origin
Connection: close
Content-Type: text/html; charset=UTF-8
```

Finding No. 35

i) **IP/URL/Application:** CALL CENTER SOLUTION Web Application.

ii) **Observation/ Vulnerability title:** Insufficient Logging.

iii) **Detailed observation / Vulnerable point**: The application does not maintain audit trail properly where all user activities must be logged. In case a malicious user tries to attack the application; the application will not be able to trace the attacker.

iv) **CVE/CWE:** CWE-778

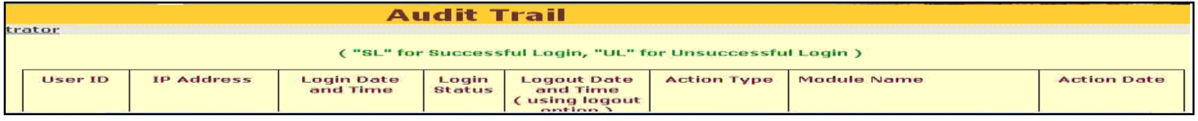
v) **Severity:** Observation

vi) **Recommendation**: An Audit trail should be incorporated in the application admin module, where all user activities have to be logged. Following points should be considered: Audits are to be generated at the time of resource access and by the same routines accessing the resource

- Information to be logged including the following: IP of the originating client, Date, Time, username if any in addition to other details to be logged in the web server.
- These IP, date, time, session details, user details (NO password), referrer, process id to be logged in application logs.
- To create audit logs use auto numbering so that every logged entry has a log number, which is not editable. Then if one audit entry is deleted a gap in the numbering sequence will appear.
- Log entries are to be hashed/signed so that changes to audit log can be detected.

Audit trails to answer the following:

- Logging of Authentication Process. Success and failed attempts.
- Logging Authentication details and changes.
- Software error and failures logged
- Should not be possible to retrieve confidential authentication information from these logs (including passwords)
- Is it possible to uniquely identify both client host and user from these logs?
- What level of information is logged by the application (read/write access, modification data, and copy/paste data)?
- Are log files time sequential and can they positively identify the time of action. The screenshot for recommended audit trail is given below.



Audit Trail

trator

("SL" for Successful Login, "UL" for Unsuccessful Login)

User ID	IP Address	Login Date and Time	Login Status	Logout Date and Time (using logout option)	Action Type	Module Name	Action Date

vii) **Current Status:** Closed

viii) **Reference** https://cwe.mitre.org/data/definitions/778.html

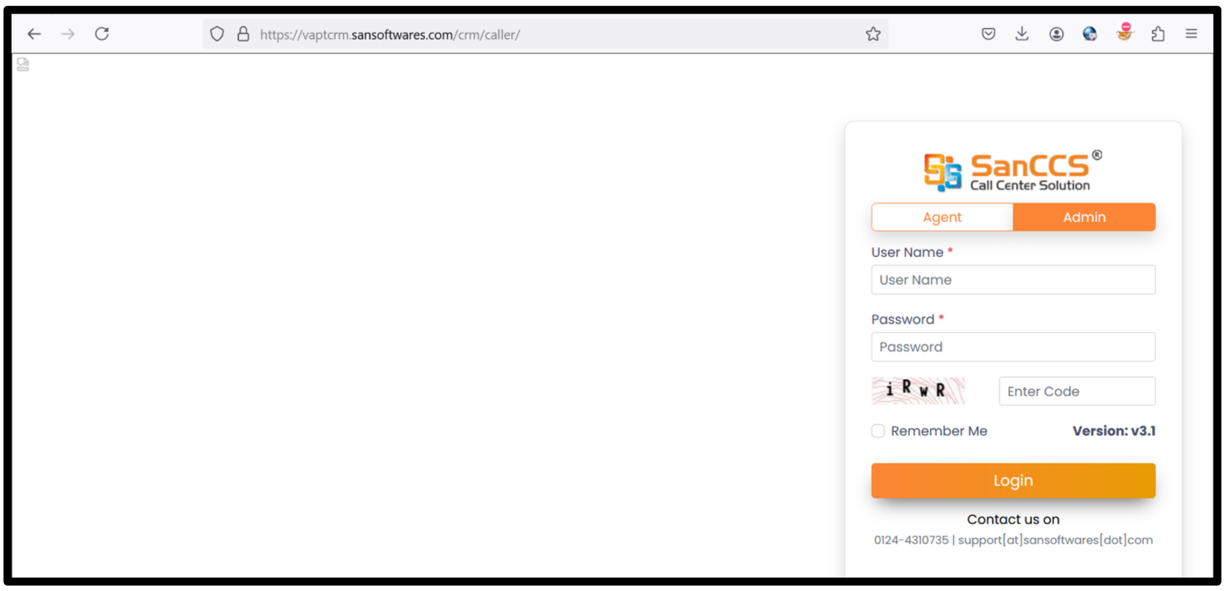
ix) **References to evidences / Proof of Concept: N/A**

Appendices

Website Crawls

https://vaptcrm.sansoftwares.com/crm/caller/
https://vaptcrm.sansoftwares.com/crm/home
https://vaptcrm.sansoftwares.com/crm/monitor
https://vaptcrm.sansoftwares.com/crm/usergroup
https://vaptcrm.sansoftwares.com/crm/usertype
https://vaptcrm.sansoftwares.com/crm/user
https://vaptcrm.sansoftwares.com/crm/agentgroup
https://vaptcrm.sansoftwares.com/crm/agent
https://vaptcrm.sansoftwares.com/crm/branch
https://vaptcrm.sansoftwares.com/crm/script
https://vaptcrm.sansoftwares.com/crm/company
https://vaptcrm.sansoftwares.com/crm/trunkgroup
https://vaptcrm.sansoftwares.com/crm/trunk
https://vaptcrm.sansoftwares.com/crm/extensiongroup
https://vaptcrm.sansoftwares.com/crm/extension
https://vaptcrm.sansoftwares.com/crm/acd
https://vaptcrm.sansoftwares.com/crm/context
https://vaptcrm.sansoftwares.com/crm/agentbreak
https://vaptcrm.sansoftwares.com/crm/paginatemaster
https://vaptcrm.sansoftwares.com/crm/favouritemenu
https://vaptcrm.sansoftwares.com/crm/process
https://vaptcrm.sansoftwares.com/crm/campaign
https://vaptcrm.sansoftwares.com/crm/did
https://vaptcrm.sansoftwares.com/crm/contactmaster
https://vaptcrm.sansoftwares.com/crm/processreport
https://vaptcrm.sansoftwares.com/crm/Tms
https://vaptcrm.sansoftwares.com/crm/formbuilder
https://vaptcrm.sansoftwares.com/crm/formdesigner
https://vaptcrm.sansoftwares.com/crm/importmaster
https://vaptcrm.sansoftwares.com/crm/filemaster
https://vaptcrm.sansoftwares.com/crm/churndata
https://vaptcrm.sansoftwares.com/crm/datamanagement
https://vaptcrm.sansoftwares.com/crm/calllogreport
https://vaptcrm.sansoftwares.com/crm/customqueryresults
https://vaptcrm.sansoftwares.com/crm/TrunkReport
https://vaptcrm.sansoftwares.com/crm/updatesoftware
https://vaptcrm.sansoftwares.com/crm/client
https://vaptcrm.sansoftwares.com/crm/Apidoc
https://vaptcrm.sansoftwares.com/crm/agenttheme
https://vaptcrm.sansoftwares.com/crm/Crmapidoc
https://vaptcrm.sansoftwares.com/crm/Softwarehealth
https://vaptcrm.sansoftwares.com/crm/searchphoneno
https://vaptcrm.sansoftwares.com/crm/archivedata
https://vaptcrm.sansoftwares.com/crm/apimaster
https://vaptcrm.sansoftwares.com/crm/registeryourcopy
https://vaptcrm.sansoftwares.com/crm/domain
https://vaptcrm.sansoftwares.com/crm/loginbackground
https://vaptcrm.sansoftwares.com/crm/recordingpath
https://vaptcrm.sansoftwares.com/crm/PurgeDatabase
https://vaptcrm.sansoftwares.com/crm/module
https://vaptcrm.sansoftwares.com/crm/user/userprofile
https://vaptcrm.sansoftwares.com/crm/caller/caller/agent/
https://vaptcrm.sansoftwares.com/crm/caller//setdata

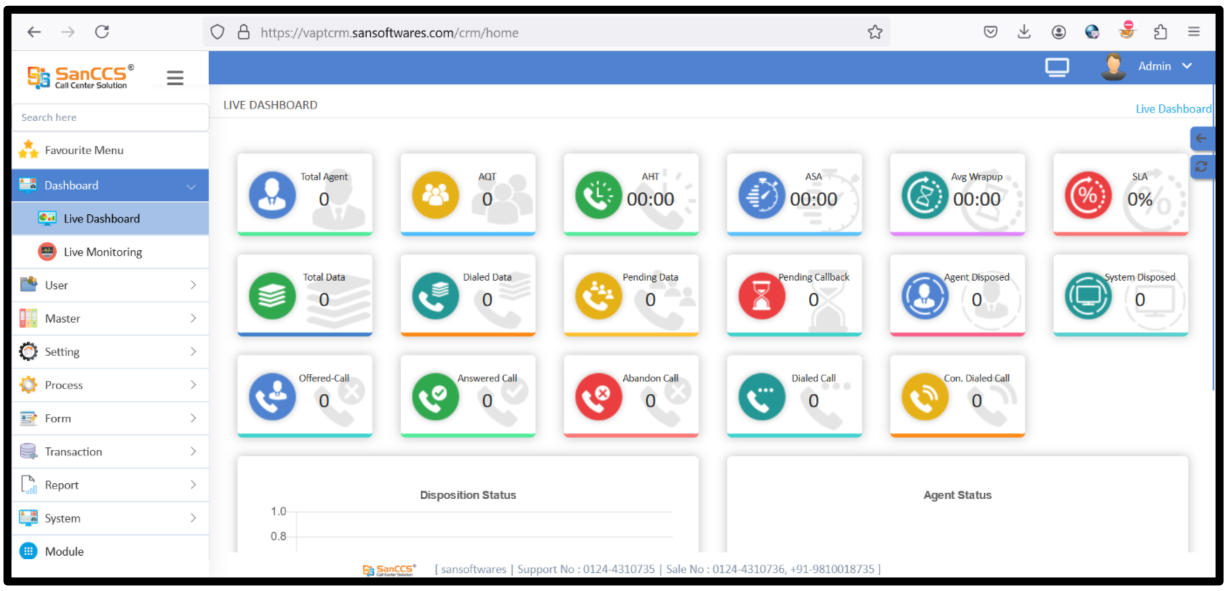
Screenshots (After Completed Audit)



https://vaptcrm.sansoftwares.com/crm/caller/

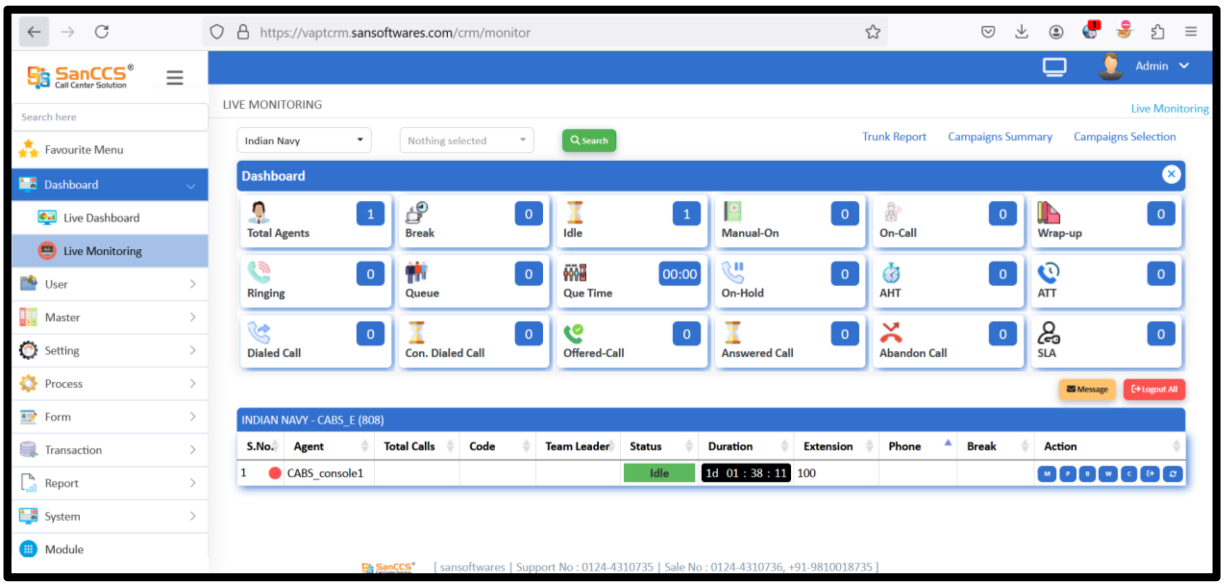
Contact us on

0124-4310735 | support[at]sansoftwares[dot]com



https://vaptcrm.sansoftwares.com/crm/home

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



https://vaptcrm.sansoftwares.com/crm/monitor

LIVE MONITORING

Indian Navy | Nothing selected | Search

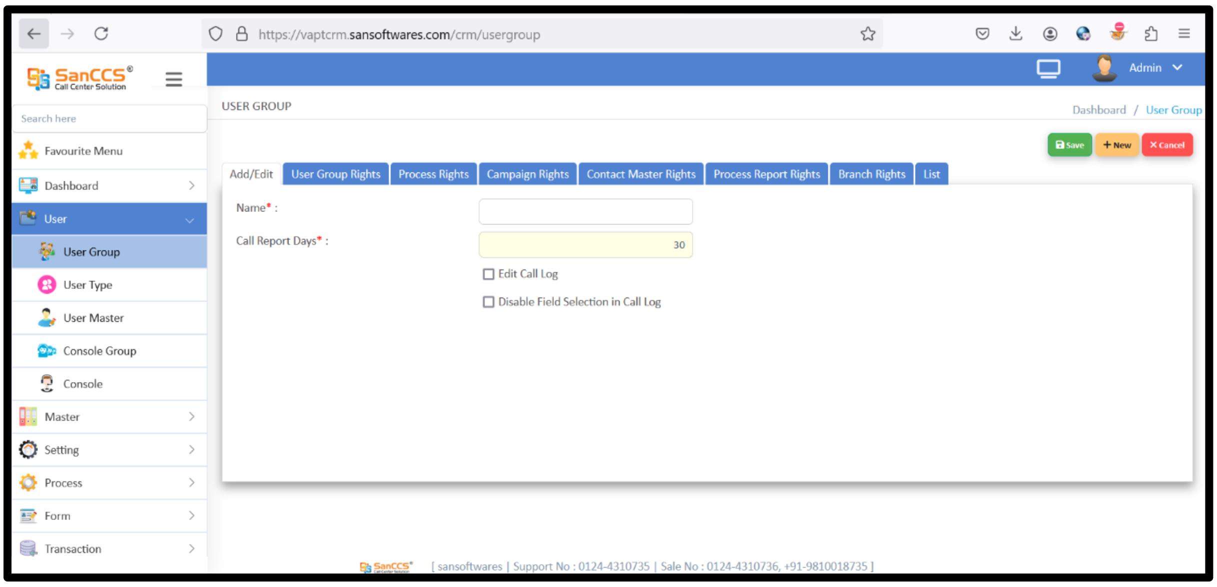
Dashboard

Total Agents 1	Break 0	Idle 1	Manual-On 0	On-Call 0	Wrap-up 0
Ringing 0	Queue 0	Que Time 00:00	On-Hold 0	AHT 0	ATT 0
Dialed Call 0	Con. Dialed Call 0	Offered-Call 0	Answered Call 0	Abandon Call 0	SLA 0

INDIAN NAVY - CABS_E (808)

S.No.	Agent	Total Calls	Code	Team Leader	Status	Duration	Extension	Phone	Break	Action
1	● CABS_console1				Idle	1d 01 : 38 : 11	100			M P B W C

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



https://vaptcrm.sansoftwares.com/crm/usergroup

USER GROUP

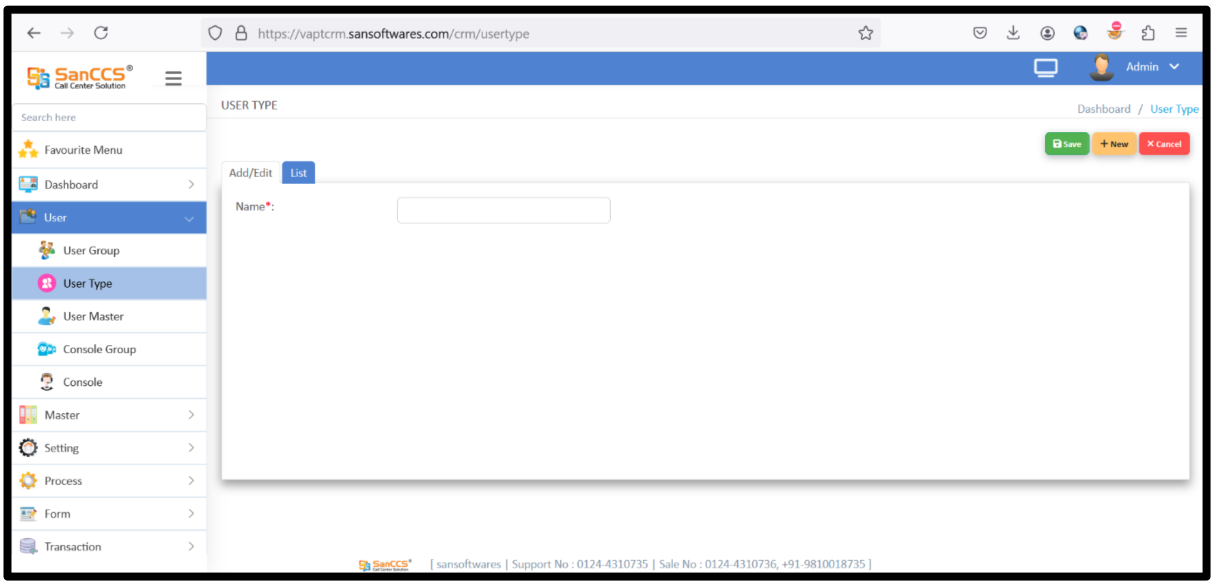
Name* :

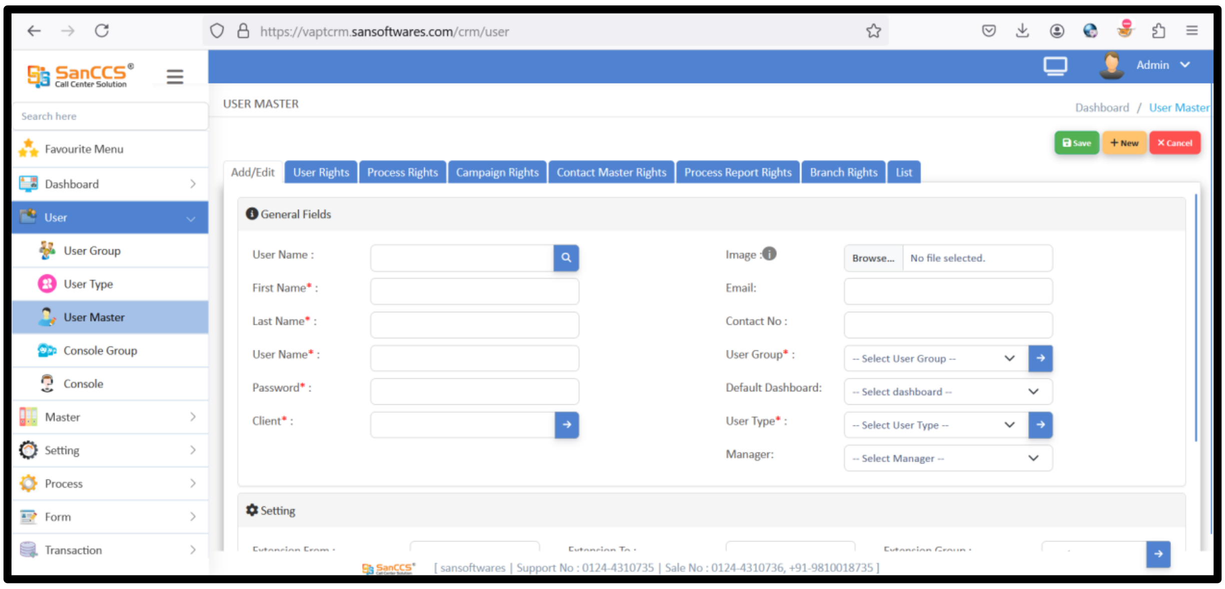
Call Report Days* : 30

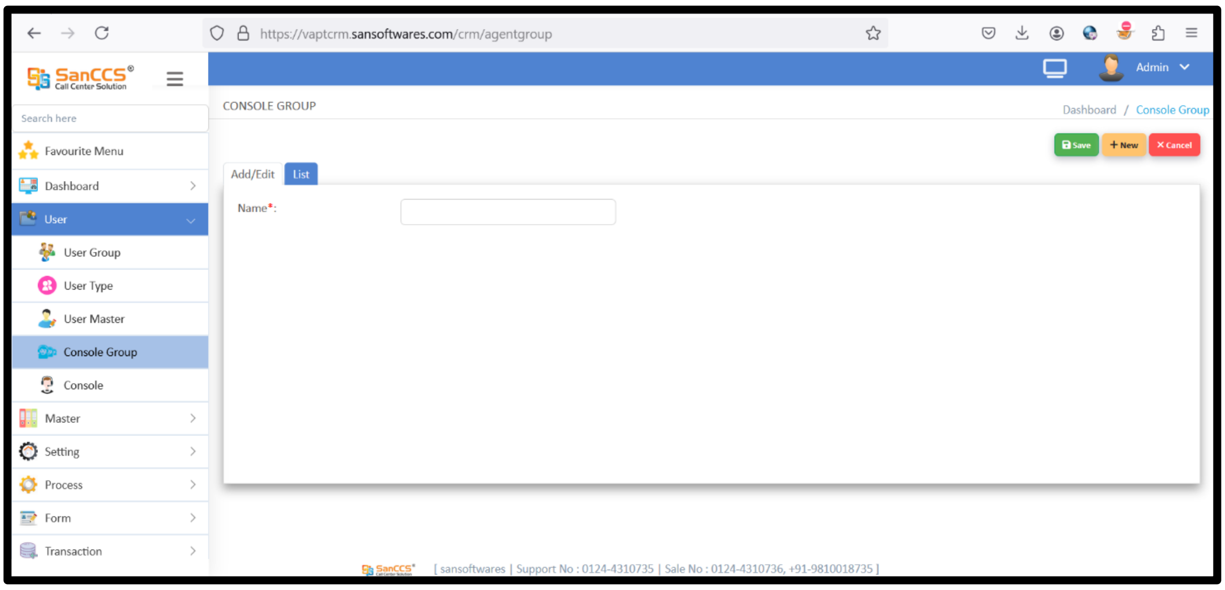
□ Edit Call Log

□ Disable Field Selection in Call Log

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/usertype
SanCCS® Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
User Group
User Type
User Master
Console Group
Console
Master
Setting
Process
Form
Transaction
USER TYPE
Dashboard / User Type
Save
+ New
✕ Cancel
Add/Edit
List
Name*:
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

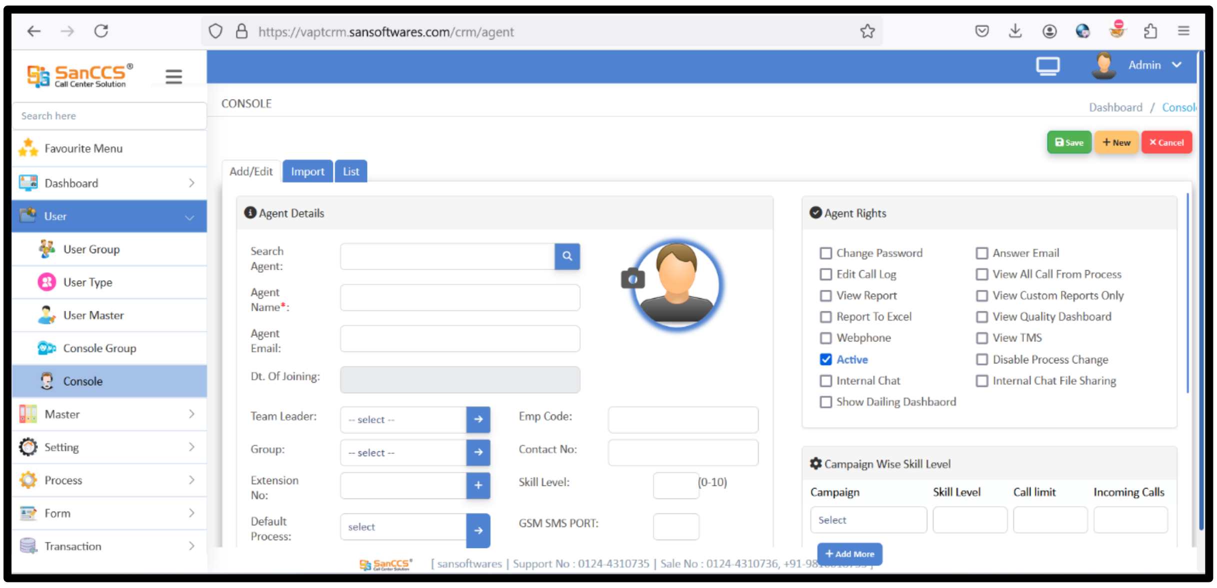

https://vaptcrm.sansoftwares.com/crm/user
SanCCS® Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
User Group
User Type
User Master
Console Group
Console
Master
Setting
Process
Form
Transaction
USER MASTER
Dashboard / User Master
Save
+ New
✕ Cancel
Add/Edit
User Rights
Process Rights
Campaign Rights
Contact Master Rights
Process Report Rights
Branch Rights
List
General Fields
User Name :
First Name* :
Last Name* :
User Name* :
Password* :
Client* :
Image :
Browse...
No file selected.
Email:
Contact No :
User Group* :
-- Select User Group --
Default Dashboard:
-- Select dashboard --
User Type* :
-- Select User Type --
Manager:
-- Select Manager --
Setting
Extension From :
Extension To :
Extension Group :
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



CONSOLE GROUP

Name*:

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



CONSOLE

Agent Details

Search Agent:

Agent Name*:

Agent Email:

Dt. Of Joining:

Team Leader: -- select --

Emp Code:

Group: -- select --

Contact No:

Extension No:

Skill Level: (0-10)

Default Process: select

GSM SMS PORT:

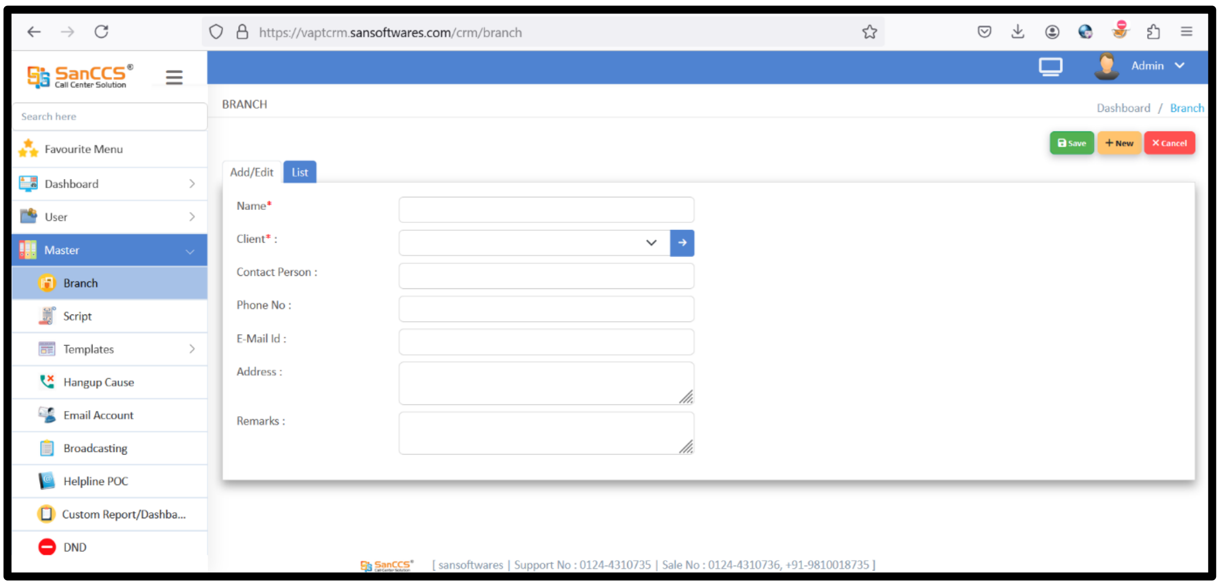
Agent Rights

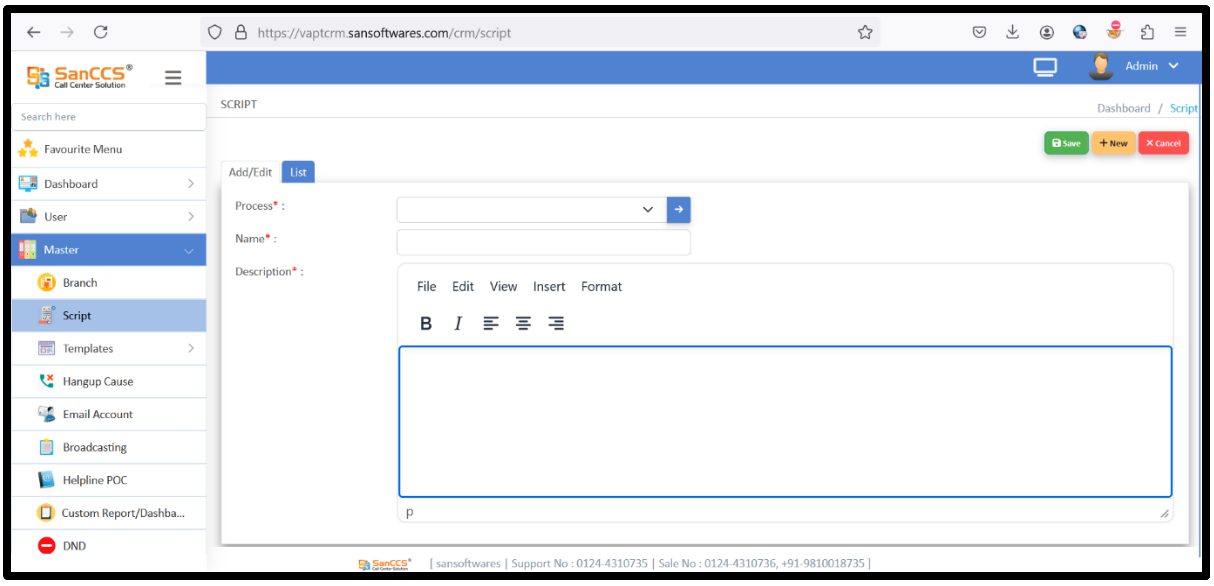
☐ Change Password
☐ Edit Call Log
☐ View Report
☐ Report To Excel
☐ Webphone
☑ Active
☐ Internal Chat
☐ Show Dailing Dashbaord
☐ Answer Email
☐ View All Call From Process
☐ View Custom Reports Only
☐ View Quality Dashboard
☐ View TMS
☐ Disable Process Change
☐ Internal Chat File Sharing

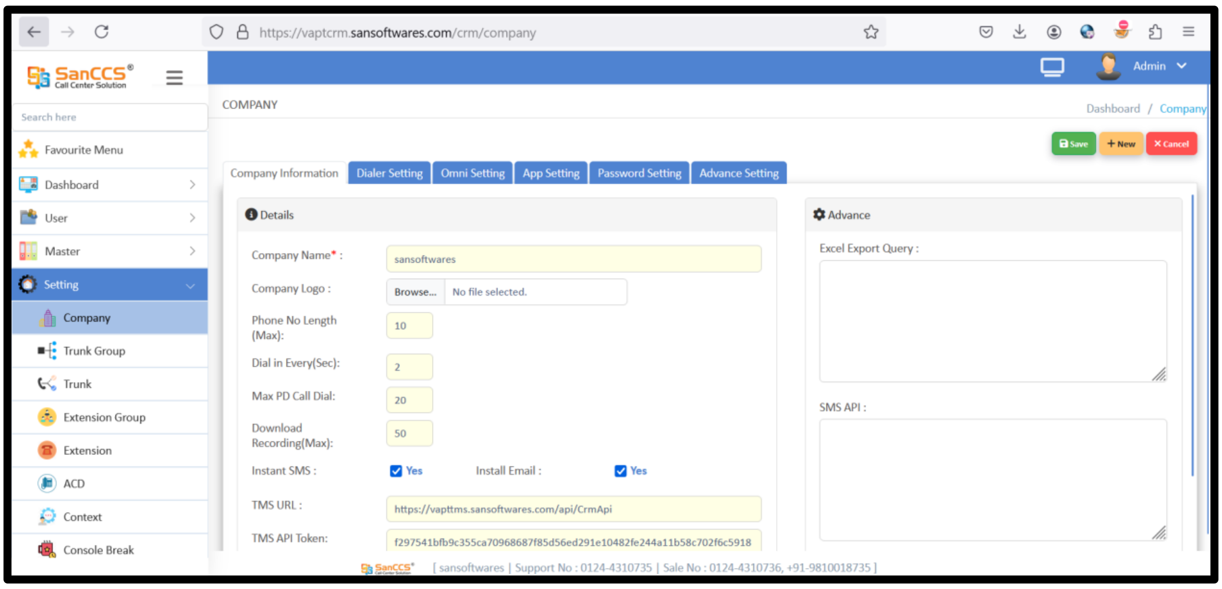
Campaign Wise Skill Level

Campaign	Skill Level	Call limit	Incoming Calls
Select			

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-98


https://vaptcrm.sansoftwares.com/crm/branch
SanCCS® Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Branch
Script
Templates
Hangup Cause
Email Account
Broadcasting
Helpline POC
Custom Report/Dashba...
DND
BRANCH
Dashboard / Branch
Save
+ New
× Cancel
Add/Edit
List
Name*
Client* :
Contact Person :
Phone No :
E-Mail Id :
Address :
Remarks :
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/script
SanCCS® Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Branch
Script
Templates
Hangup Cause
Email Account
Broadcasting
Helpline POC
Custom Report/Dashba...
DND
SCRIPT
Dashboard / Script
Save
+ New
× Cancel
Add/Edit
List
Process* :
Name* :
Description* :
File
Edit
View
Insert
Format
B
I
p
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



COMPANY

Details

Company Name* : sansoftwares

Company Logo : Browse... No file selected.

Phone No Length (Max): 10

Dial in Every(Sec): 2

Max PD Call Dial: 20

Download Recording(Max): 50

Instant SMS : ☑ Yes Install Email : ☑ Yes

TMS URL : https://vapttms.sansoftwares.com/api/CrmApi

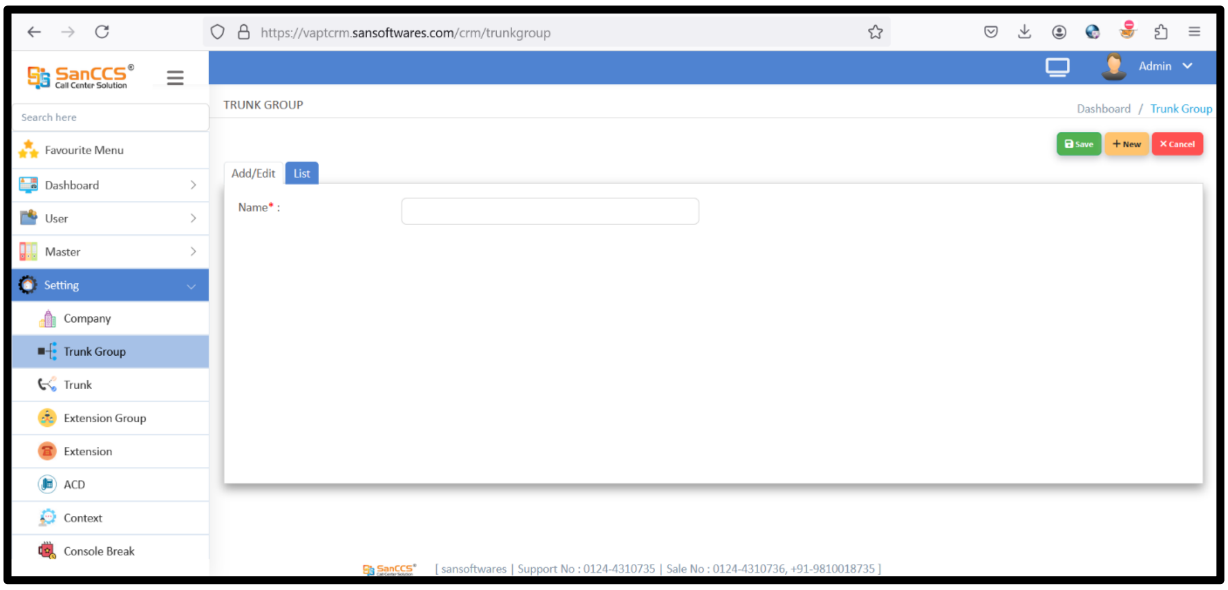
TMS API Token: f297541bfb9c355ca70968687f85d56ed291e10482fe244a11b58c702f6c5918

Advance

Excel Export Query :

SMS API :

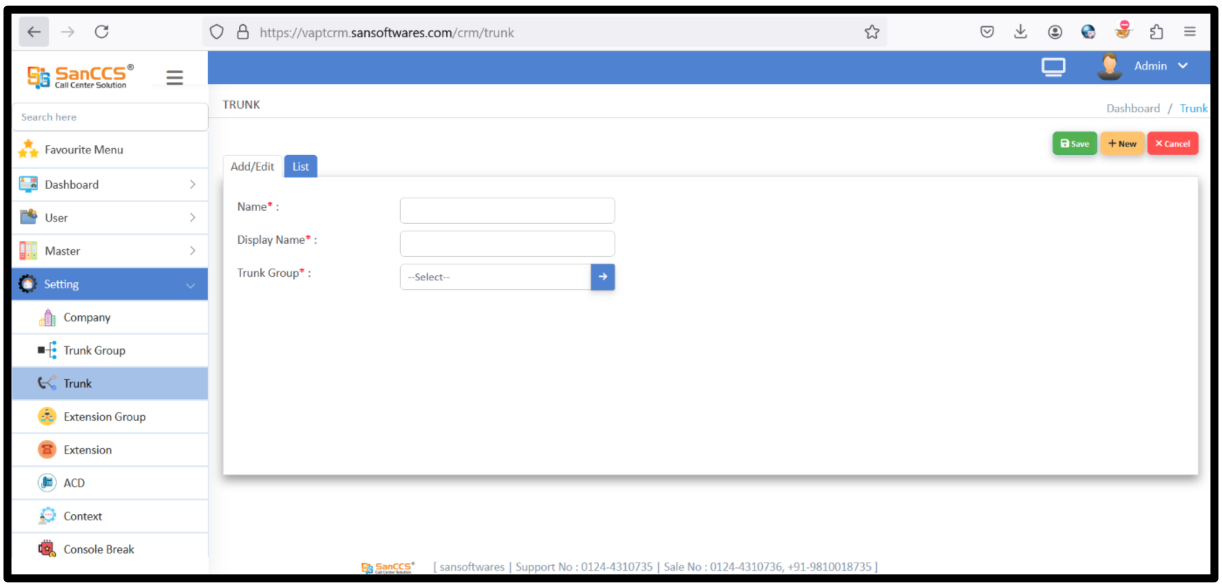
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



TRUNK GROUP

Name* :

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/trunk

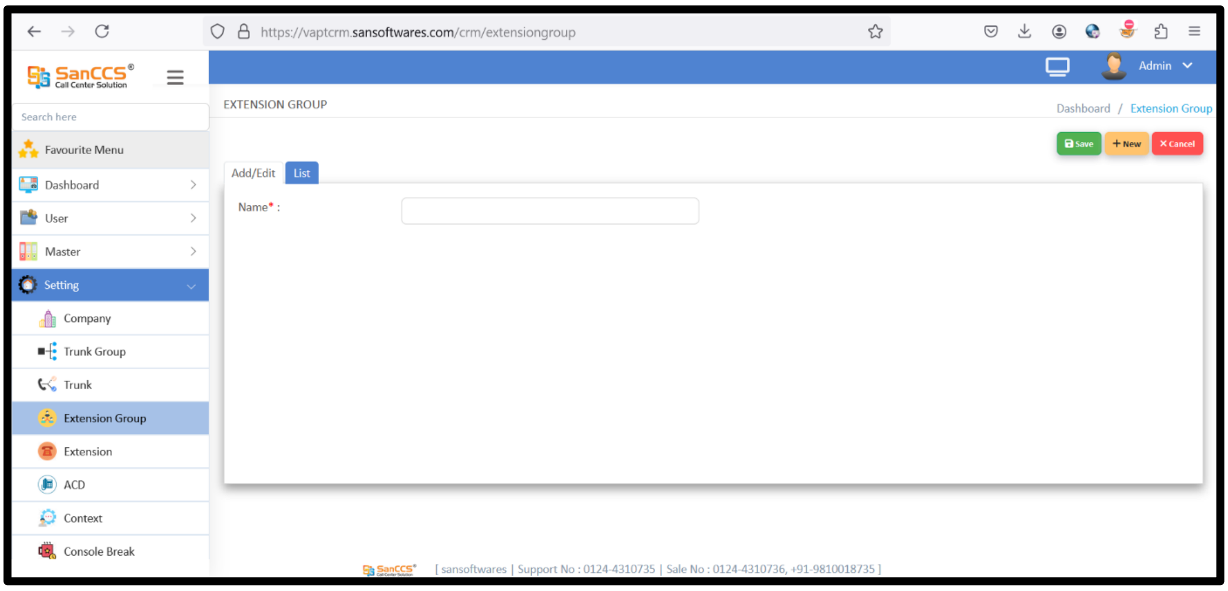
TRUNK

Name* :

Display Name* :

Trunk Group* : --Select--

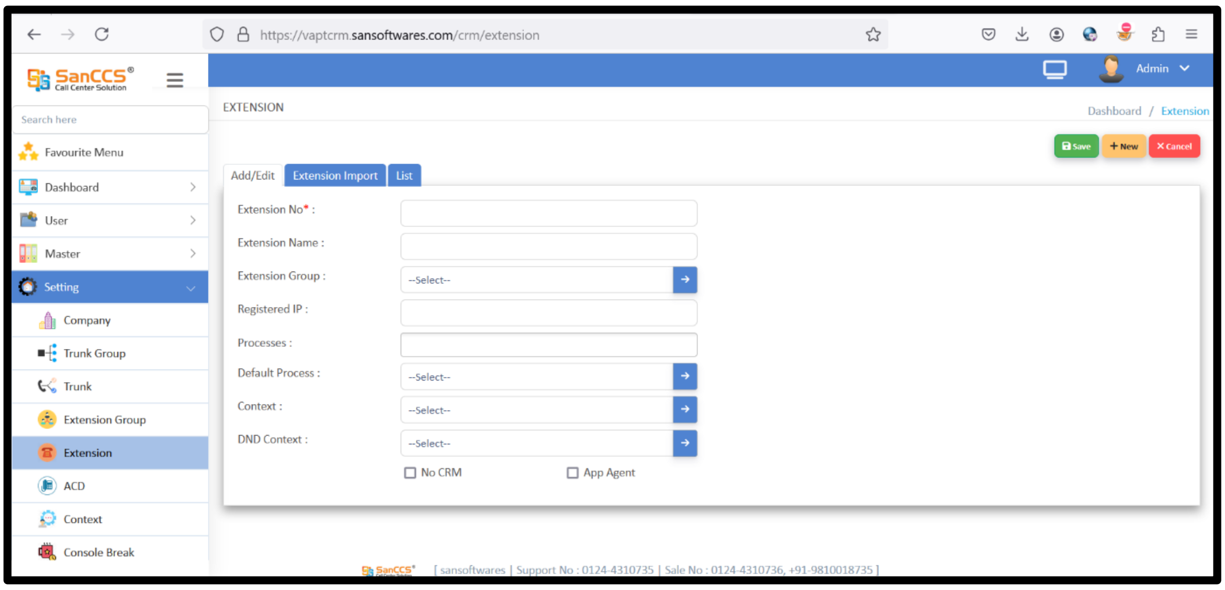
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/extensiongroup

EXTENSION GROUP

Name* :

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

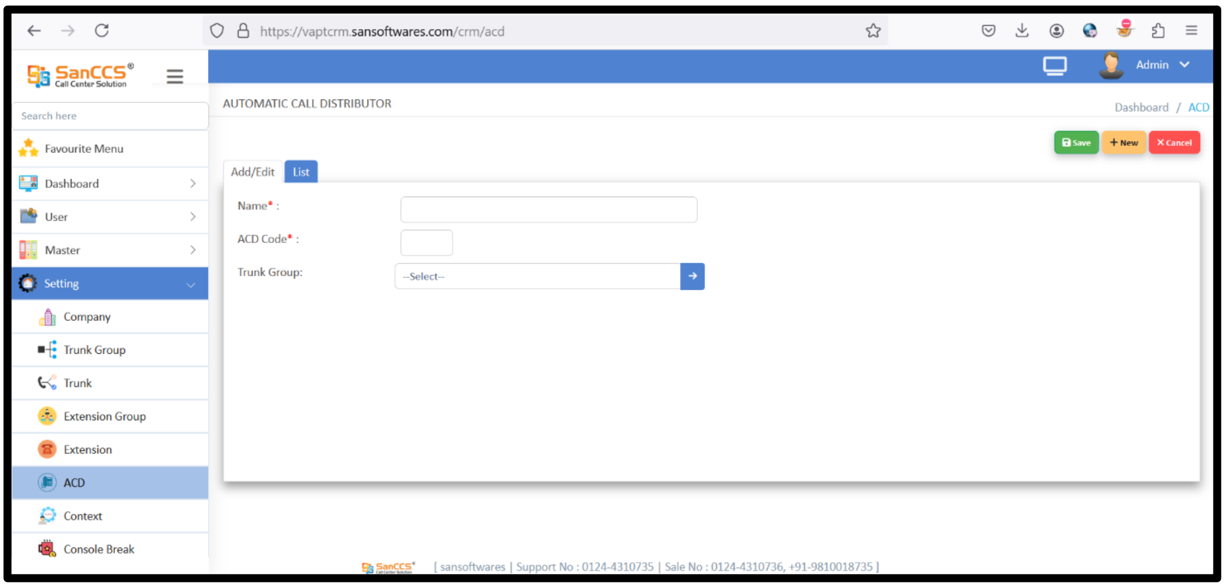


EXTENSION

Extension No* :	
Extension Name :	
Extension Group :	--Select--
Registered IP :	
Processes :	
Default Process :	--Select--
Context :	--Select--
DND Context :	--Select--

☐ No CRM ☐ App Agent

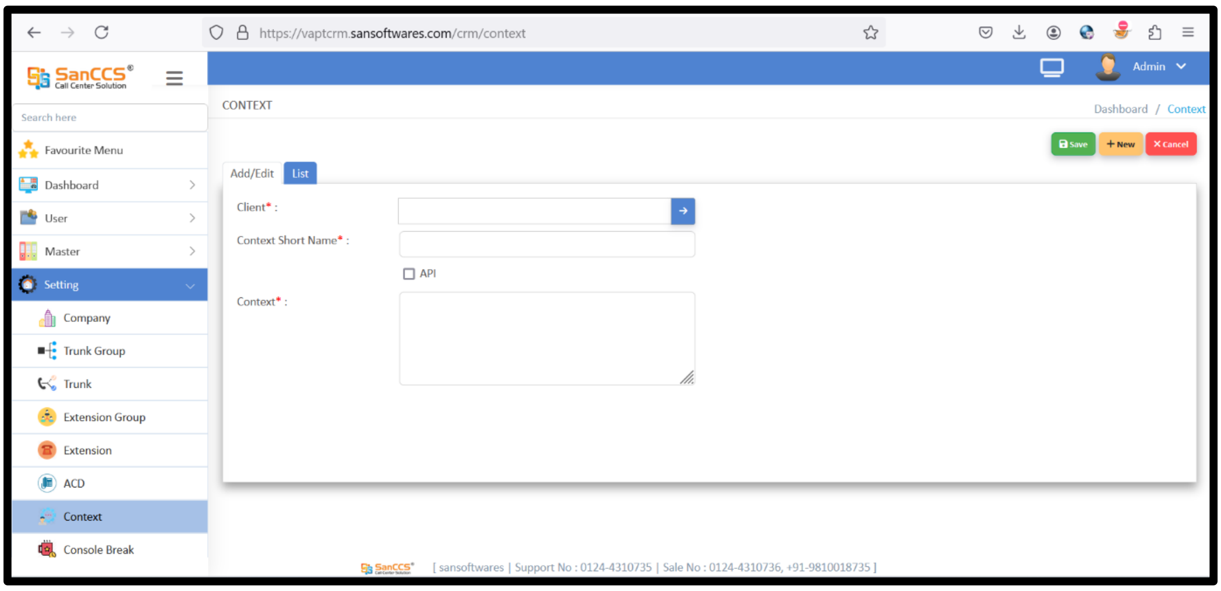
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

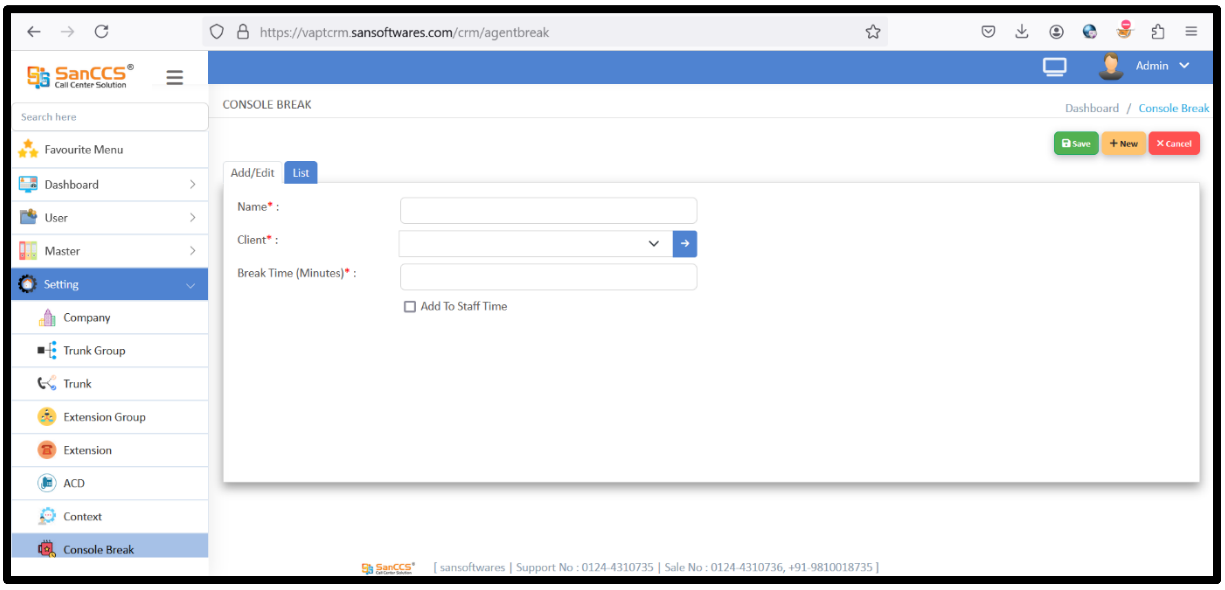


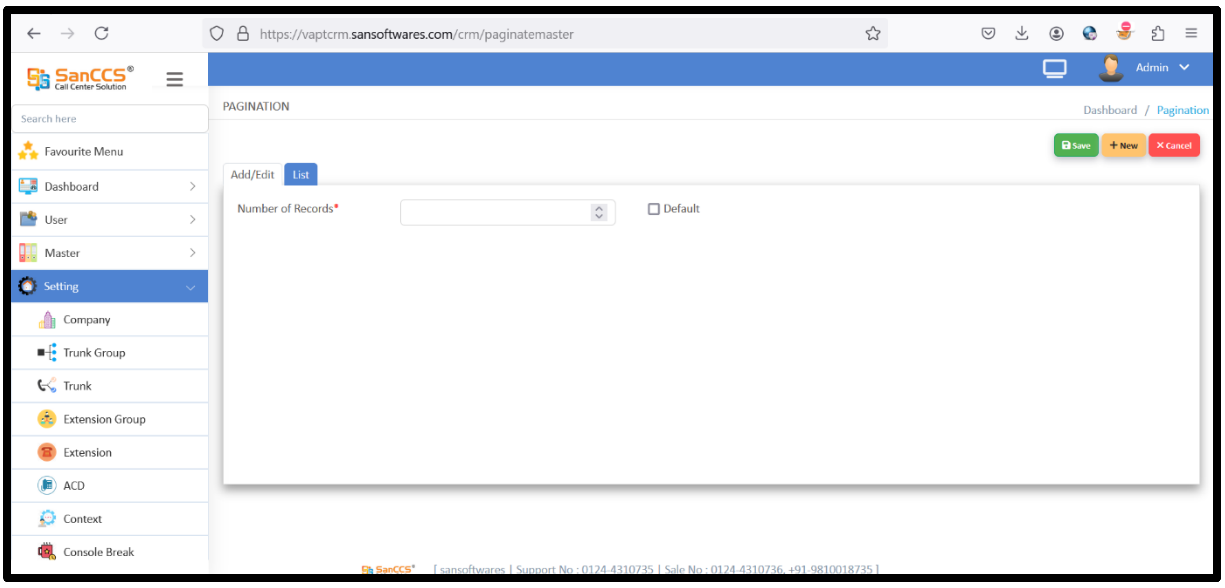
AUTOMATIC CALL DISTRIBUTOR

Name* :	
ACD Code* :	
Trunk Group:	--Select--

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/context
SanCCS Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Setting
Company
Trunk Group
Trunk
Extension Group
Extension
ACD
Context
Console Break
CONTEXT
Dashboard / Context
Save
+ New
✕ Cancel
Add/Edit
List
Client* :
Context Short Name* :
□ API
Context* :
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/agentbreak
SanCCS Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Setting
Company
Trunk Group
Trunk
Extension Group
Extension
ACD
Context
Console Break
CONSOLE BREAK
Dashboard / Console Break
Save
+ New
✕ Cancel
Add/Edit
List
Name* :
Client* :
Break Time (Minutes)* :
□ Add To Staff Time
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



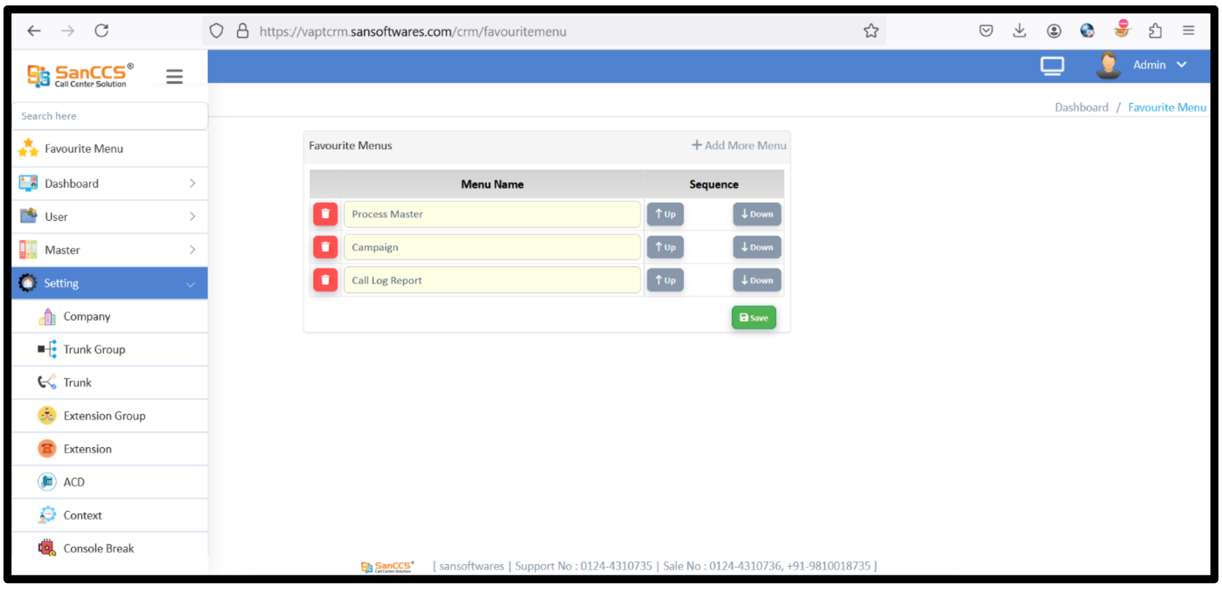
PAGINATION

Dashboard / Pagination

Number of Records*

□ Default

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

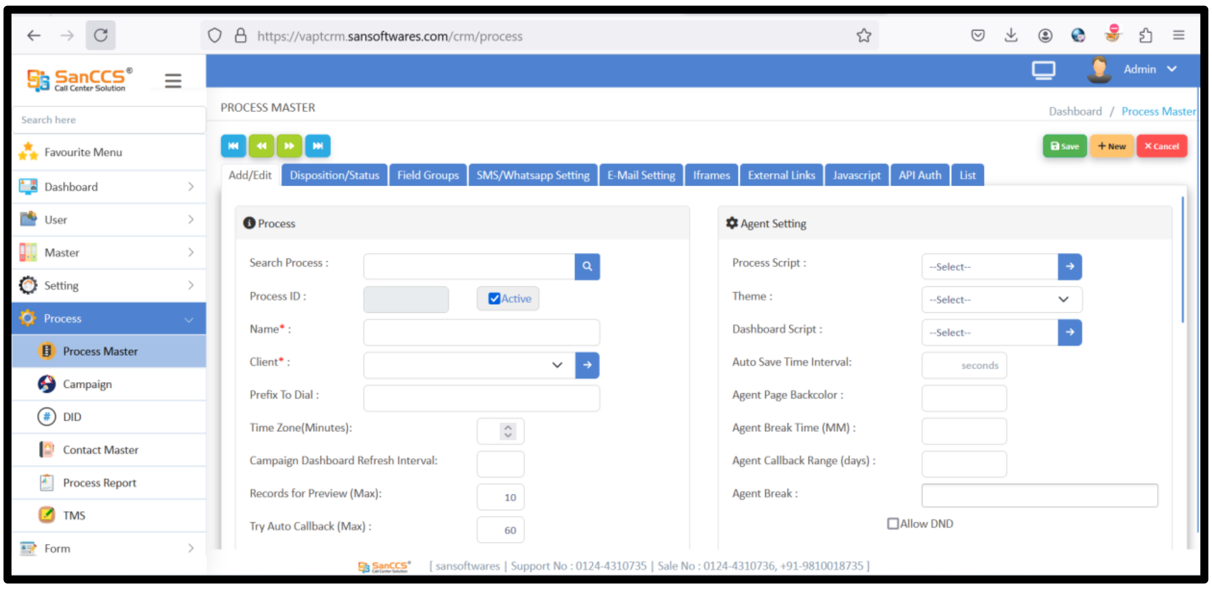


Dashboard / Favourite Menu

Favourite Menus

	Menu Name	Sequence	
	Process Master	↑ Up	↓ Down
	Campaign	↑ Up	↓ Down
	Call Log Report	↑ Up	↓ Down

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



PROCESS MASTER

Process

Search Process :

Process ID : ☑ Active

Name* :

Client* :

Prefix To Dial :

Time Zone(Minutes):

Campaign Dashboard Refresh Interval:

Records for Preview (Max): 10

Try Auto Callback (Max) : 60

Agent Setting

Process Script : --Select--

Theme : --Select--

Dashboard Script : --Select--

Auto Save Time Interval: seconds

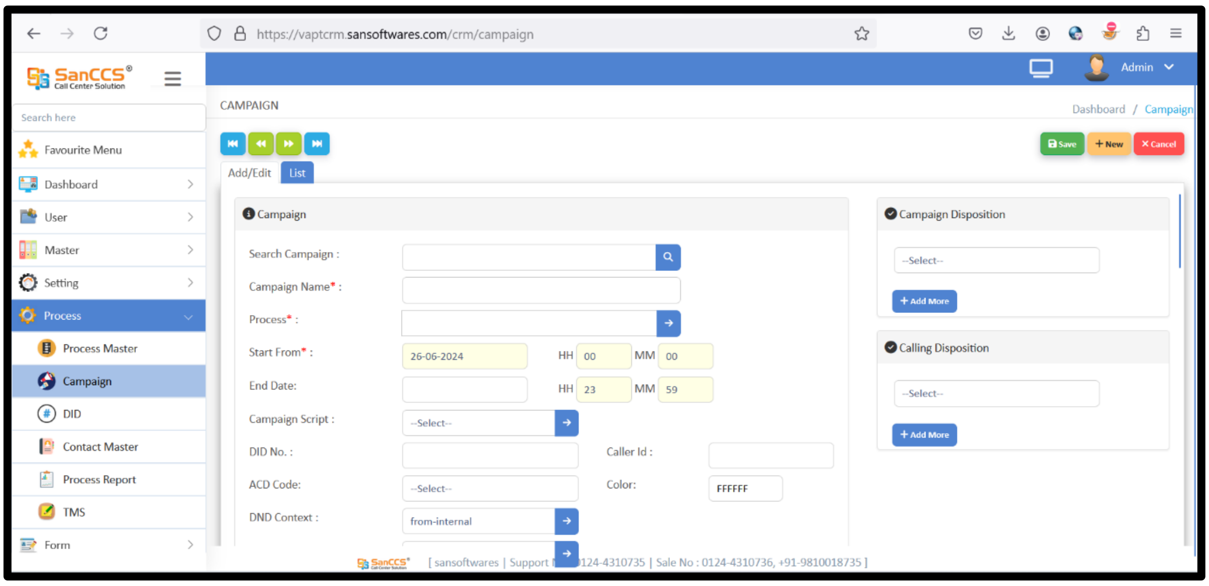
Agent Page Backcolor :

Agent Break Time (MM) :

Agent Callback Range (days) :

Agent Break :

□ Allow DND



CAMPAIGN

Campaign

Search Campaign :

Campaign Name* :

Process* :

Start From* : 26-06-2024 HH 00 MM 00

End Date: HH 23 MM 59

Campaign Script : --Select--

DID No. : Caller Id :

ACD Code: --Select-- Color: FFFFFF

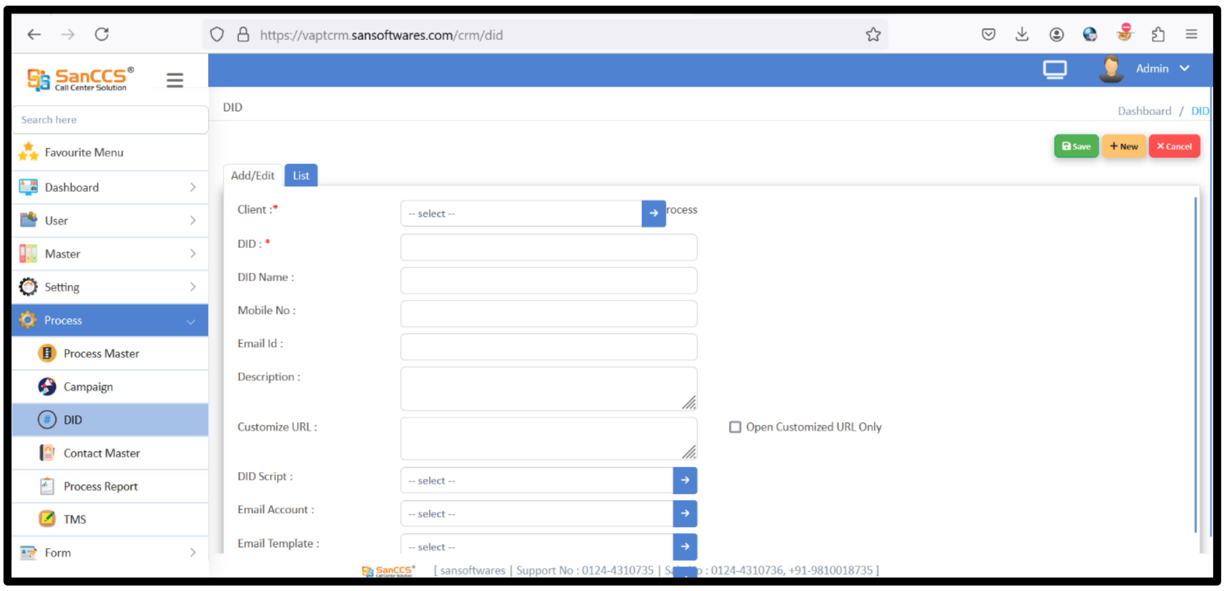
DND Context : from-internal

Campaign Disposition

--Select--

Calling Disposition

--Select--



Client :* -- select -- rocess

DID : *

DID Name :

Mobile No :

Email Id :

Description :

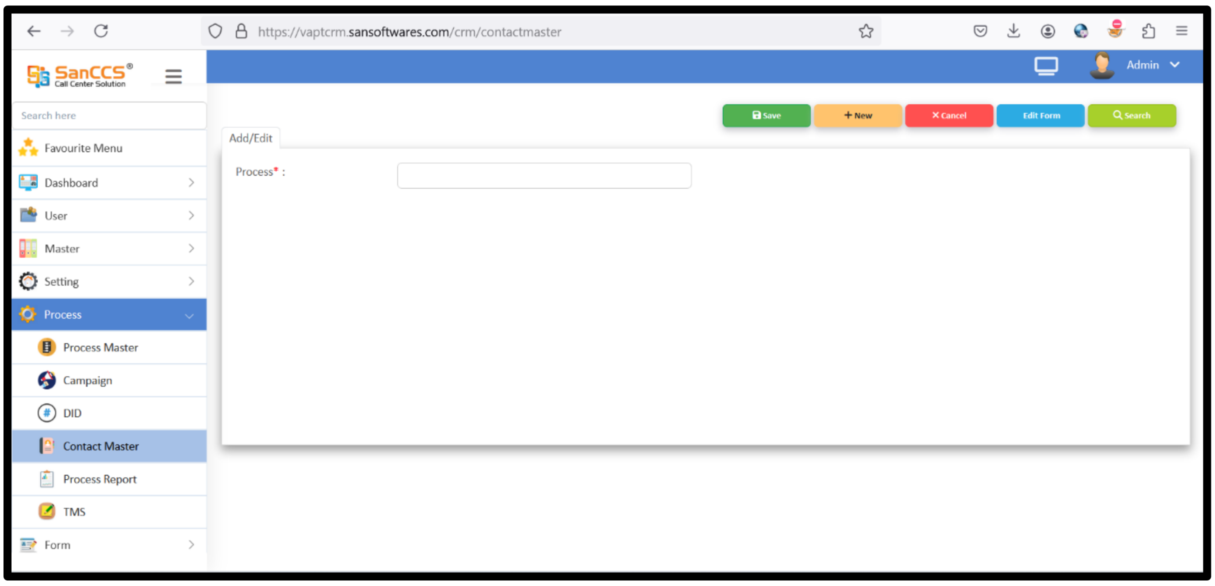
Customize URL : □ Open Customized URL Only

DID Script : -- select --

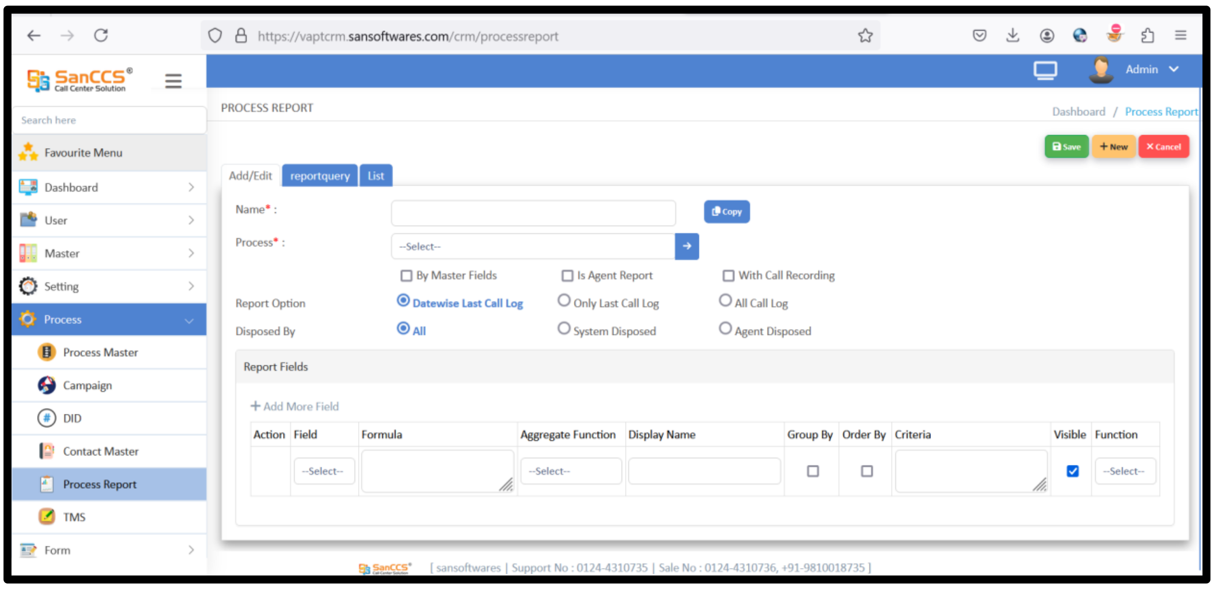
Email Account : -- select --

Email Template : -- select --

[sansoftwares | Support No : 0124-4310735 | S... : 0124-4310736, +91-9810018735]



Process* :



PROCESS REPORT

Dashboard / Process Report

Name* :

Process* : --Select--

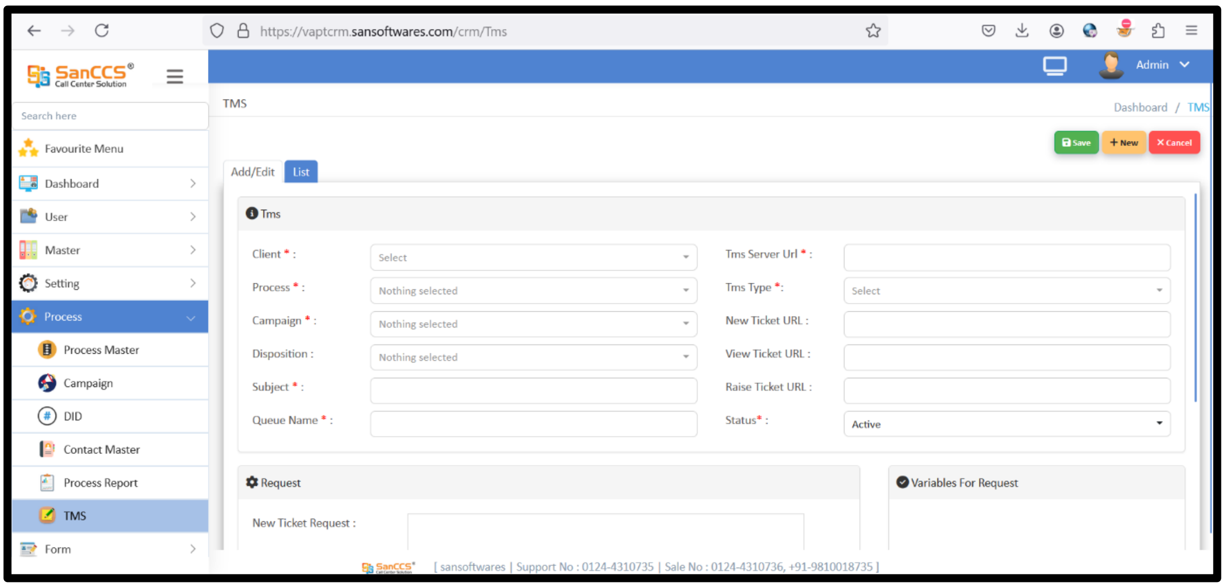
□ By Master Fields □ Is Agent Report □ With Call Recording

Report Option ● Datewise Last Call Log ○ Only Last Call Log ○ All Call Log

Disposed By ● All ○ System Disposed ○ Agent Disposed

Report Fields

Action	Field	Formula	Aggregate Function	Display Name	Group By	Order By	Criteria	Visible	Function
	--Select--		--Select--		□	□		☑	--Select--


https://vaptcrm.sansoftwares.com/crm/Tms
SanCCS® Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Setting
Process
Process Master
Campaign
DID
Contact Master
Process Report
TMS
Form
Save
+ New
✕ Cancel
Add/Edit
List
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

TMS

Dashboard / TMS

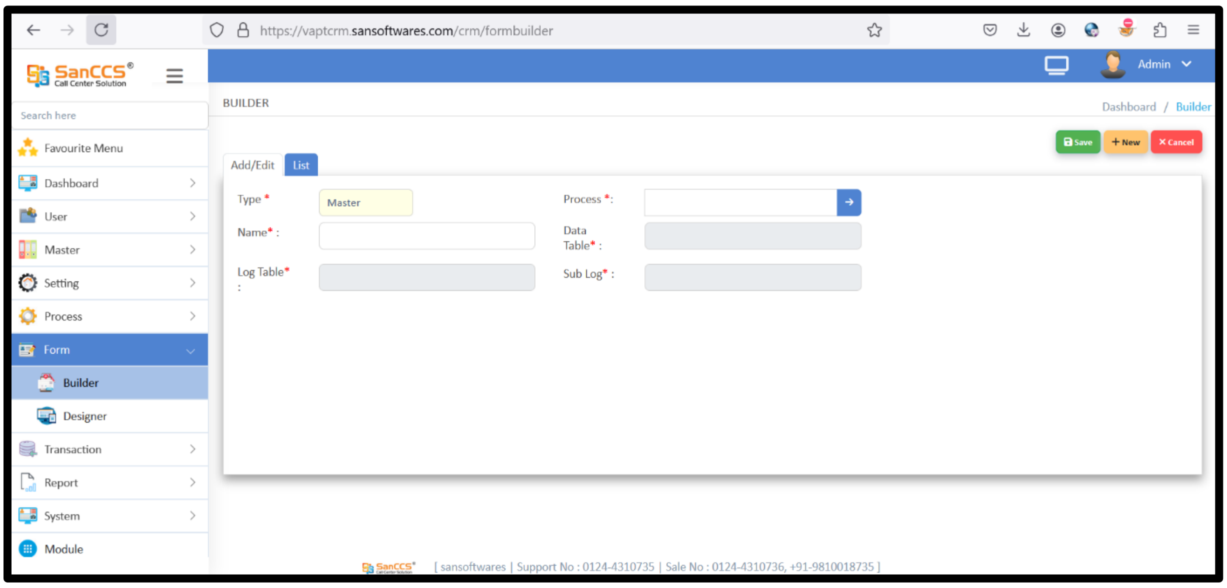
Tms

Client * :	Select	Tms Server Url * :	
Process * :	Nothing selected	Tms Type * :	Select
Campaign * :	Nothing selected	New Ticket URL :	
Disposition :	Nothing selected	View Ticket URL :	
Subject * :		Raise Ticket URL :	
Queue Name * :		Status* :	Active

Request

New Ticket Request :

Variables For Request



Type * Master

Process *:

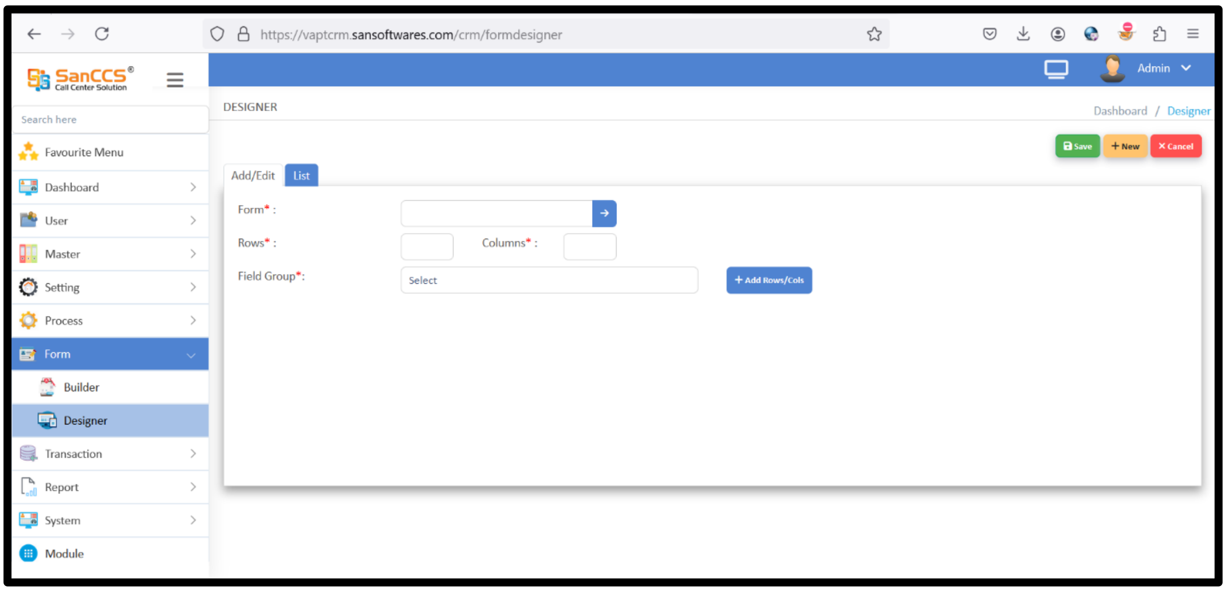
Name* :

Data Table* :

Log Table* :

Sub Log* :

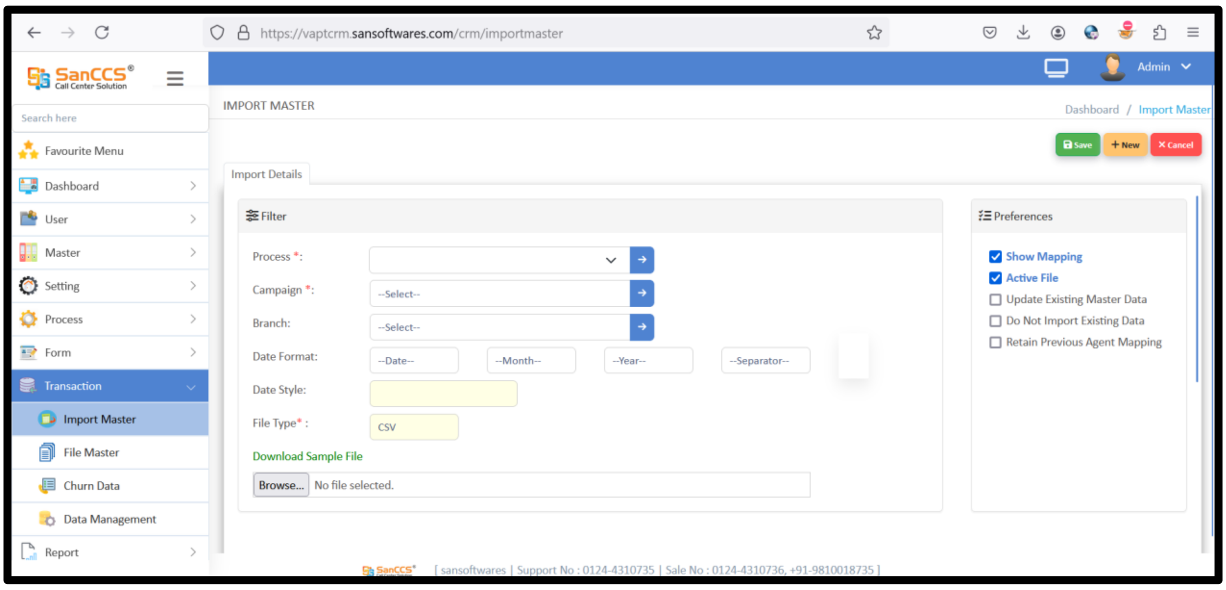
SanCCS® [sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



Form* :

Rows* : Columns* :

Field Group*: Select



IMPORT MASTER

Import Details

Filter

Process *:

Campaign *: --Select--

Branch: --Select--

Date Format: --Date-- --Month-- --Year-- --Separator--

Date Style:

File Type* : CSV

Download Sample File

Browse... No file selected.

Preferences

☑ Show Mapping

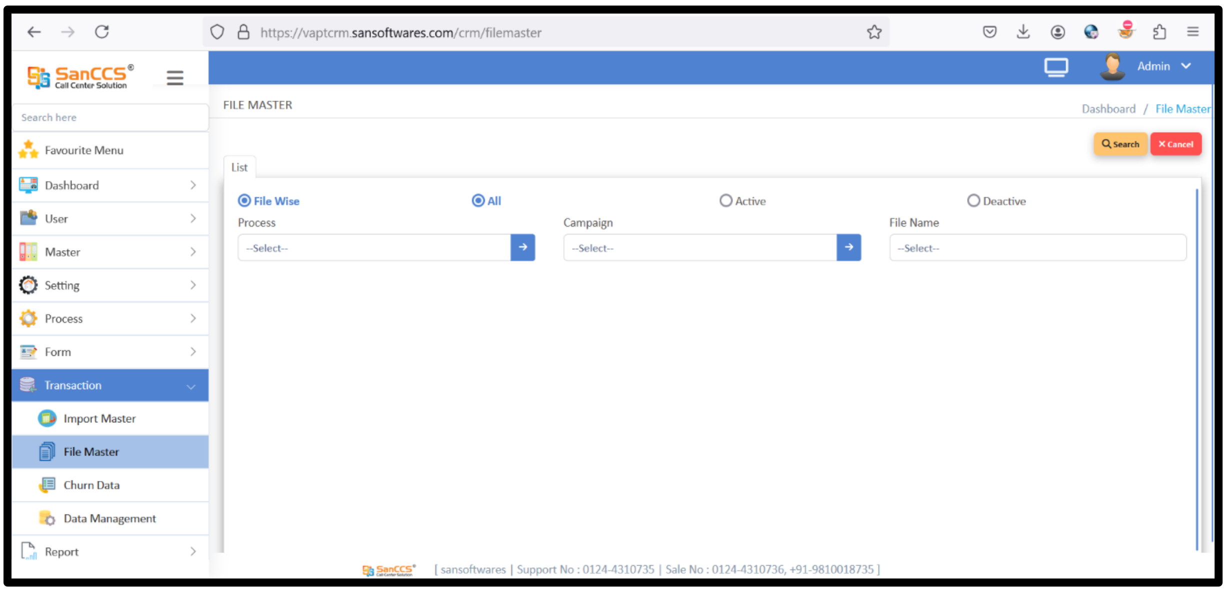
☑ Active File

□ Update Existing Master Data

□ Do Not Import Existing Data

□ Retain Previous Agent Mapping

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



FILE MASTER

List

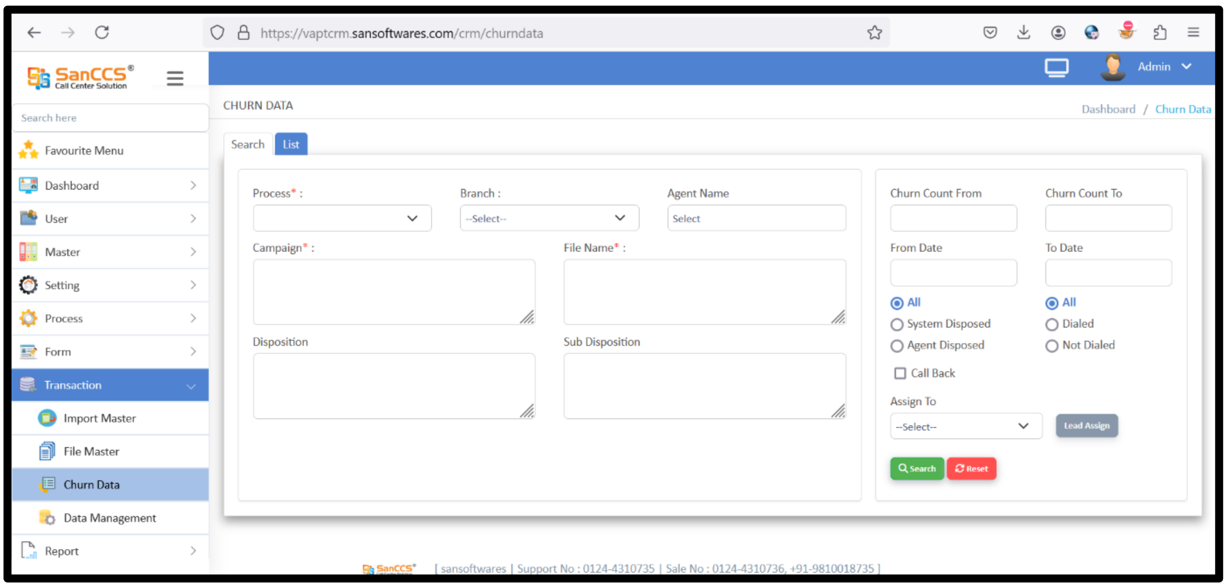
● File Wise ● All ○ Active ○ Deactive

Process: --Select--

Campaign: --Select--

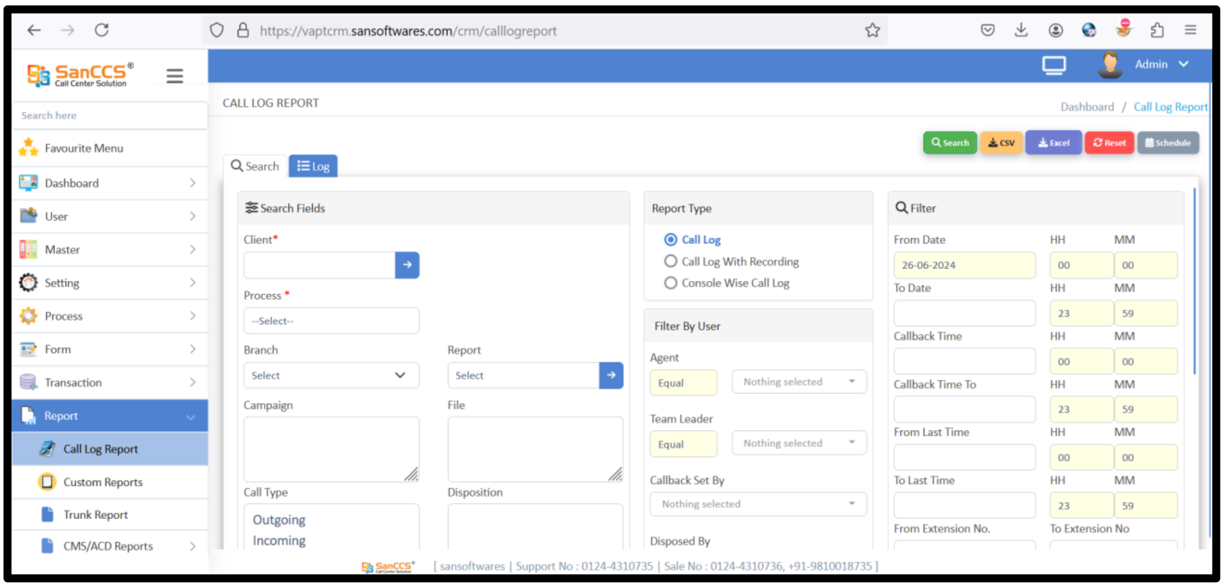
File Name: --Select--

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



https://vaptcrm.sansoftwares.com/crm/churndata

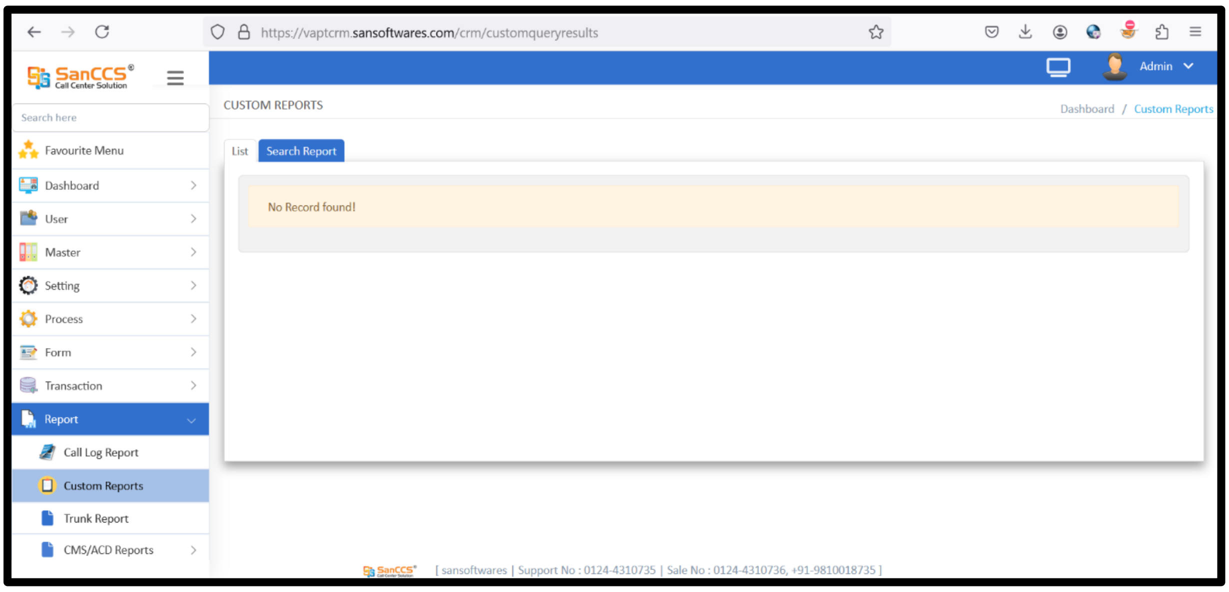
- ● All
- ○ System Disposed
- ○ Agent Disposed
- ● All
- ○ Dialed
- ○ Not Dialed
- □ Call Back



https://vaptcrm.sansoftwares.com/crm/calllogreport

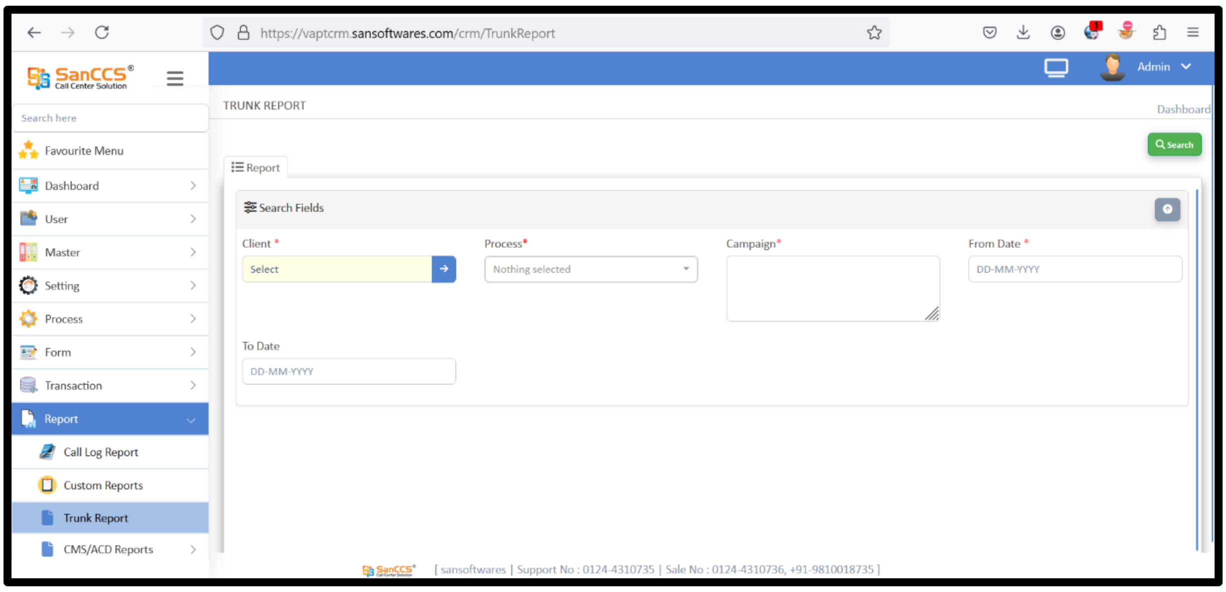
- ● Call Log
- ○ Call Log With Recording
- ○ Console Wise Call Log

		HH	MM
From Date	26-06-2024	00	00
To Date		23	59
Callback Time		00	00
Callback Time To		23	59
From Last Time		00	00
To Last Time		23	59


https://vaptcrm.sansoftwares.com/crm/customqueryresults
SanCCS Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Setting
Process
Form
Transaction
Report
Call Log Report
Custom Reports
Trunk Report
CMS/ACD Reports
Dashboard / Custom Reports
List
Search Report
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

CUSTOM REPORTS

No Record found!



TRUNK REPORT

Search Fields

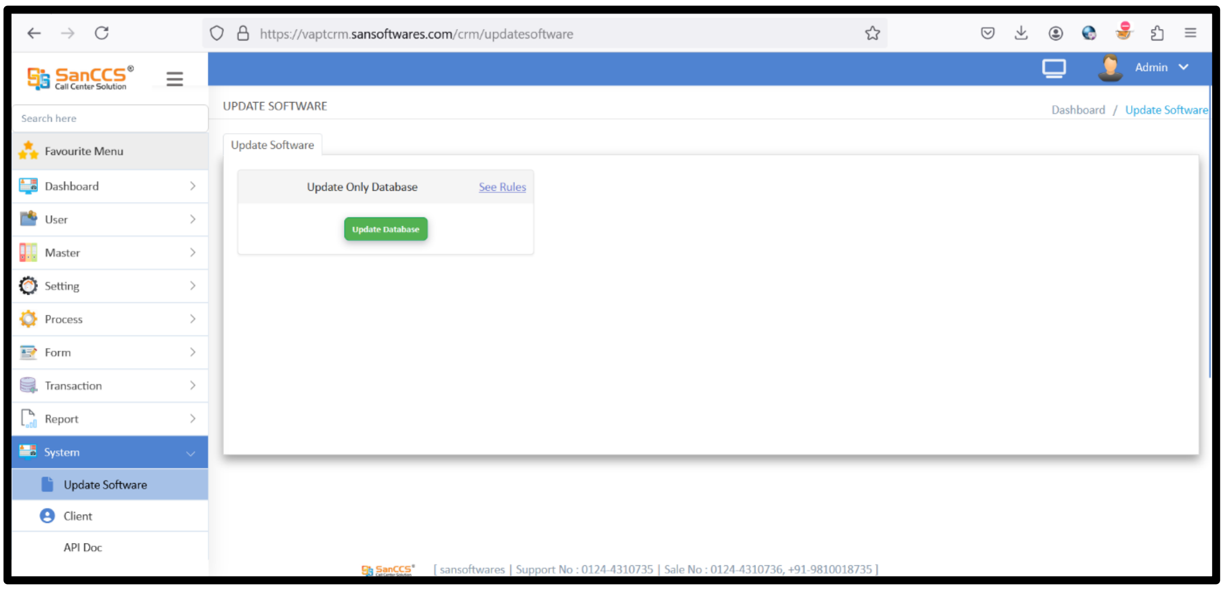
Client * Select

Process* Nothing selected

Campaign*

From Date * DD-MM-YYYY

To Date DD-MM-YYYY



https://vaptcrm.sansoftwares.com/crm/updatesoftware

UPDATE SOFTWARE

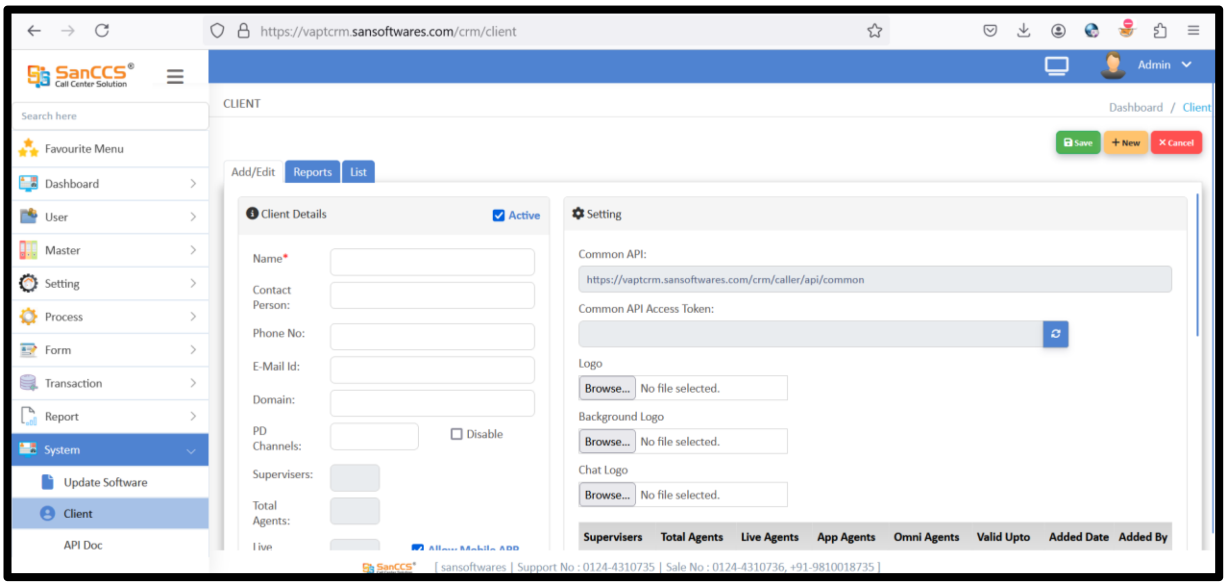
Dashboard / Update Software

Update Software

Update Only Database | See Rules

Update Database

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



https://vaptcrm.sansoftwares.com/crm/client

CLIENT

Dashboard / Client

Client Details ☑ Active

Name*:

Contact Person:

Phone No:

E-Mail Id:

Domain:

PD Channels: □ Disable

Supervisers:

Total Agents:

Live

☑ Allow Mobile APP

Setting

Common API:

https://vaptcrm.sansoftwares.com/crm/caller/api/common

Common API Access Token:

Logo

Browse... No file selected.

Background Logo

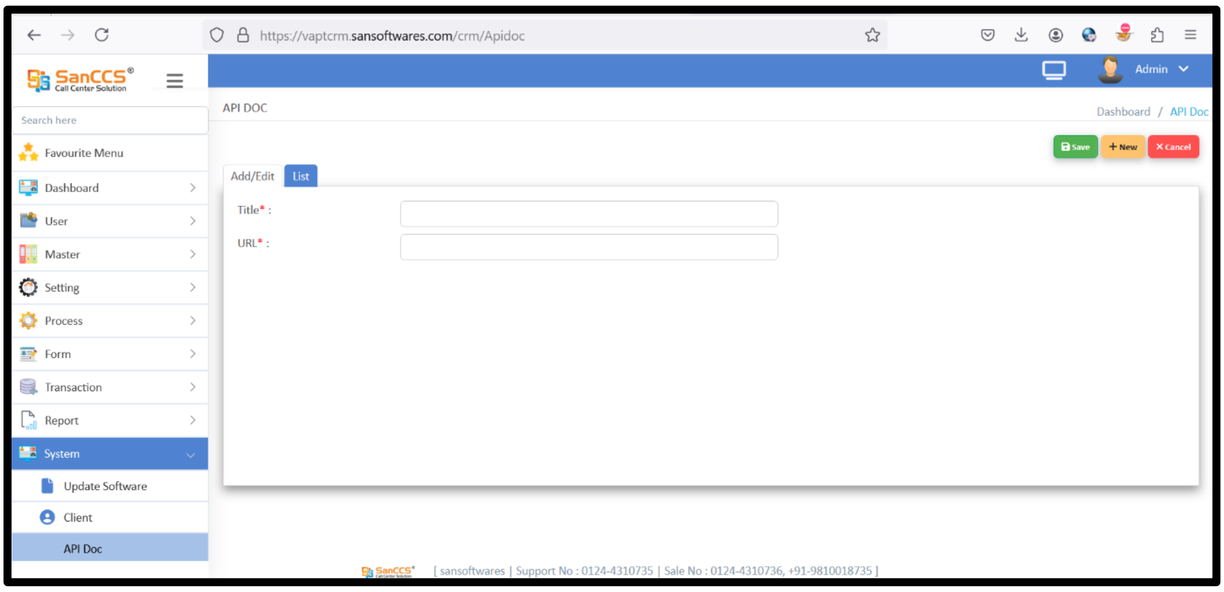
Browse... No file selected.

Chat Logo

Browse... No file selected.

Supervisers	Total Agents	Live Agents	App Agents	Omni Agents	Valid Upto	Added Date	Added By

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/Apidoc

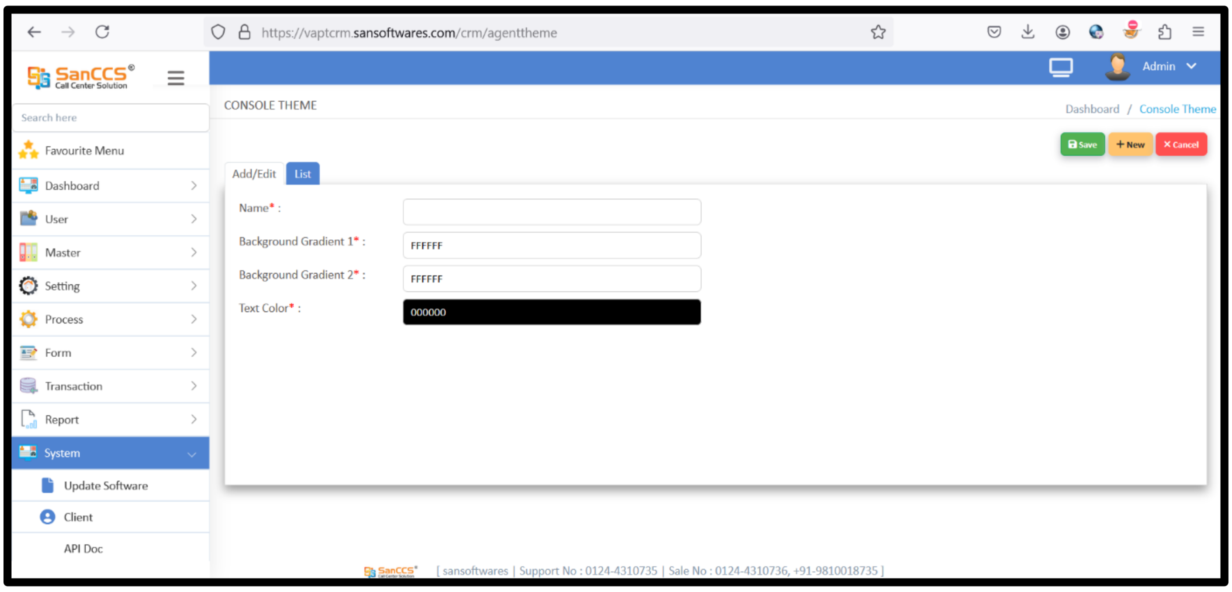
API DOC

Dashboard / API Doc

Title* :

URL* :

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/agenttheme

CONSOLE THEME

Dashboard / Console Theme

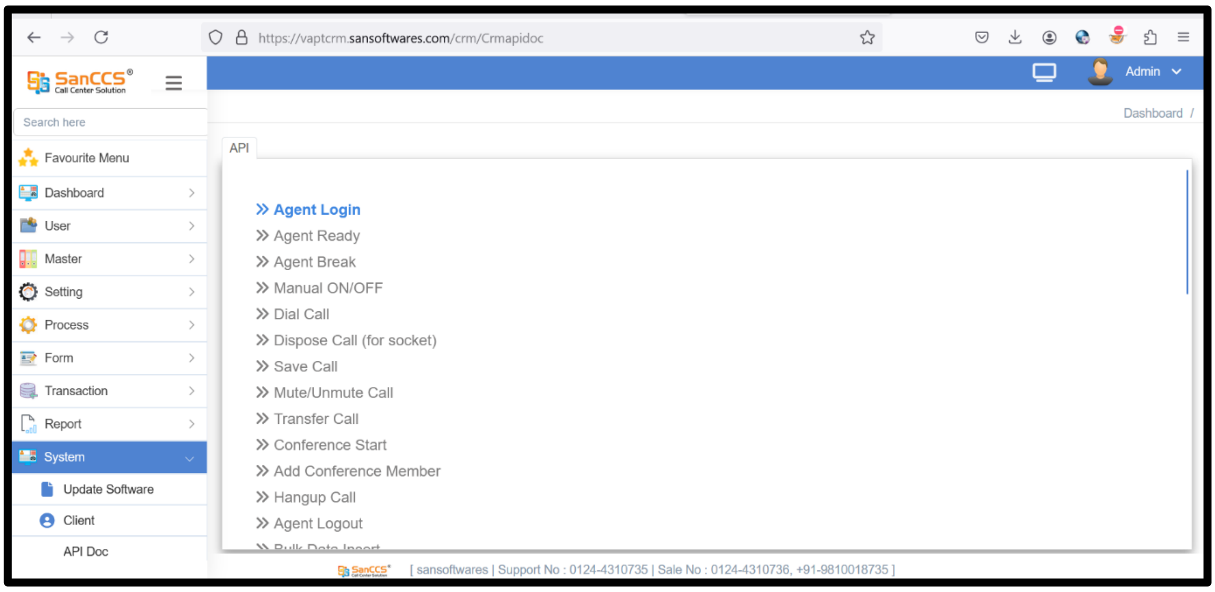
Name* :

Background Gradient 1* : FFFFFF

Background Gradient 2* : FFFFFF

Text Color* : 000000

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

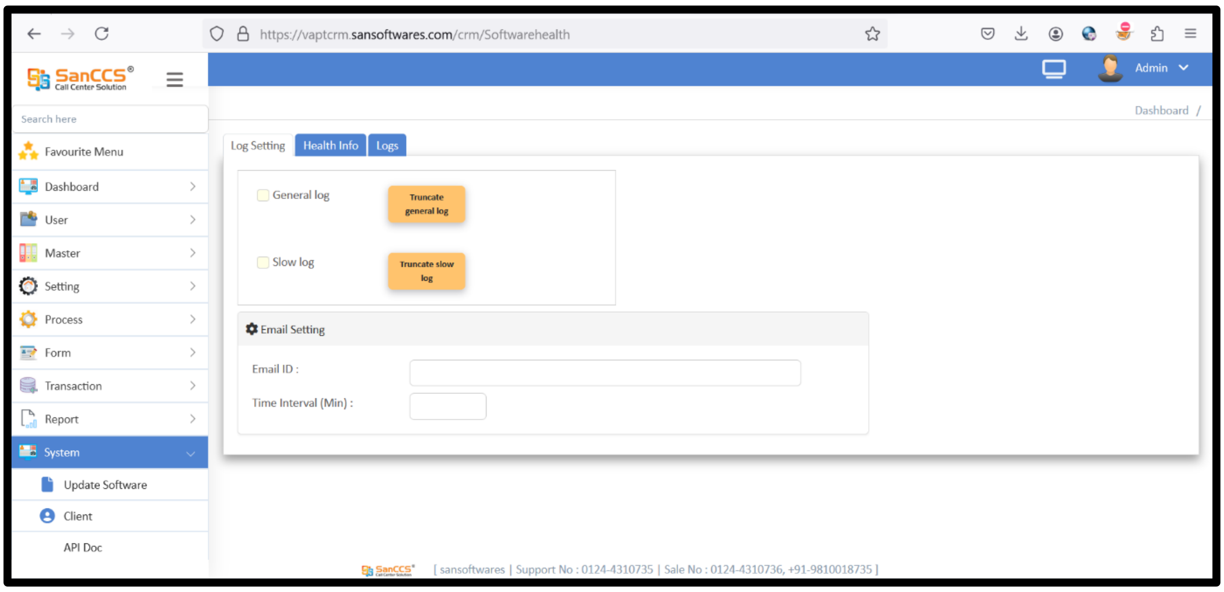


https://vaptcrm.sansoftwares.com/crm/Crmapidoc

API

- » **Agent Login**
- » Agent Ready
- » Agent Break
- » Manual ON/OFF
- » Dial Call
- » Dispose Call (for socket)
- » Save Call
- » Mute/Unmute Call
- » Transfer Call
- » Conference Start
- » Add Conference Member
- » Hangup Call
- » Agent Logout
- » Bulk Data Insert

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



https://vaptcrm.sansoftwares.com/crm/Softwarehealth

□ General log

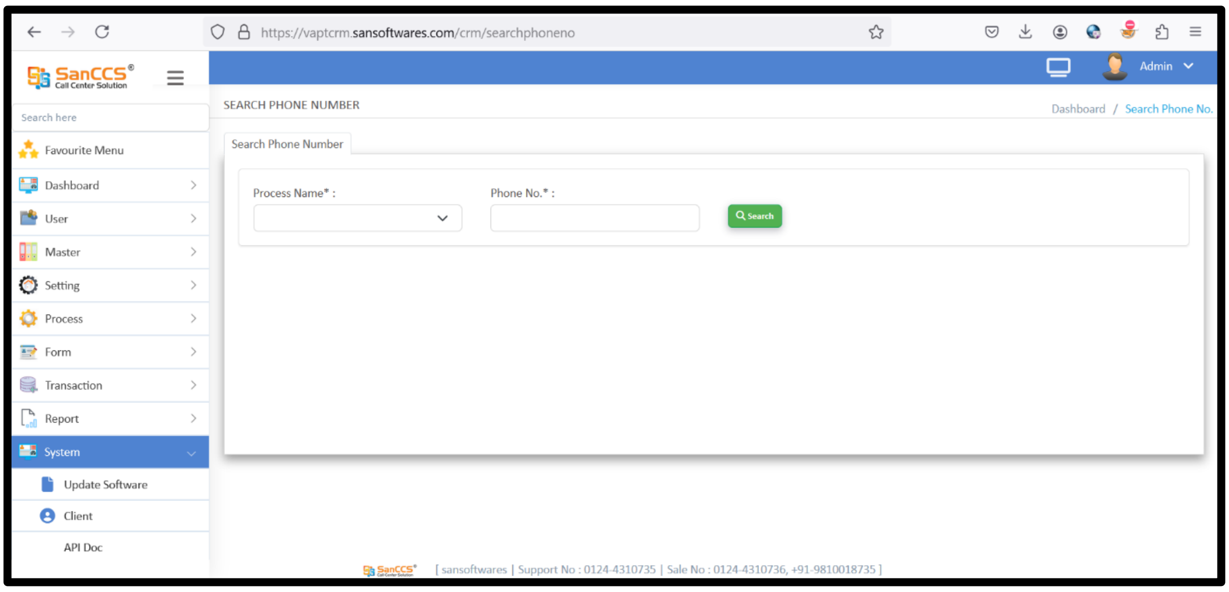
□ Slow log

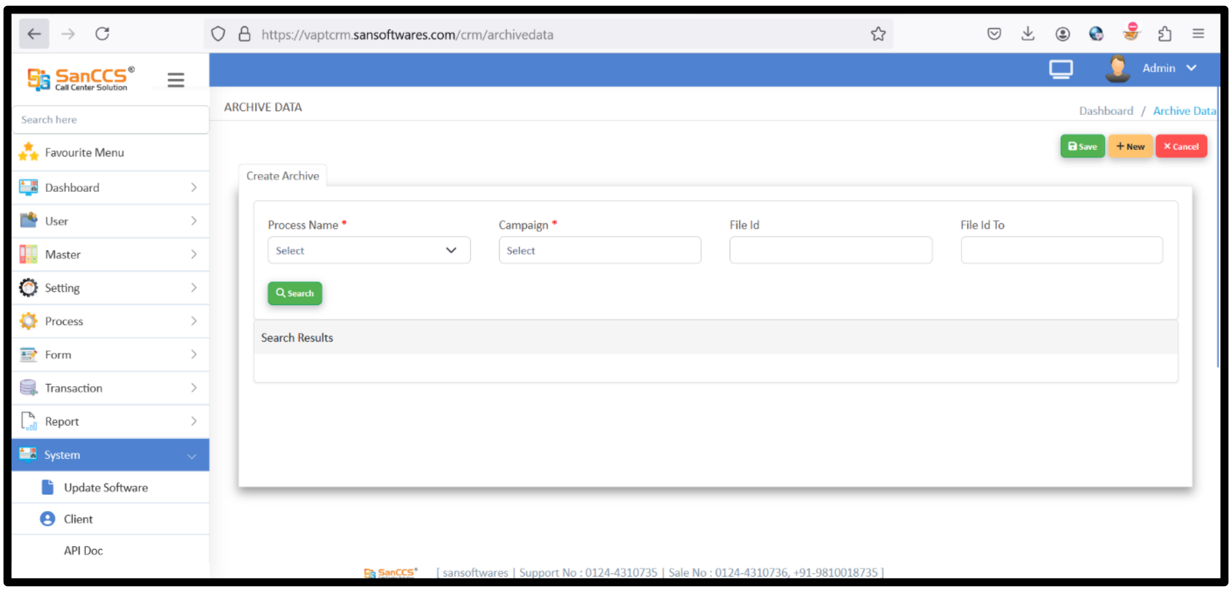
Email Setting

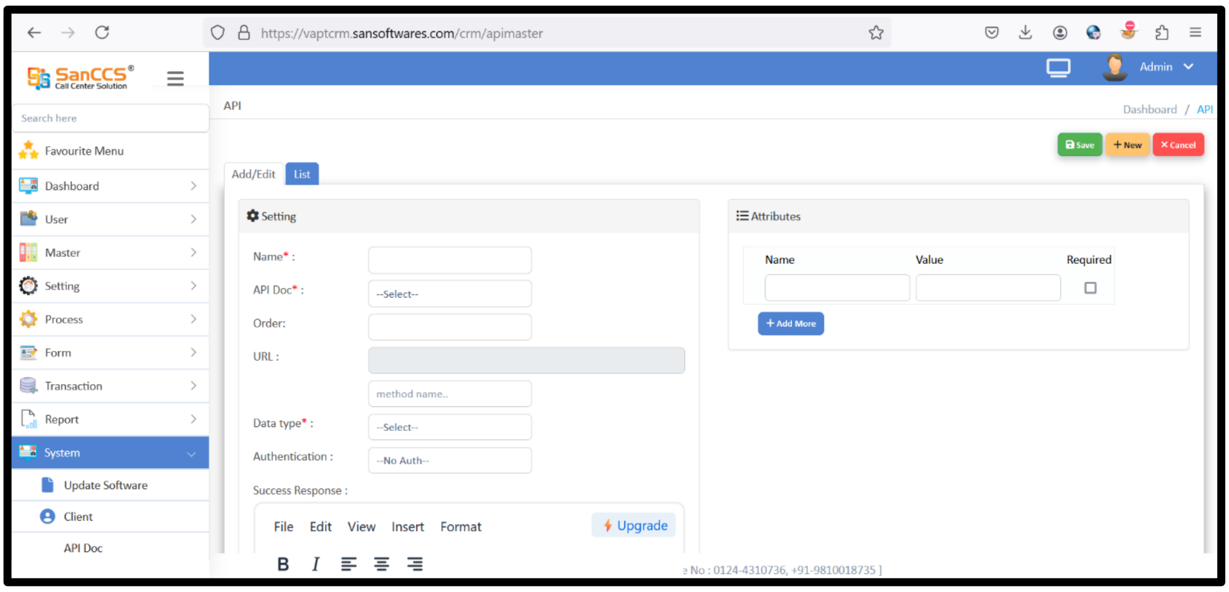
Email ID :

Time Interval (Min) :

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/searchphoneno
SanCCS® Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Setting
Process
Form
Transaction
Report
System
Update Software
Client
API Doc
SEARCH PHONE NUMBER
Dashboard / Search Phone No.
Search Phone Number
Process Name* :
Phone No.* :
Search
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]


https://vaptcrm.sansoftwares.com/crm/archivedata
SanCCS® Call Center Solution
Admin
Search here
Favourite Menu
Dashboard
User
Master
Setting
Process
Form
Transaction
Report
System
Update Software
Client
API Doc
ARCHIVE DATA
Dashboard / Archive Data
Save
+ New
× Cancel
Create Archive
Process Name *
Select
Campaign *
Select
File Id
File Id To
Search
Search Results
[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



API

Setting

Name* :

API Doc* : --Select--

Order:

URL :

method name..

Data type* : --Select--

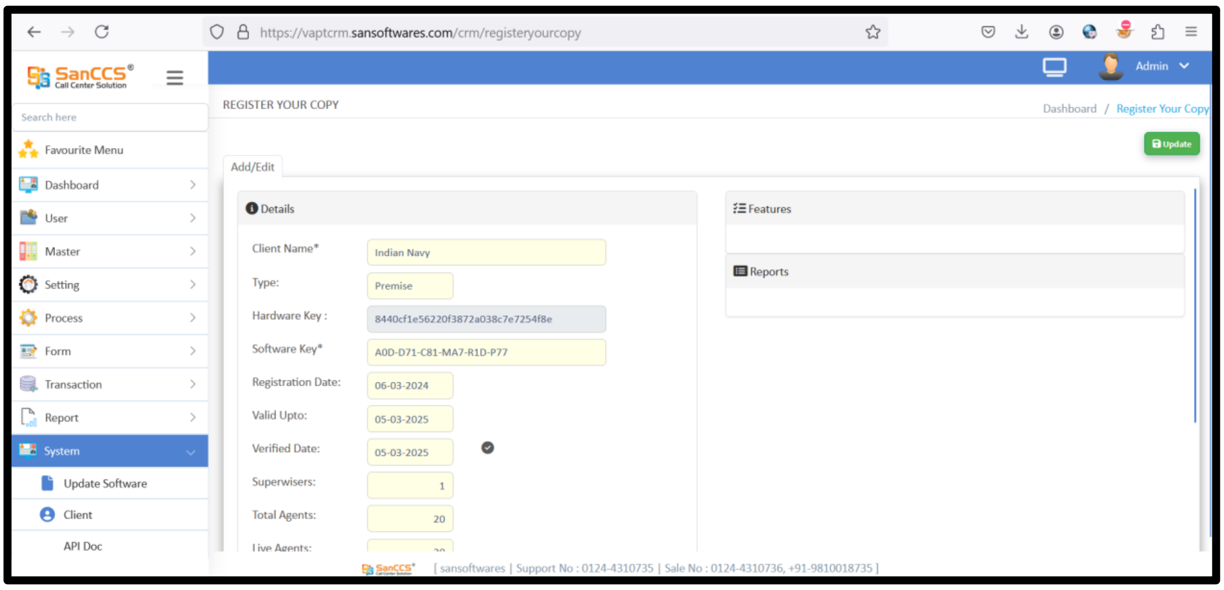
Authentication : --No Auth--

Success Response :

Attributes

Name	Value	Required
		□

No : 0124-4310736, +91-9810018735]



REGISTER YOUR COPY

Details

Client Name* Indian Navy

Type: Premise

Hardware Key : 8440cf1e56220f3872a038c7e7254f8e

Software Key* A0D-D71-C81-MA7-R1D-P77

Registration Date: 06-03-2024

Valid Upto: 05-03-2025

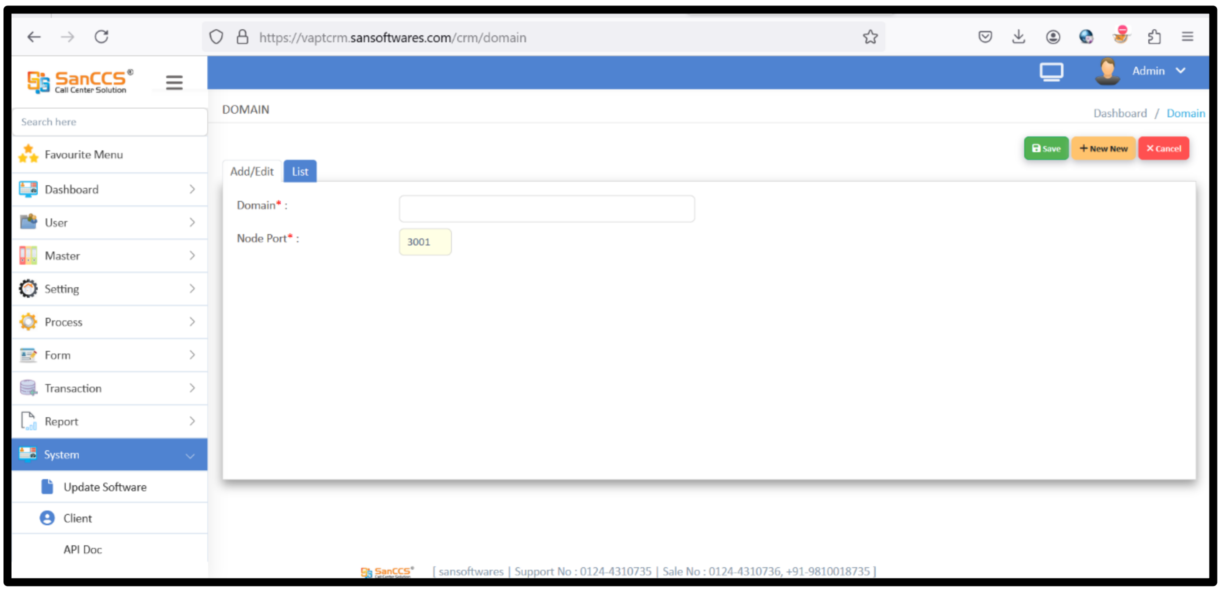
Verified Date: 05-03-2025 ✓

Superwisers: 1

Total Agents: 20

Live Agents: 20

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



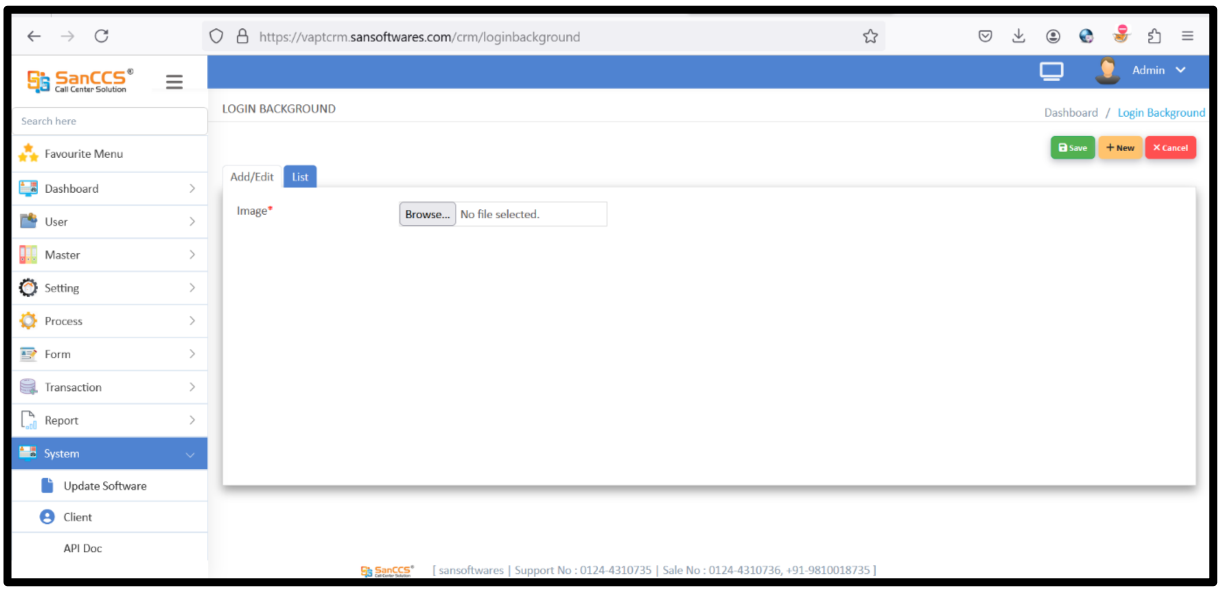
https://vaptcrm.sansoftwares.com/crm/domain

DOMAIN

Domain* :

Node Port* : 3001

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]

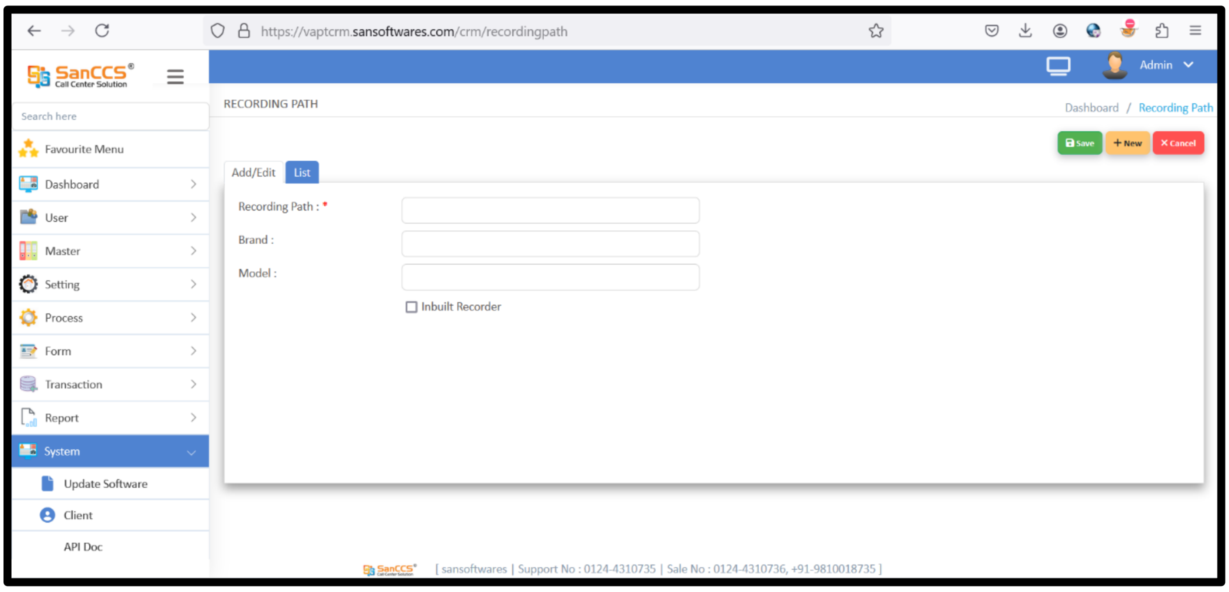


https://vaptcrm.sansoftwares.com/crm/loginbackground

LOGIN BACKGROUND

Image* Browse... No file selected.

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



RECORDING PATH

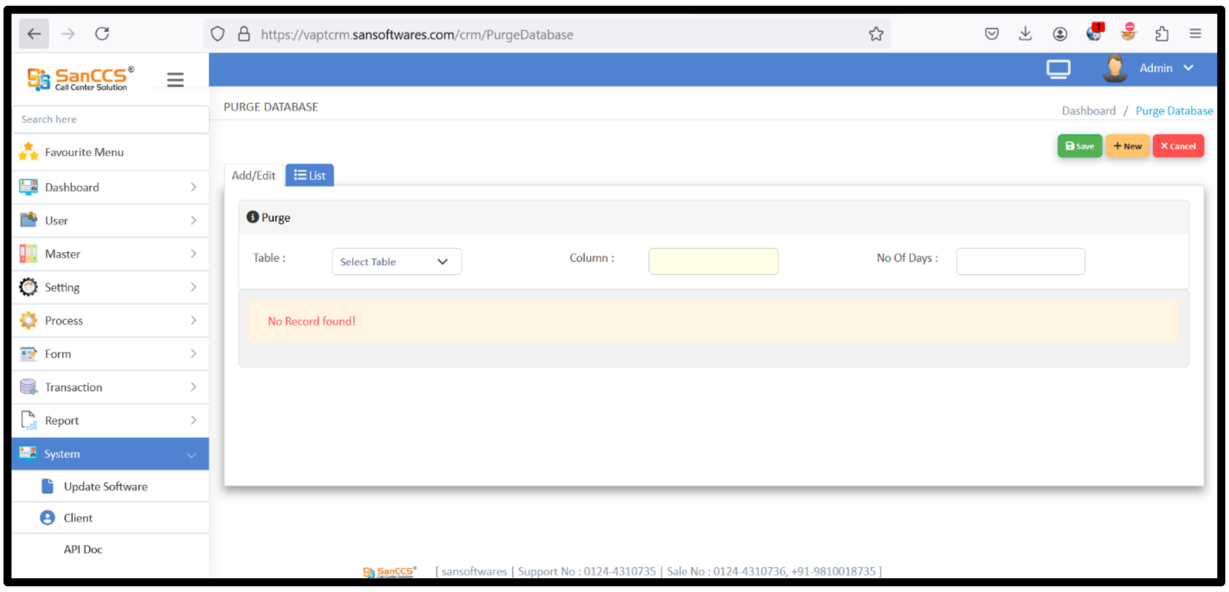
Recording Path : *

Brand :

Model :

□ Inbuilt Recorder

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



PURGE DATABASE

Purge

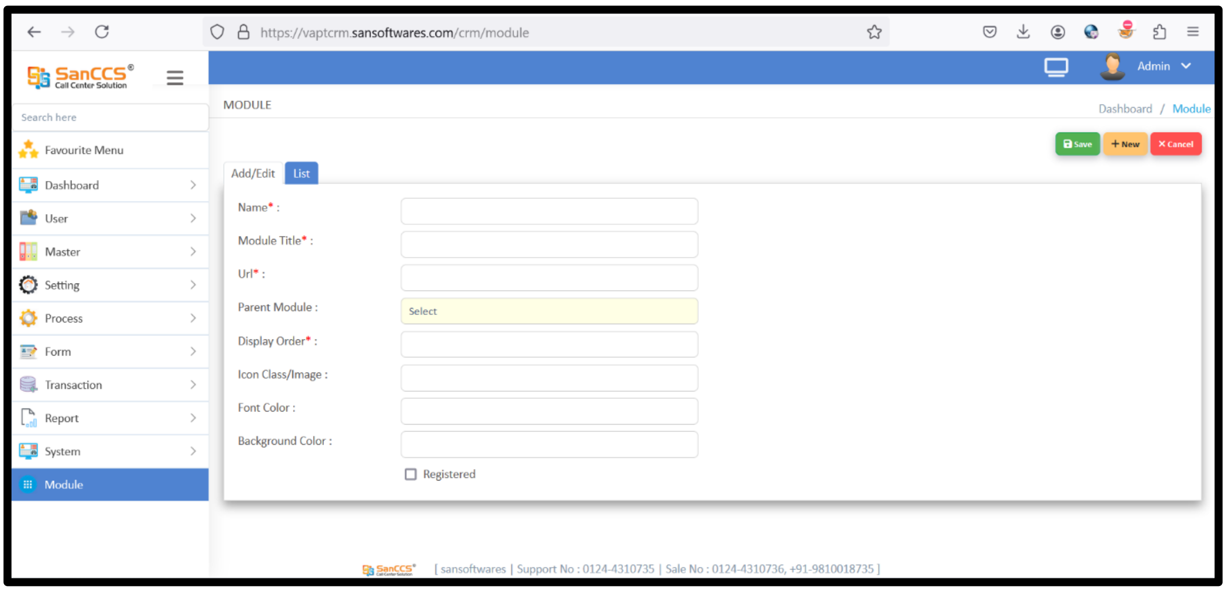
Table : Select Table

Column :

No Of Days :

No Record found!

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



MODULE

Name* :

Module Title* :

Url* :

Parent Module : Select

Display Order* :

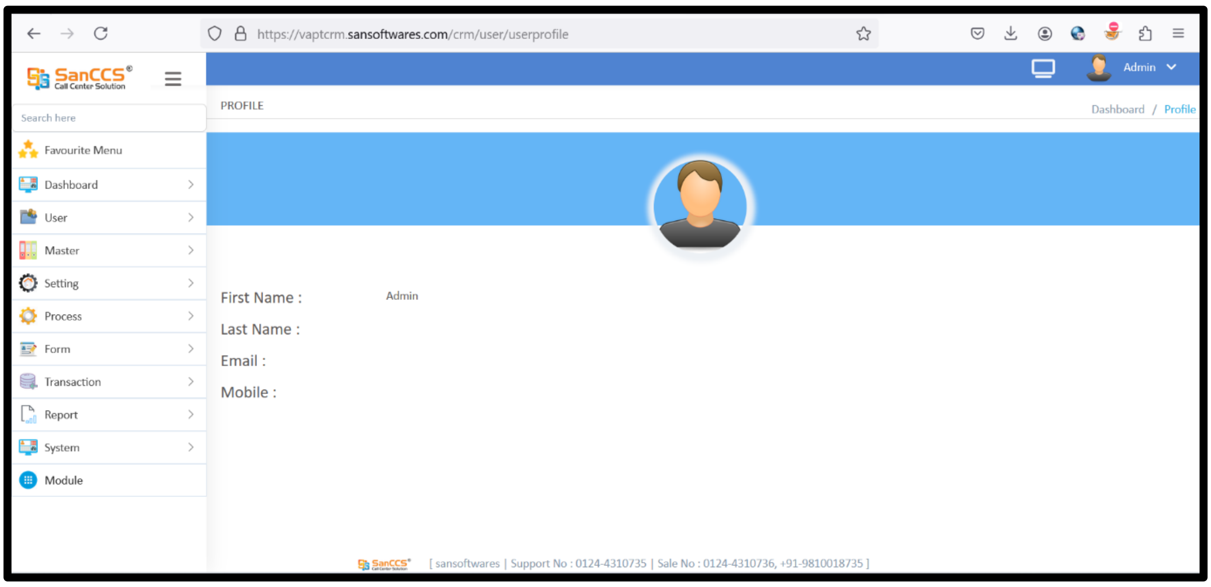
Icon Class/Image :

Font Color :

Background Color :

☐ Registered

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



PROFILE

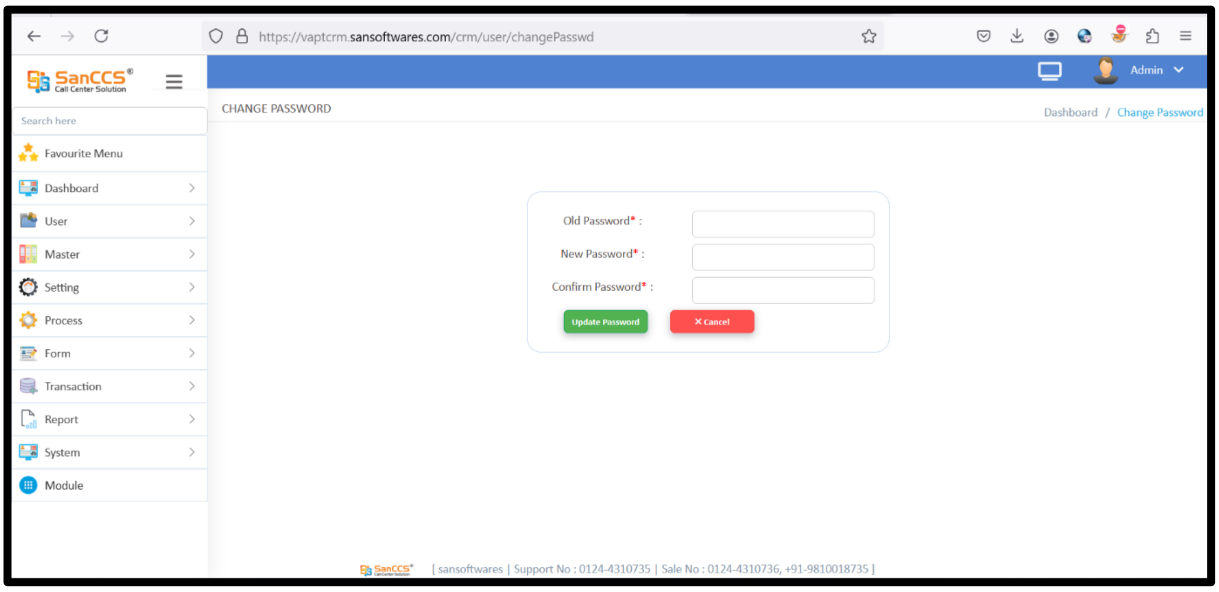
First Name : Admin

Last Name :

Email :

Mobile :

[sansoftwares | Support No : 0124-4310735 | Sale No : 0124-4310736, +91-9810018735]



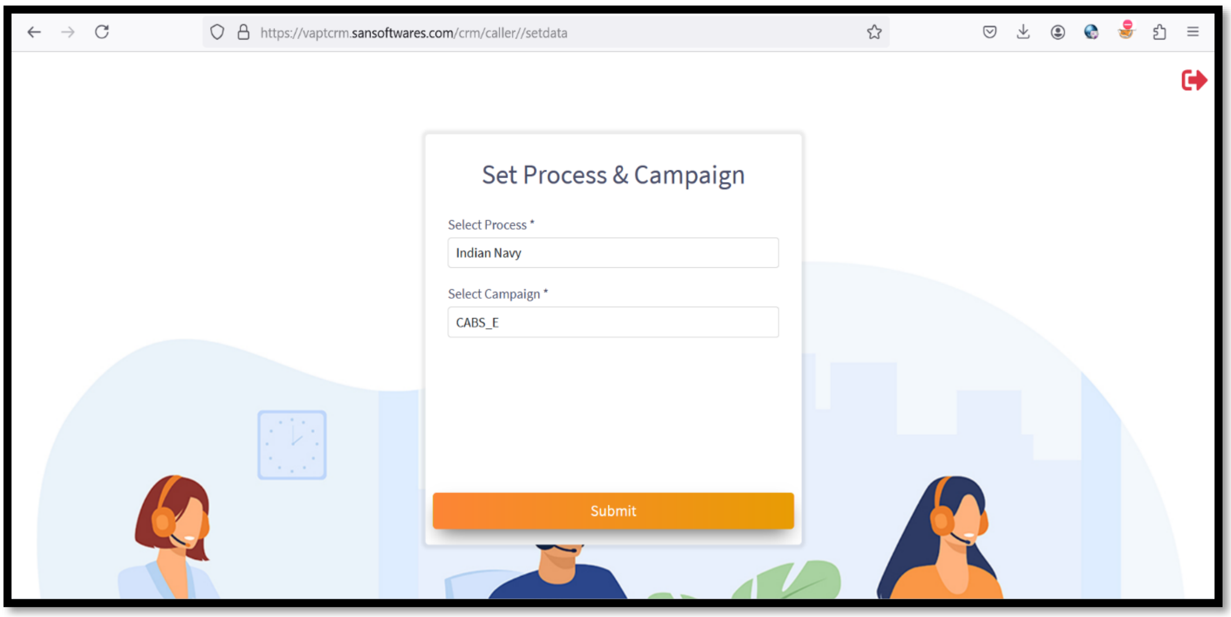
https://vaptcrm.sansoftwares.com/crm/user/changePasswd

CHANGE PASSWORD

Old Password* :

New Password* :

Confirm Password* :

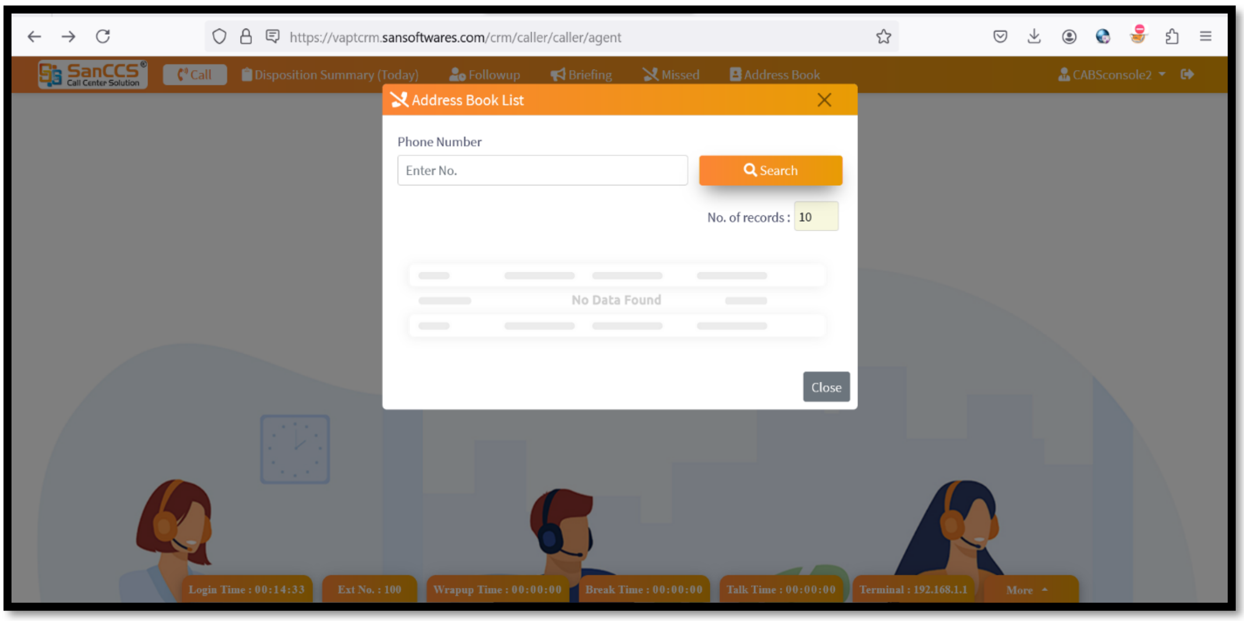


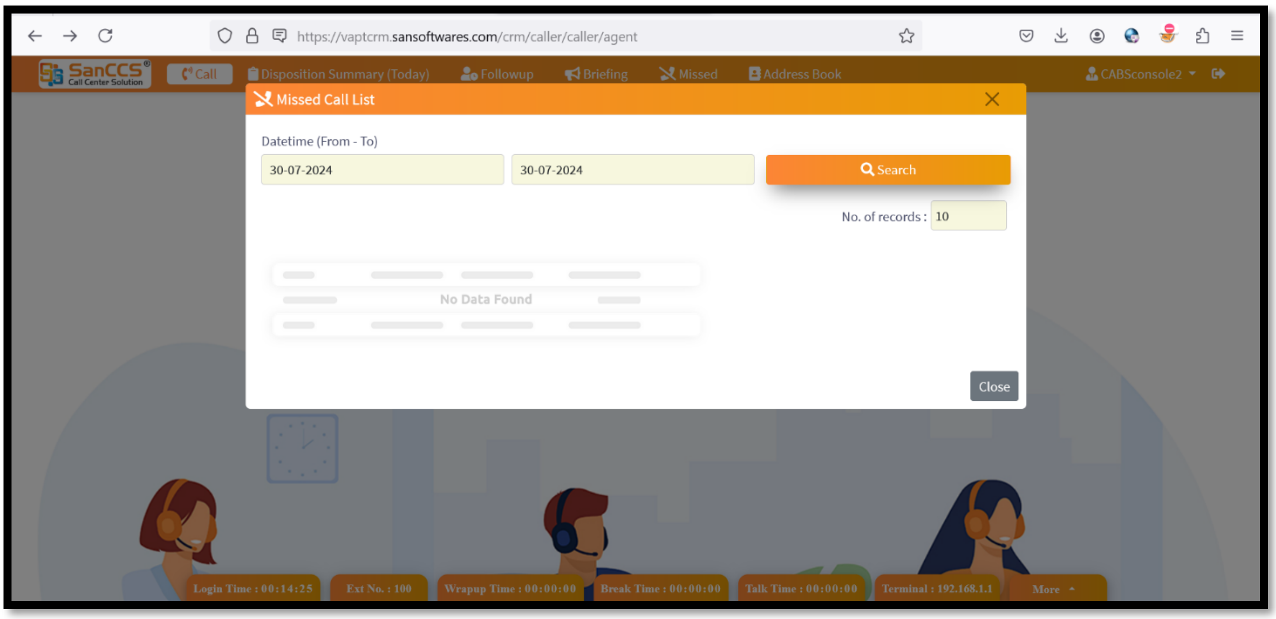
https://vaptcrm.sansoftwares.com/crm/caller//setdata

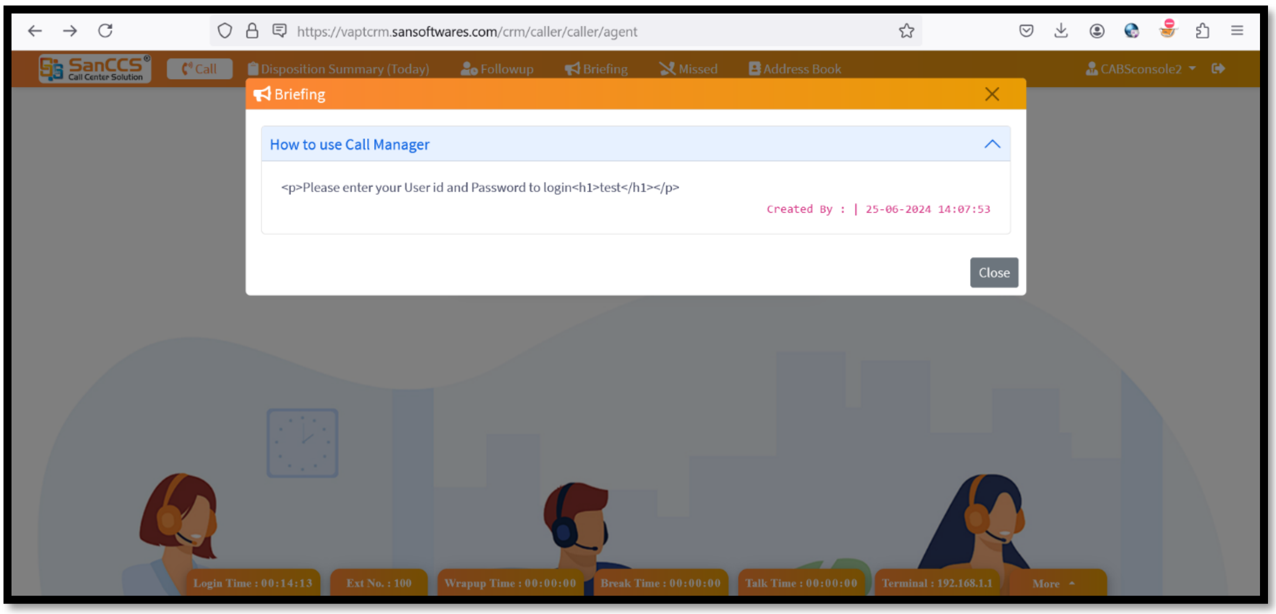
Set Process & Campaign

Select Process *: Indian Navy

Select Campaign *: CABS_E


https://vaptcrm.sansoftwares.com/crm/caller/caller/agent
SanCCS Call Center Solution
Call
Disposition Summary (Today)
Followup
Briefing
Missed
Address Book
CABSconsole2
Address Book List
Phone Number
Enter No.
Search
No. of records : 10
No Data Found
Close
Login Time : 00:14:33
Ext No. : 100
Wrapup Time : 00:00:00
Break Time : 00:00:00
Talk Time : 00:00:00
Terminal : 192.168.1.1
More


https://vaptcrm.sansoftwares.com/crm/caller/caller/agent
SanCCS Call Center Solution
Call
Disposition Summary (Today)
Followup
Briefing
Missed
Address Book
CABSconsole2
Missed Call List
Datetime (From - To)
30-07-2024
30-07-2024
Search
No. of records : 10
No Data Found
Close
Login Time : 00:14:25
Ext No. : 100
Wrapup Time : 00:00:00
Break Time : 00:00:00
Talk Time : 00:00:00
Terminal : 192.168.1.1
More



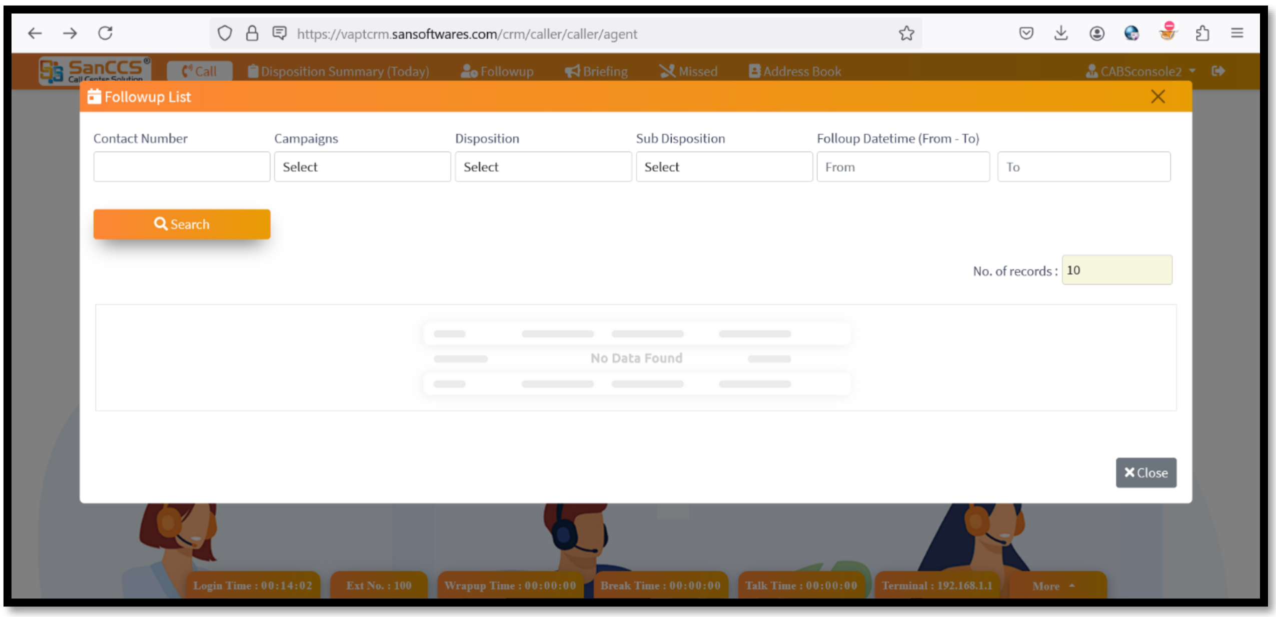
https://vaptcrm.sansoftwares.com/crm/caller/caller/agent

Briefing

How to use Call Manager

<p>Please enter your User id and Password to login<h1>test</h1></p>

Created By : | 25-06-2024 14:07:53



https://vaptcrm.sansoftwares.com/crm/caller/caller/agent

Followup List

Contact Number

Campaigns: Select

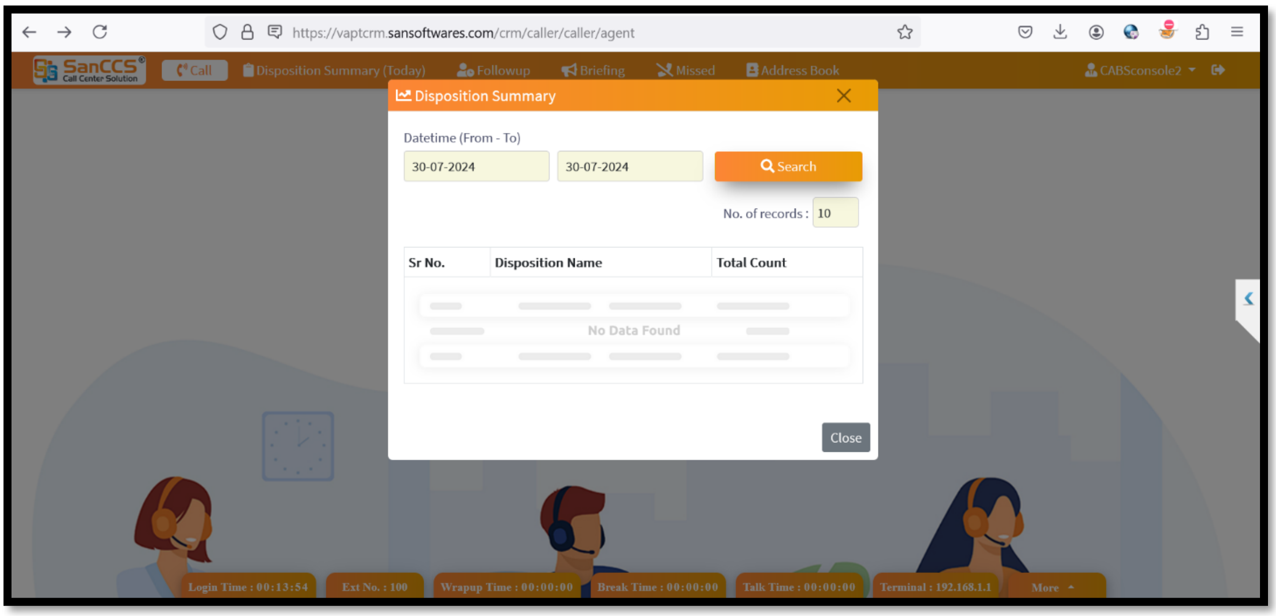
Disposition: Select

Sub Disposition: Select

Folloup Datetime (From - To): From To

No. of records : 10

No Data Found


https://vaptcrm.sansoftwares.com/crm/caller/caller/agent
SanCCS Call Center Solution
Call
Disposition Summary (Today)
Followup
Briefing
Missed
Address Book
CABSconsole2
Disposition Summary
Search
Close
More

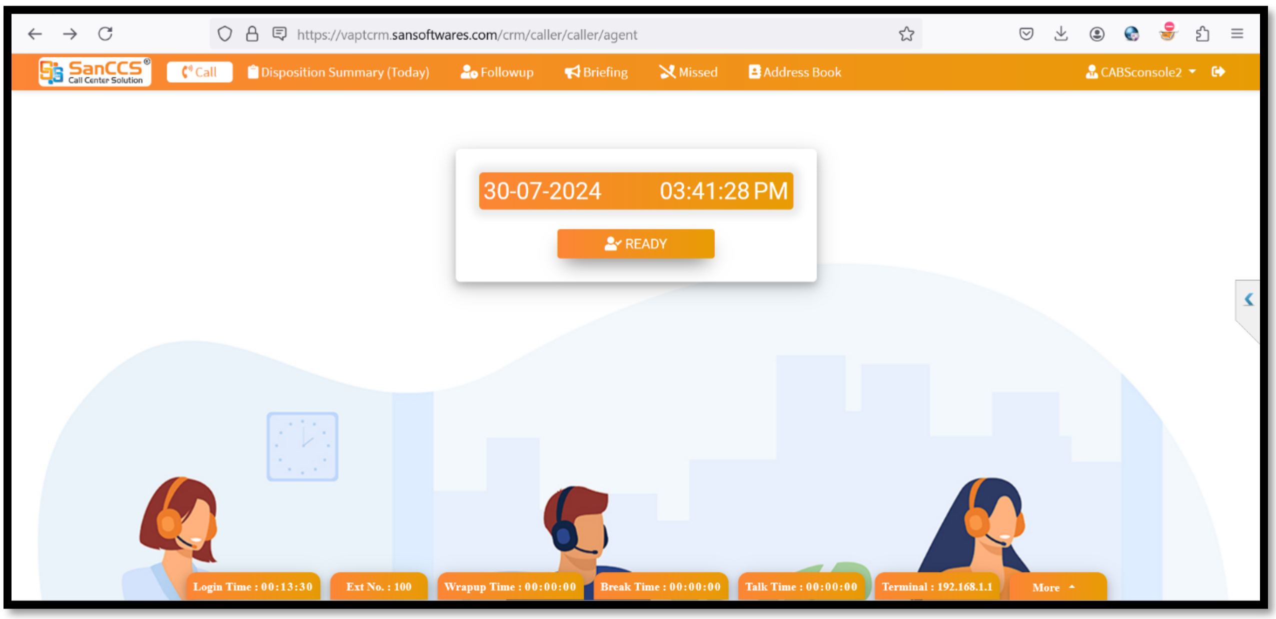
Datetime (From - To)

30-07-2024 | 30-07-2024

No. of records : 10

Sr No.	Disposition Name	Total Count
	No Data Found	

Login Time : 00:13:54 | Ext No. : 100 | Wrapup Time : 00:00:00 | Break Time : 00:00:00 | Talk Time : 00:00:00 | Terminal : 192.168.1.1


https://vaptcrm.sansoftwares.com/crm/caller/caller/agent
SanCCS Call Center Solution
Call
Disposition Summary (Today)
Followup
Briefing
Missed
Address Book
CABSconsole2
READY
More

30-07-2024 03:41:28 PM

Login Time : 00:13:30 | Ext No. : 100 | Wrapup Time : 00:00:00 | Break Time : 00:00:00 | Talk Time : 00:00:00 | Terminal : 192.168.1.1

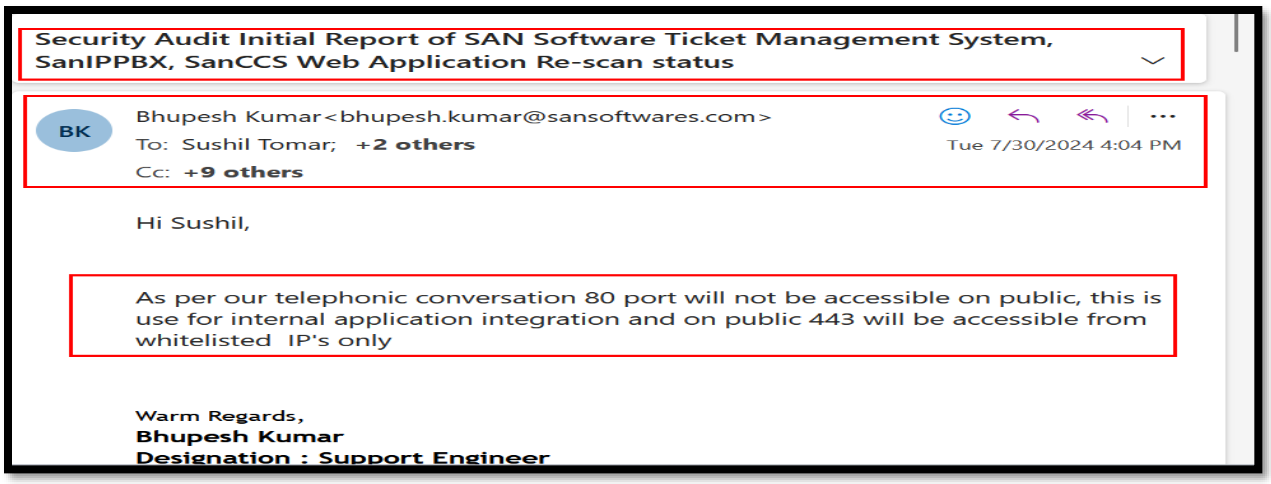
Annexure#1

Recommendation(s):

- Folder containing “JAVA” pages should be given “READ ONLY”.
- The following uploading folders to be given “READ and WRITE” permission.
  URL: /var/www/html/crm/upload
- Hosted equivalent of the following URL to be deployed over latest TLS:
  URL: https://vaptcrm.sansoftwares.com/crm/caller/
- Server and JAVA version should not be disclosed in the Response header of the application.
- Server and JAVA version should be stabled in the production environment.
- HTTP Security Headers should be implemented in the application before goes live in Production.

Note:

1. All the malicious scripts or data being saved into the database during the audit shall be removed once the site goes live.
2. If any modification in the application is made in the future the website should be subjected to the security audit as per the directives of Cert-In.
3. Screenshot has been attached for mail confirmation of Multiple port are open vulnerability.



Security Audit Initial Report of SAN Software Ticket Management System, SanIPPBX, SanCCS Web Application Re-scan status

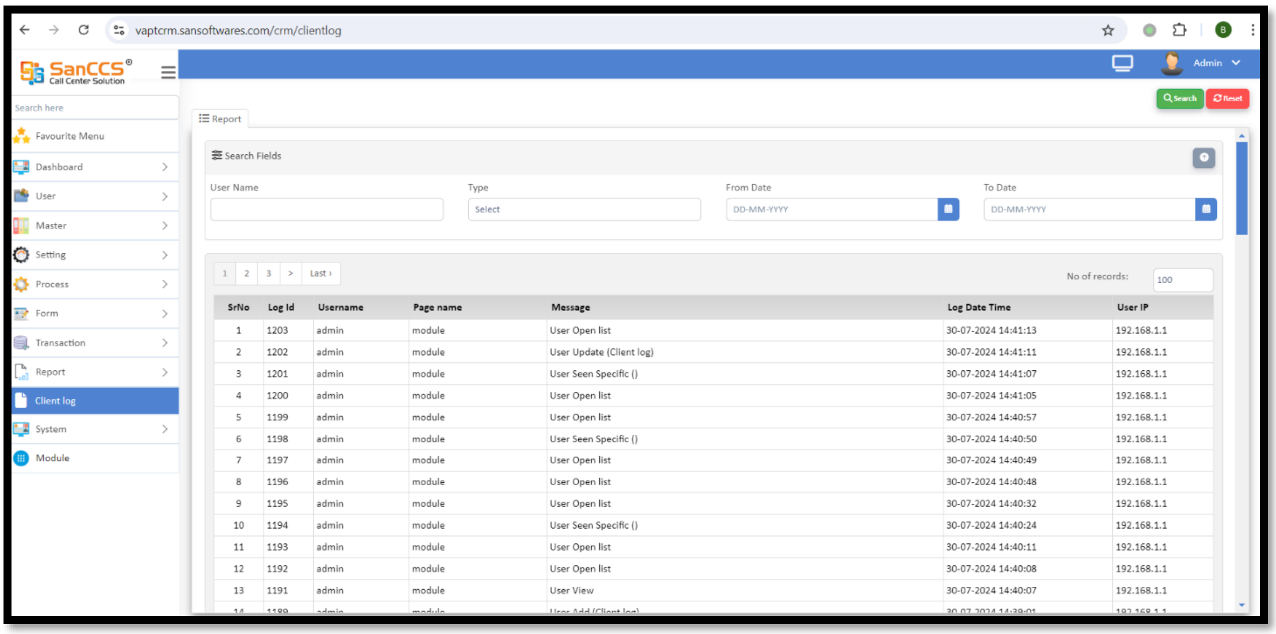
BK Bhupesh Kumar<bhupesh.kumar@sansoftwares.com>
To: Sushil Tomar; **+2 others**
Cc: **+9 others**
Tue 7/30/2024 4:04 PM

Hi Sushil,

As per our telephonic conversation 80 port will not be accessible on public, this is use for internal application integration and on public 443 will be accessible from whitelisted IP's only

Warm Regards,
Bhupesh Kumar
Designation : Support Engineer

4. Screenshot has been attached for Audit logs are maintained in the application.



User Name:

Type: Select

From Date: DD-MM-YYYY

To Date: DD-MM-YYYY

No of records: 100

SrNo	Log Id	Username	Page name	Message	Log Date Time	User IP
1	1203	admin	module	User Open list	30-07-2024 14:41:13	192.168.1.1
2	1202	admin	module	User Update (Client log)	30-07-2024 14:41:11	192.168.1.1
3	1201	admin	module	User Seen Specific ()	30-07-2024 14:41:07	192.168.1.1
4	1200	admin	module	User Open list	30-07-2024 14:41:05	192.168.1.1
5	1199	admin	module	User Open list	30-07-2024 14:40:57	192.168.1.1
6	1198	admin	module	User Seen Specific ()	30-07-2024 14:40:50	192.168.1.1
7	1197	admin	module	User Open list	30-07-2024 14:40:49	192.168.1.1
8	1196	admin	module	User Open list	30-07-2024 14:40:48	192.168.1.1
9	1195	admin	module	User Open list	30-07-2024 14:40:32	192.168.1.1
10	1194	admin	module	User Seen Specific ()	30-07-2024 14:40:24	192.168.1.1
11	1193	admin	module	User Open list	30-07-2024 14:40:11	192.168.1.1
12	1192	admin	module	User Open list	30-07-2024 14:40:08	192.168.1.1
13	1191	admin	module	User View	30-07-2024 14:40:07	192.168.1.1
14	1189	admin	module	User Add (Client log)	30-07-2024 14:39:01	192.168.1.1