

RESTRICTED
INTERIM REPORT

Tele: 39707

B/51106/ArCyGp/T-3/T&E/ E-ISAC

08 Nov 2024

DTE GEN OF MIL OPS
(ARMY CYBER GP)

CYBER SECURITY AUDIT OF WEB APPL: ENTERPRISE- INDIAN ARMY SECURE
ACCESS CARD APPL (E-ISAC)

1. Ref the fwg: -
 - (a) ACG note No B/51106/ArCyGp/T-3/T&E/ E-ISAC dt 05 Nov 2024.
 - (b) ACG note No B/51106/ArCyGp/T-3/T&E/ E-ISAC dt 28 Oct 2024.
 - (c) ASDC note No 1705005/AFSAC/03566/SDG/ASDC dt 18 Oct 2024.
 - (d) ACG letter No B/51106/ArCyGp/T-3/T&E/Adv1 dt 24 Aug 2023.
2. The VDI of the web appl “**E-ISAC**” handed over to ACG after initial config by developer rep on 01 Nov 2024 was analysed for cyber security compliance as per the dirns laid down in the Army Cyber Security Policy (ACSP)-2023.
3. Detls of vulnerabilities obs during current iteration are as under: -
 - (a) **Open Ports.** A No of open ports were detected on the web server. The screenshot for the same is att as **Appx A. Suggested mitigation methodology is to block all other ports except the port used by web server by implementing firewall rules.**
 - (b) **Improper RBAC leading to Privilege Escalation.** It has been obs that RBAC has not been properly impl in the appl. In the present state, a non-admin user can update profile of an admin user. Screenshot is att at **Appx B. It is strongly ‘R’ to impl RBAC on all modules incl in the appl as per envisaged role of regd users.**
 - (c) **Password Type Input with Autocomplete not Disabled.** The user end web browser has the built-in functionality of remembering user input in the form of username and password. Screenshot of the same is att as **Appx C.** This functionality results in storage/ caching of vital user credentials on the client machine (browser cache) and the same can be subsequently exploited. In the ibid application, autocomplete functionality for Password has not been set to off. Suggested mitigation methodology is to disable this functionality wherein the option of password auto complete is not avbl to the user.
 - (d) **Simultaneous Multiple Logins.** In its present state, the appl has not been configured to ensure unique login of users. This is exhibited by the ability of a user/ admin to login into the sys from multiple devices simultaneously. Screenshot of the same is at **Appx D.** To ensure the requisite std of cyber security, **it is strongly recom that the login of user credentials be restd to a single instance only. The latest session established with a particular user ID should be maintained and all previous sessions should be terminated.**

RESTRICTED

(e) **Non-Functional Modules/ links.** It is obs within the web appl that some of the modules/ links are non-functional. "Fetch Data from DB" while applying for new I-card is not functional in the appl. The screenshot is att at **Appx E**. Suggested mitigation methodology is to carry out appl wide mitigation of similar vulnerabilities and all modules/ functionalities linked with the appl as per its final dply.

(f) **Data Validation.** It is obs that server error msg is being generated by the web appl on supplying malformed inputs which indicates presence of faulty appl code. Screenshot is att at **Appx F**. Necessary controls wrt user input validation have not been impl within the subject web appl. **It is 'R' to validate the input fds against type, length, format and rg of data and iden and correct all such instances of code.**

(g) **Body Parameters Accepted in Query.** It is obs that body parameters are accepted in the URL within the devp web appl. List of URLs is att as **Appx G**. Attacking query parameters sent via GET requests is easier than body parameters sent via POST requests. Suggested mitigation methodology is to use POST requests to submit data to the appl and to ensure that body parameters sent via query string are not accepted by the appl.

(h) **Non-Encryption of Data at Rest.** In present status Army No, Mobile Nos etc are being stored in clear format in the database. The screenshot of the same is att as **Appx H**. **Suggested mitigation methodology is to ensure that all sensitive data is identified and secured at rest with latest secure encryption methods.**

(j) **System Administrator Acct Config.** Default System Admin acct 'sa' has been obs in the database. Screenshot is at as **Appx J**. The sysadmin acct is vulnerable in its default configuration as it can be exploited to perform unauth activities on the web appl database. **It is 'R' to rename the SA acct and to change the password for SA and other logins on a regular basis.**

(k) **Unused/ Commented Code.** It is obs that instances of unused code are present within the source code of the web appl. Screenshot is att at **Appx K**. **It is 'R' to remove the unused/ commented code and appl wide mitigation be undertaken.**

(l) **Misconfig Session Cookie.** It is observed that a dummy cookie named "MySecureCookie" with a default static value of "cookieValue" is being assigned to all users. Screenshot is att at **Appx L**. **It is 'R' to reconsider usage of ibid session cookie.**

4. Apropos, the fwg actions are requested to be undertaken by the sponsor/ developer: -

(a) Mitigation of all instances of aforementioned vulnerabilities in the appl.

(b) Post mitigation fwd vulnerability wise mitigation methodology alongwith screenshots for the better understanding of the Test Team.

(c) **Dummy Data.** The VDI submitted for lab test to be populated with dummy data for all roles (minimum two users each for CO, Adj, Records).

5. Ref letter mentioned at Para 1(d), sponsor should info the IP addr of the machine from where the remote mitigation of highlighted vulnerabilities will be undertaken so that the same can be whitelisted in the ACG firewall. **In the absence of intimation of any prog for three months from the date of issue of this letter, the website/appl Security Vetting case will be deemed to be closed.**

6. A Compendium of advisories is hosted at Army Cyber Gp on the link "*Web Development > Test & Eval Advisories*", as a ready reckoner, which will assist the developer in addressing the security issues in the website/ web appl. It is requested that same be ref to seek necessary assist. Also, a **mitigation asst desk** has been est at Army Cyber Gp where the developer rep can clarify any issues in the VA report and undertake in-situ mitigation of vulnerabilities.

7. For info and necessary action pl.

Sd/x-x-x-x-x-
(Manmeet Singh)
Lt Col
Staff Offr
for Cdr

Encls. As above

ASDC

Copy to: -







DGMO (MO-12) }
AFSAC Cell (DGMI/MI-11) } - For info pl.

<p><u>For any asst, pl contact</u> Appl Mitigation Asst Helpline No Army – 410000 39707 <u>For Appl vetting status visit</u> ACG website > Web/ Appl Devp > Web/ Appl Vetting Status</p>
--

Appx A

(Ref Para 3 (a) of Army Cyber Gp
letter No B/51106/ArCyGp/T-3/T&E
/E-ISAC dt 08 Nov 2024)

SCREENSHOT OF OPEN PORTS

	135	tcp	open
	139	tcp	open
	443	tcp	open
	2382	tcp	open
	3389	tcp	open
	5985	tcp	open

RESTRICTED

Appx B

(Ref Para 3 (b) of Army Cyber Gp letter No B/51106/ArCyGp/T-3/T&E /E-ISAC dt 08 Nov 2024)

SCREENSHOT OF IMPROPER RBAC LEADING TO PRIVILEGE ESCALATION

The screenshot shows the 'Enterprise IA Secure Access Card (E-ISAC)' interface. The user is logged in as COL AKASH DEEP (IC897878X). The 'Unit Mapping Details' section shows the user is mapped to Unit MP6, SUS No 1122334X, Comd SOUTHERN COMD, Corps No Corps, and Bde No Bde. The 'Domain Details' section shows the user is mapped to Domain ID mp6f_user1, Army No IC897878X, Role User, Appt COL (SIGS LIAISON), Mapped By Admin, and Mapped Date 03 October 2024. The 'Personal Information' section shows the user's Service No IC897, Rank Colonel, Name UPDATED BY ACG, Mobile No 8787484545, Army Contact No 2342, and Thumb Print 3422.

Unit Mapping Details			
Unit	MP6	SUS No	1122334X
Unit Type	Unit	Comd	SOUTHERN COMD
Corps	No Corps	Div	No Div
Bde	No Bde		

Domain Details			
Mapped Domain ID	mp6f_user1	Army No	IC897878X
Role	User	Appt	COL (SIGS LIAISON)
Mapped By	Admin	Mapped Date	03 October 2024

Personal Information			
Service No	IC897	Rank	Colonel
Mobile No	8787484545	Army Contact No	2342
Name	UPDATED BY ACG		
Thumb Print	3422		

Logged in as a Non-admin user and updating Profile

The screenshot shows the 'Enterprise IA Secure Access Card (E-ISAC)' interface. The user is logged in as CAPT UPDATED BY ACG (IC15692L). The 'Unit Mapping Details' section shows the user is mapped to Software Development Center, SUS No 1233334L, Comd THEARTRE COMD, Corps No Corps, and Bde No Bde. The 'Domain Details' section shows the user is mapped to Domain ID Admin, Army No IC15692L, Role Admin, Appt 2IC, Mapped By Admin, and Mapped Date 13 February 2024.

Unit Mapping Details			
Software Development Center	SUS No	1233334L	
	Comd	THEARTRE COMD	
Corps	Div	No Div	
Bde			

Domain Details			
Mapped Domain ID	Admin	Army No	IC15692L
Role	Admin	Appt	2IC
Mapped By	Admin	Mapped Date	13 February 2024

Profile of Admin User Updated by a Non-Admin User

Note :-

The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

Appx C

(Ref Para 3 (c) of Army Cyber Gp
letter No B/51106/ArCyGp/T-3/T&E
/E-ISAC dt 08 Nov 2024)

**SCREENSHOT OF PASSWORD TYPE INPUT WITH AUTOCOMPLETE NOT
DISABLED**

```
<div class="form-group">
  <label class="form-label fs-6" for="Password">Password</label>
  <input class="form-control" placeholder="Password" type="password" data-val="true" data-val-required="The Password field is required." id="Password"
  <span class="text-danger field-validation-valid" data-valmsg-for="Password" data-valmsg-replace="true"></span>
</div>
<input hidden type="password" data-val="true" data-val-equalto="Password and confirmation password do not match." data-val-equalto-other="*.Pas
<div class="text-center" >
  <button type="submit" class="btn btn-primary mt-2" onclick="return SubmitsEncry1(false)">Proceed</button>
</div>
```

Note :-

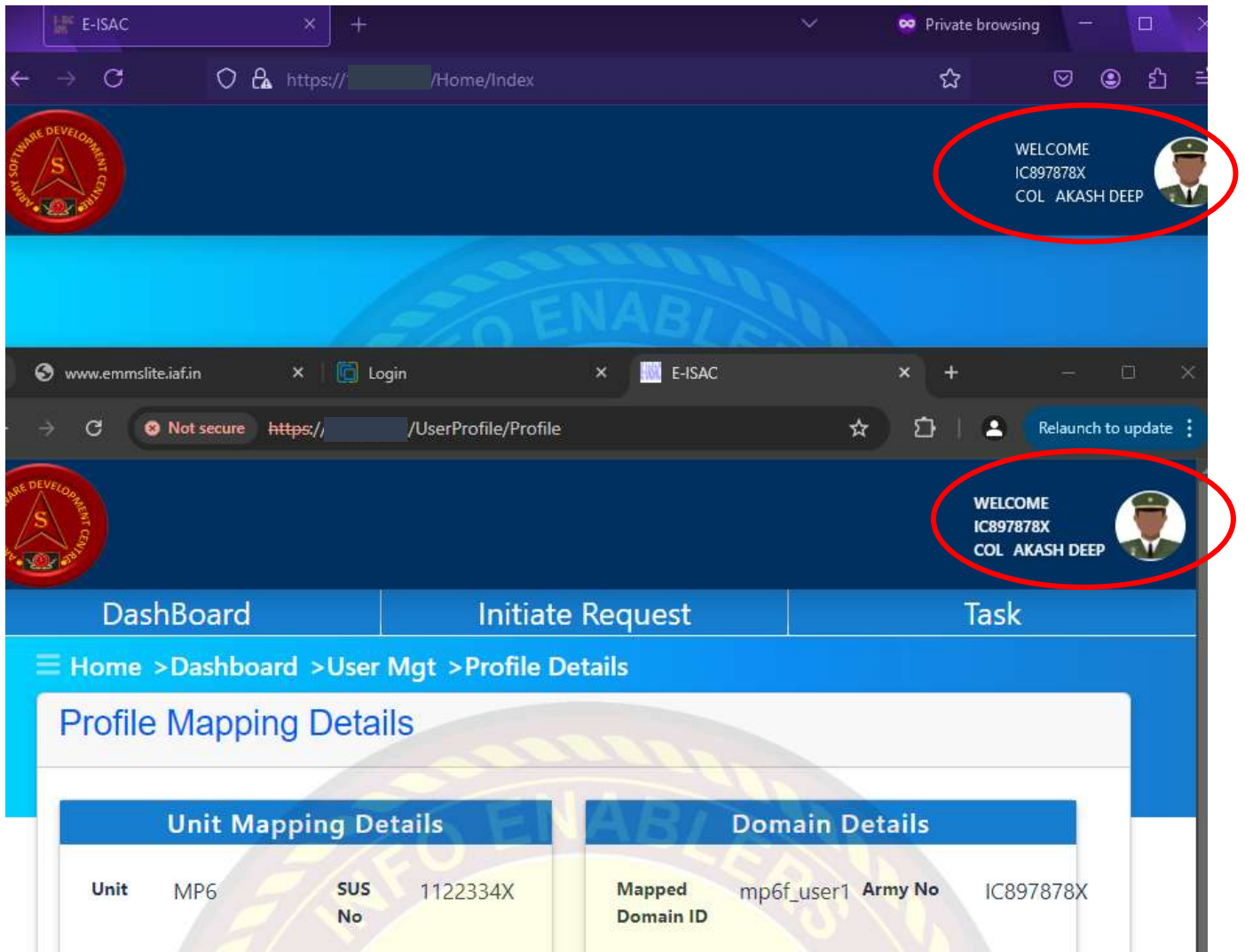
The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

RESTRICTED

Appx D

(Ref Para 3 (d) of Army Cyber Gp
letter No B/51106/ArCyGp/T-3/T&E
/E-ISAC dt 08 Nov 2024)

SCREENSHOT OF SIMULTANEOUS MULTIPLE LOGINS



Same User Logged in from two different clients

Note :-

The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

RESTRICTED

RESTRICTED

Appx E

(Ref Para 3 (e) of Army Cyber Gp
letter No B/51106/ArCyGp/T-3/T&E
/E-ISAC dt 08 Nov 2024)

SCREENSHOT OF NON-FUNCTIONAL MODULES/ LINKS

The screenshot displays a web application interface for an I-Card Application Request. The browser address bar shows the URL: <https://10.0.0.142/BasicDetail/Registration>. The page header includes a logo on the left, a welcome message "WELCOME IC897878X COL AKASH DEEP" on the right, and a red notification banner stating "Not Fetach Data From Api". The main navigation bar has three tabs: "DashBoard", "Initiate Request", and "Task". The "Initiate Request" tab is active, showing the "I-Card Appl Request For IC897878X" form. The form is divided into two main sections: "Requisition Details" and "Applicant Personal Particulars As Per Service Records".

Requisition Details

Logged in User Detls	Col Akash Deep (IC897878X) (mp6f_user1)	Category	Offrs
Unit Name	MP6 (1122334X)	Reason For Applying	First time Smart card

Applicant Personal Particulars As Per Service Records

Service No *	IC897878X	Fetch Data From DB
Rank *	Select Rank	

The "Fetch Data From DB" button is circled in red, indicating it is non-functional. A red notification banner at the top right of the form also states "Not Fetach Data From Api".

"Fetch Data from DB" button is not functional

Note :-

The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

RESTRICTED

RESTRICTED

Appx G

(Ref Para 3 (g) of Army Cyber Gp
letter No B/51106/ArCyGp/T-3/T&E
/E-ISAC dt 08 Nov 2024)

LIST OF AFFECTED URLs - BODY PARAMETERS ACCEPTED IN QUERY

Ser No	Affected URLs
1.	https://10.0.0.142/Home/Task
2.	https://10.0.0.142/UserProfile/Profile
3.	https://10.0.0.142/BasicDetail/ApprovalForIO
4.	https://10.0.0.142/Home/MyTask/SkNPc1BlbmRpbmc=
5.	https://10.0.0.142/Account/Profile
6.	https://10.0.0.142/Home/Request
7.	https://10.0.0.142/Home/GetDashboardCount
8.	https://10.0.0.142/Master/GetByApptId
9.	https://10.0.0.142/Master/GetALLByUnitMapId
10.	https://10.0.0.142/Master/GetAllMMaster
11.	https://10.0.0.142/UserProfile/GetByArmyNoOrAspnetuserId

Note :-

The above list is indicative only. Appl wide mitigation of this issue needs to be carried out.

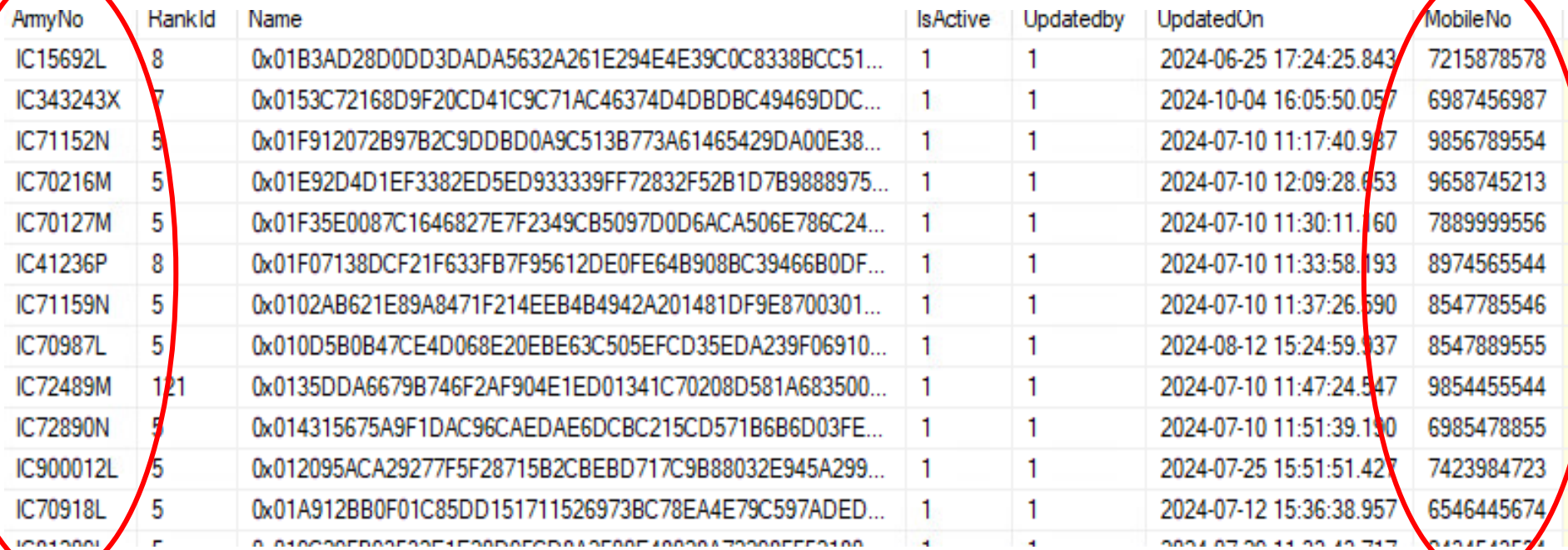
RESTRICTED

RESTRICTED

Appx H

(Ref Para 3 (h) of Army Cyber Gp letter No B/51106/ArCyGp/T-3/T&E /E-ISAC dt 08 Nov 2024)

SCREENSHOT OF NON-ENCRYPTION OF DATA AT REST



AmyNo	RankId	Name	IsActive	Updatedby	UpdatedOn	MobileNo
IC15692L	8	0x01B3AD28D0DD3DADA5632A261E294E4E39C0C8338BCC51...	1	1	2024-06-25 17:24:25.843	7215878578
IC343243X	7	0x0153C72168D9F20CD41C9C71AC46374D4DBDBC49469DDC...	1	1	2024-10-04 16:05:50.057	6987456987
IC71152N	5	0x01F912072B97B2C9DDBD0A9C513B773A61465429DA00E38...	1	1	2024-07-10 11:17:40.987	9856789554
IC70216M	5	0x01E92D4D1EF3382ED5ED933339FF72832F52B1D7B9888975...	1	1	2024-07-10 12:09:28.653	9658745213
IC70127M	5	0x01F35E0087C1646827E7F2349CB5097D0D6ACA506E786C24...	1	1	2024-07-10 11:30:11.160	7889999556
IC41236P	8	0x01F07138DCF21F633FB7F95612DE0FE64B908BC39466B0DF...	1	1	2024-07-10 11:33:58.193	8974565544
IC71159N	5	0x0102AB621E89A8471F214EEB4B4942A201481DF9E8700301...	1	1	2024-07-10 11:37:26.590	8547785546
IC70987L	5	0x010D5B0B47CE4D068E20EBE63C505EFCDD35EDA239F06910...	1	1	2024-08-12 15:24:59.937	8547889555
IC72489M	121	0x0135DDA6679B746F2AF904E1ED01341C70208D581A683500...	1	1	2024-07-10 11:47:24.547	9854455544
IC72890N	5	0x014315675A9F1DAC96CAEDAE6DCBC215CD571B6B6D03FE...	1	1	2024-07-10 11:51:39.190	6985478855
IC900012L	5	0x012095ACA29277F5F28715B2CBEED717C9B88032E945A299...	1	1	2024-07-25 15:51:51.427	7423984723
IC70918L	5	0x01A912BB0F01C85DD151711526973BC78EA4E79C597ADED...	1	1	2024-07-12 15:36:38.957	6546445674
IC01000L	5	0x0100...	1	1	2024-07-20 11:22:42.717	8121512554

'Army No' and 'Mobile Nos' are stored in plain text in Database

Note :-

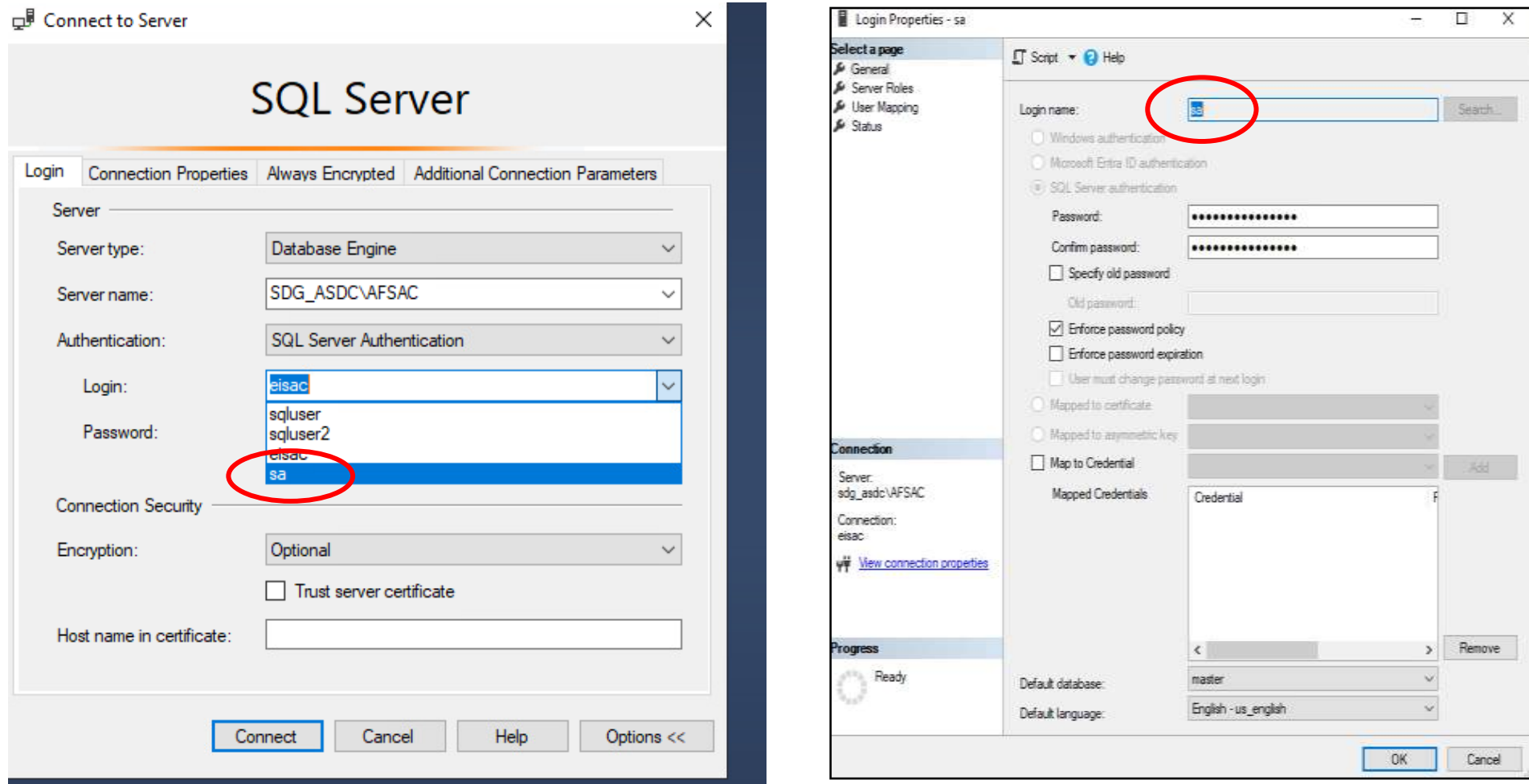
The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

RESTRICTED

Appx J

(Ref Para 3 (j) of Army Cyber Gp letter No B/51106/ArCyGp/T-3/T&E/E-ISAC dt 08 Nov 2024)

SCREENSHOT OF SYSTEM ADMINISTRATOR ACCT CONFIGURATION



Note :-

The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

Appx K

(Ref Para 3 (k) of Army Cyber Gp letter No B/51106/ArCyGp/T-3/T&E /E-ISAC dt 08 Nov 2024)

SCREENSHOT OF UNUSED/ COMMENTED CODE

```
//api:
//using (var client = new HttpClient())
//{
//    //client.BaseAddress = new Uri("https://api.postalpincode.in/");
//    client.BaseAddress = new Uri("https://localhost:7002/api/Fetch/GetData/");
//    //using (HttpResponseMessage response = await client.GetAsync("ICNumber/" + ICNumber))
//    using (HttpResponseMessage response = await client.GetAsync(ICNumber))
//    {
//        if (response.IsSuccessStatusCode)
//        {
//            var responseContent = response.Content.ReadAsStringAsync().Result;
//            response.EnsureSuccessStatusCode();
//            DTOApiResponse? responseData = JsonConvert.DeserializeObject<DTOApiResponse>(responseContent);
//            DateTime DOB, DOC;
//            TimeSpan timeSpan = new TimeSpan(0, 0, 0, 0, 0);
//            DOB = responseData.DOB.Date + timeSpan;
//            DOC = responseData.DateOfCommissioning.Date + timeSpan;
//            responseData.DOB = DOB;
//            responseData.DateOfCommissioning = DOC;
//            responseData.Status = true;
//            return Ok(responseData);
//        }
//        else
//        {
//            DTOApiResponse dtoApiResponse = new DTOApiResponse();
//            dtoApiResponse.Status = false;
//            dtoApiResponse.Message = "Data Not Found.";
//            return Ok(dtoApiResponse);
//        }
//    }
//}
```

```
//public async Task<IActionResult> AppStatus(string TrackingId)
//{
//    //DTOApplicationTrack dtoApplicationTrack=new DTOApplicationTrack();
//    //try
//    //{
//        dtoApplicationTrack = await _basicDetailBL.ApplicationHistory(TrackingId);
//        if (dtoApplicationTrack.dTOApplicationDetails != null)
//        {
//            ViewBag.IsData = 1;
//        }
//        else
//        {
//            ViewBag.IsData = 0;
//        }
//    }
//    //catch (Exception ex) {
//    //    ViewBag.IsData = 0;
//    //}
//    //return View(dtoApplicationTrack);
//    ViewBag.IP=HttpContext.Connection.RemoteIpAddress.MapToIPv4().ToString();
//    return View();
//}
```

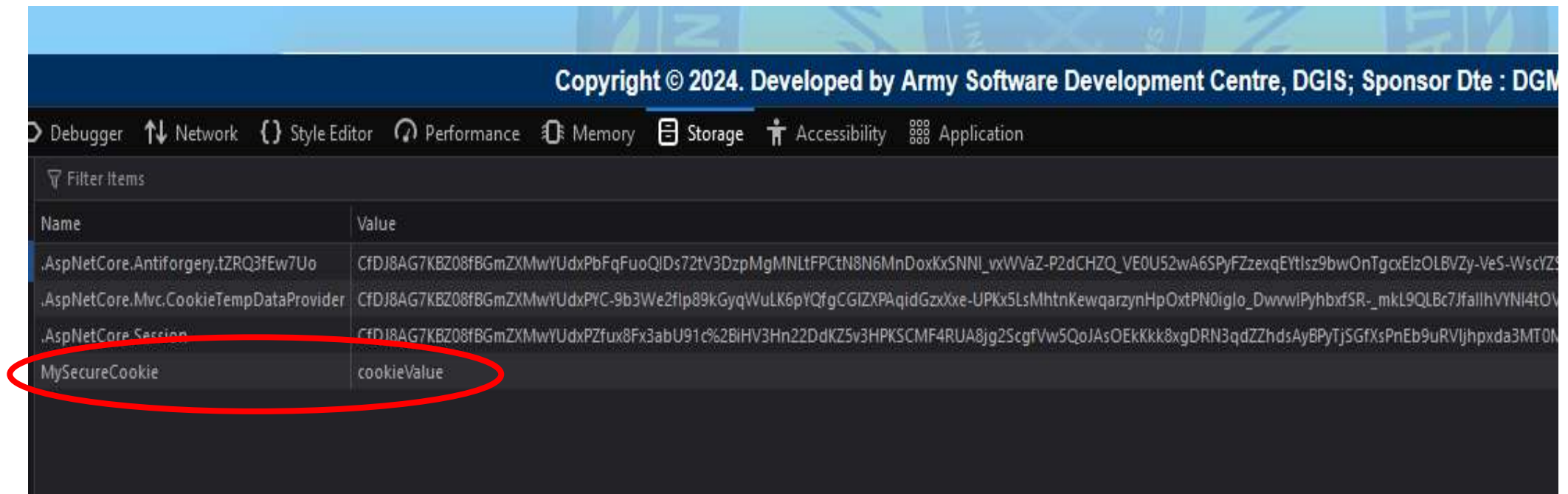
Note :-

The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

Appx L

(Ref Para 3 (I) of Army Cyber Gp letter No B/51106/ArCyGp/T-3/T&E /E-ISAC dt 08 Nov 2024)

SCREENSHOT OF MISCONFIG SESSION COOKIE



Note :-

The above screenshot is an indicative example only. Appl wide mitigation of this issue needs to be carried out.

RESTRICTED

RESTRICTED