E-Arogya - Bug #66

Feature # 65 (New): Security Audit

[Security Audit] 1- Privilege Escalation

17/04/2024 03:24 PM - Kalyan Battula

Status:	Closed	**Start date:**	17/04/2024
Priority:	High	**Due date:**	
Assignee:	Kranti Boddu	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

Privilege Escalation

CWE : CWE-269
Description :
Access control (or authorization) is the application of constraints on who (or what) can perform attempted actions or access resources that they have requested. In this context, application allows a user to access the resources which need to be protected.
Affected Path(s) :
https://earogya.satragroup.in/configuration/all_master *-Applicable to entire application
Impact :
The degree of escalation depends on what privileges the attacker is authorized to possess, and what privileges can be obtained in a successful exploit.
Recommendation :
It is recommended to implement role based access control at server side. Validate the user's cookies/authorization tokens at server side properly before providing access to any resource.
Evidence/Proof Of Concept :
Step 1: Login to the application with test1_dr credentials in in browser1 and test1_fd credentials in browser2.

Step 2: It is observed that there are different tabs in both logins as shown in below screenshot.

Step 3: Click on the edit tab in test1_fd login Copy the URL "https://earogya.satragroup.in/configuration/all_master"

Step 4: Click on the edit tab in test1_dr login Paste the URL "https://earogya.satragroup.in/configuration/all_master"
Step 5: Try to access the browser1 observed that test1_dr also able to access the same page as shown below screenshot.

---

clipboard-202404171521-irigs.png

clipboard-202404171522-6zgfz.png

clipboard-202404171523-1jsnj.png

clipboard-202404171523-okcmo.png

clipboard-202404171524-txmho.png

History

#1 - 17/04/2024 03:53 AM - Kalyan Battula

- Subject changed from [Security Audit] Privilege Escalation to [Security Audit] 1- Privilege Escalation

#2 - 21/04/2024 08:17 PM - Kranti Boddu

- Status changed from New to In Progress

- Assignee set to Kranti Boddu

#3 - 25/04/2024 03:30 AM - Kranti Boddu

- Status changed from In Progress to Resolved

#4 - 03/05/2024 05:24 AM - Sivakanth Kesiraju

- Target version set to Sprint 1 (29th April - 3rd May)

#5 - 03/05/2024 05:28 AM - Sivakanth Kesiraju

- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit

#6 - 30/09/2024 04:36 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171521-irigs.png	445 KB	17/04/2024	Kalyan Battula
clipboard-202404171522-6zgfz.png	64.9 KB	17/04/2024	Kalyan Battula
clipboard-202404171523-1jsnj.png	98.1 KB	17/04/2024	Kalyan Battula
clipboard-202404171523-okcmo.png	86.7 KB	17/04/2024	Kalyan Battula
clipboard-202404171524-txmho.png	110 KB	17/04/2024	Kalyan Battula