E-Arogya - Bug #69

Feature # 65 (New): Security Audit

[Security Audit] 4- User Account Takeover

17/04/2024 03:36 PM - Kalyan Battula

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

Description

4- User Account Takeover
CWE : CWE-285
Description :
The software does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.
Affected Path(s) :
https://earogya.satragroup.in/login *-Applicable to entire application
Impact :
An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Recommendation :
It is recommended to make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.
Evidence/Proof Of Concept :
Step 1: Access the application and go to forgot password page.Enter valid user then capture the request as shown in below screenshot.
clipboard-202404171535-tehk1.png

Step 2: Change userid 316 to 317 then forword the requet.Observe the response Password changed sucessfully with Modified user.
clipboard-202404171535-k8l7w.png

History

#1 - 17/04/2024 04:57 AM - Harish Beechani

- Assignee set to Vasudev Mamidi

#2 - 24/04/2024 12:06 AM - Pavan kumar Siddamsetti

- Status changed from New to In Progress

#3 - 24/04/2024 12:49 AM - Vasudev Mamidi

- 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 05:23 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171535-tehk1.png	48.2 KB	17/04/2024	Kalyan Battula

clipboard-202404171535-k8l7w.png	33.7 KB	17/04/2024	Kalyan Battula