E-Arogya - Bug #68

Feature # 65 (New): Security Audit

[Security Audit] 3-Broken Access Control

17/04/2024 03:33 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

Broken Access Control
CWE : CWE-425
Description :
The application allows an unauthenticated user to access the pages that should be accessible to the administrator only. This happens due to the improper implementation of access controls set by the application.
Affected Path(s) :
https://earogya.satragroup.in/change-password *-Applicable to entire application
Impact :
Attackers acting as users or administrators, or users using privileged functions have the ability of creating, accessing, updating or deleting every record.
Recommendation :
The default should always be denial.
Everyone should be denied access to everything, and then every specific role can be explicitly granted access for each function needed.
Log failed attempts to access features to make sure everything is configured correctly.
Reference:
https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control
Evidence/Proof Of Concept :
Step 1: In the application it was observed that certain internal pages were accessible to the end user with out any authentication.
clipboard-202404171532-uersf.png

History

#1 - 17/04/2024 03:55 AM - Kalyan Battula

- Subject changed from [Security Audit] Broken Access Control to [Security Audit] 3-Broken Access Control

#2 - 21/04/2024 09:30 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 04:35 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171532-uersf.png	432 KB	17/04/2024	Kalyan Battula