E-Arogya - Bug #77

Feature # 65 (New): Security Audit

[Security Audit] 12- OTP Bypass

17/04/2024 03:51 PM - Kalyan Battula

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

Description

12 -OTP Bypass
CWE : CWE-287
Description :
In this application OTP is disclosed in response.
Affected Path(s) :
https://earogya.satragroup.in/login *-Applicable to entire application
Impact :
Attacker can us e the OTP value to bypass the login without the actual user intervention
Recommendation :
It is recommended not to disclose the OTP in the response
Evidence/Proof Of Concept :
Step 1: Access the application and Go to forgot password page and enter random OTP as shown in below screenshot.
clipboard-202404171550-mtklz.png

Step 2: Successfully Navigate the password change page.
clipboard-202404171551-tbu68.png

Step 3: Capture the above request and Observe the response.New Password has been changed successfully even after entering the invalid OTP as shown in below screenshot.
clipboard-202404171551-lxzyq.png

History

#1 - 17/04/2024 04:21 AM - Harish Beechani

- Assignee set to Harish Beechani

#2 - 24/04/2024 12:46 AM - Vasudev Mamidi

- Status changed from New to Closed

#3 - 03/05/2024 05:28 AM - Sivakanth Kesiraju

- Target version set to Security Audit

Files

clipboard-202404171550-mtklz.png	569 KB	17/04/2024	Kalyan Battula
clipboard-202404171551-tbu68.png	553 KB	17/04/2024	Kalyan Battula
clipboard-202404171551-lxzyq.png	54.8 KB	17/04/2024	Kalyan Battula