E-Arogya - Feature #254

Feature # 235 (New): [Security Audit Round 2]

[Security Audit Round 2] OTP Bypass (Repeated)

01/05/2024 12:51 PM - Kalyan Battula

Status:	Closed	**Start date:**	01/05/2024
Priority:	High	**Due date:**	
Assignee:	Kalyan Battula	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

OTP Bypass (Repeated)
observation : Repeated
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
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-202405011248-oee8f.png

Step 2: Successfully Navigate the password change page
clipboard-202405011249-cnlo2.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-202405011249-cqemn.png

Step 4: Functionality issue
clipboard-202405011250-b1cy5.png
Recommendation :
It is recommended not to disclose the OTP in the response

History

#1 - 03/05/2024 05:27 AM - Sivakanth Kesiraju

- Target version set to Security Audit

#2 - 10/05/2024 06:14 AM - Harish Beechani

- Status changed from New to Resolved

#3 - 10/05/2024 06:18 AM - Harish Beechani

- Assignee set to Harish Beechani

#4 - 10/05/2024 07:16 AM - Harish Beechani

- Status changed from Resolved to Ready for Prod

#5 - 16/05/2024 04:53 AM - Kalyan Battula

- Status changed from Ready for Prod to Closed

- Assignee changed from Harish Beechani to Kalyan Battula

Now working fine throwing warning alert

Files

clipboard-202405011248-oee8f.png	479 KB	01/05/2024	Kalyan Battula
clipboard-202405011249-cnlo2.png	465 KB	01/05/2024	Kalyan Battula
clipboard-202405011249-cqemn.png	48.7 KB	01/05/2024	Kalyan Battula
clipboard-202405011250-b1cy5.png	430 KB	01/05/2024	Kalyan Battula