E-Arogya - Bug #82

Feature # 65 (New): Security Audit

[Security Audit]17 - OTP Bruteforce

17/04/2024 03:59 PM - Kalyan Battula

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

Description

17 - OTP Bruteforce
CWE : CWE-799
Description :
Application allows users to submit multiple wrong OTPs which lead to bruteforce attacks to guess the correct OTP.
Affected Path(s) :
https://earogya.satragroup.in/login *-Applicable to entire application
Impact :
Account takeover can be possible by using this vulnerability.
Recommendation :
It is recommended to allow only 3 to 5 wrong attempts of OTPs. After the limit block the mobile number for some time or provide a new OTP.
Evidence/Proof Of Concept :
Step 1: Application accepting multiple OTP requests which leads to brute force the OTP by submitting multiple requests.
clipboard-202404171559-juppf.png

History

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

- Assignee set to Harish Beechani

#2 - 17/04/2024 04:21 AM - Harish Beechani

- Status changed from New to In Progress

#3 - 17/04/2024 04:59 AM - Harish Beechani

- Assignee changed from Harish Beechani to Srinivas Kanukolanu

#4 - 24/04/2024 12:45 AM - Vasudev Mamidi

- Status changed from In Progress to Closed

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

- Target version set to Security Audit

Files

clipboard-202404171559-juppf.png	54.9 KB	17/04/2024	Kalyan Battula