E-Arogya - Bug #76

Feature # 65 (New): Security Audit

[Security Audit] 11- OTP Flooding

17/04/2024 03:49 PM - Kalyan Battula

Status:	Closed	**Start date:**	24/04/2024
Priority:	Normal	**Due date:**	
Assignee:	Harish Beechani	**% Done:**	100%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

11- OTP Flooding
CWE : CWE-770
Description :
This attack consists of generation of large number of OTP requests to a single mobile number and email.
Affected Path(s) :
https://earogya.satragroup.in/login *-Applicable to entire application
Impact :
The attacker could stop the availability of service or cause a performance decrease.
Recommendation :
It is recommended to send only 5 or 10 OTPs to a single mobile number for a period of time. After one successful OTP transaction (OTP sending and verifying) this count can be rest. Implement CAPTCHA mechanism for the request that is making OTP request.
Evidence/Proof Of Concept :
Step 1: Navigate to forgot password page and enter any Email.
clipboard-202404171547-lwfhr.png

Step 2: Multiple OTP's sent to Mobile as shown in below screenshot.
clipboard-202404171547-gejso.png

Step 3: It is observed that there is no rate limit for otp.

clipboard-202404171548-qoelw.png

Step 4: Multiple OTP's sent to Mobile as shown in below screenshot.

clipboard-202404171549-witvn.png

Subtasks:

Bug # 107: To stop the bot attack added captch in ui	**Closed**

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 Resolved

#3 - 24/04/2024 12:56 AM - Vasudev Mamidi

- Subtask #107 added

#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 05:20 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171547-lwfhr.png	564 KB	17/04/2024	Kalyan Battula
clipboard-202404171547-gejso.png	99.2 KB	17/04/2024	Kalyan Battula
clipboard-202404171548-qoelw.png	198 KB	17/04/2024	Kalyan Battula
clipboard-202404171549-witvn.png	226 KB	17/04/2024	Kalyan Battula