E-Arogya - Feature #284

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

[Security Audit Round 2] Clickjacking Attack (Repeated)

01/05/2024 01:21 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

Clickjacking Attack (Repeated)
CWE : CWE-1021
Description :
Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.
Affected Path(s) :
https://earogya.satragroup.in/ *-Applicable to entire application
Impact :
An attacker can host this domain in other evil site by using iframe and if a user fills the given field it can directly redirect as logs to attacker and after its redirect to your web server. Leading to steal user information too and use that host site as phishing of your site its CSRF and Clickjacking.
Evidence/Proof Of Concept :
Step 1: Sample HTML code for Clickjacking.

clipboard-202405011321-9tpav.png
Step 2: Clickjacking attack is successfully executed as shown in the screenshot.
clipboard-202405011321-uhqql.png

Recommendation :
It is recommended to implement any of the following:
Use the X-FRAME Options header in response headers and set its value to DENY or Same Origin or ALLOW-FROM a specified URL
Use Content-Security-Policy header and set frame-ancestors attribute to self.

History

#1 - 02/05/2024 09:15 PM - Vasudev Mamidi

- Assignee set to Vasu Malladi

#2 - 03/05/2024 04:16 AM - Harish Beechani

- Status changed from New to Resolved

#3 - 03/05/2024 05:23 AM - Sivakanth Kesiraju

- Target version set to Sprint 1 (29th April - 3rd May)

#4 - 03/05/2024 05:28 AM - Sivakanth Kesiraju

- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit

#5 - 10/05/2024 07:18 AM - Harish Beechani

- Status changed from Resolved to Ready for Prod

#6 - 16/05/2024 04:48 AM - Kalyan Battula

- Status changed from Ready for Prod to Closed

- Assignee changed from Vasu Malladi to Kalyan Battula

Files

clipboard-202405011321-9tpav.png	36.8 KB	01/05/2024	Kalyan Battula
clipboard-202405011321-uhqql.png	113 KB	01/05/2024	Kalyan Battula