E-Arogya - Bug #94

Feature # 65 (New): Security Audit

[Security Audit] 29 -Clickjacking Attack

17/04/2024 04:13 PM - Kalyan Battula

Status:	Closed	**Start date:**	17/04/2024
Priority:	Low	**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

29- Clickjacking Attack
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.
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.
Evidence/Proof Of Concept :
Step 1: Sample HTML code for Clickjacking.

clipboard-202404171612-ysseq.png
Step 2: Clickjacking attack is successfully executed as shown in the screenshot.
clipboard-202404171613-zrplx.png

History

#1 - 25/04/2024 11:48 PM - Vasudev Mamidi

- Status changed from New to Resolved

#2 - 28/04/2024 09:29 PM - Vasudev Mamidi

- Assignee set to Sivakanth Kesiraju

#3 - 28/04/2024 09:29 PM - Vasudev Mamidi

- Assignee changed from Sivakanth Kesiraju to Srinivas Kanukolanu

#4 - 03/05/2024 05:23 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 04:34 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171612-ysseq.png	25.7 KB	17/04/2024	Kalyan Battula
clipboard-202404171613-zrplx.png	112 KB	17/04/2024	Kalyan Battula