

E-Arogya - Bug #86

Feature # 65 (New): Security Audit

[Security Audit ] 21 -Insufficient Anti-Automation

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

Status:	Closed	Start date:	17/04/2024
Priority:	Normal	Due date:	
Assignee:	Raju Kuthadi	% Done:	0%
Category:		Estimated time:	0:00 hour
Target version:	Security Audit	Spent time:	0:00 hour
Deployed In:		Category:	
<div>Description</div> <div>21- Insufficient Anti-Automation</div> <div>CWE : CWE-799</div> <div>Description :</div> <div>Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually. Certain web site functionalities should be protected against automated attacks.</div> <div>Affected Path(s) :</div> <div><a href="https://earogya.satragroup.in/login">https://earogya.satragroup.in/login</a> *-Applicable to entire application</div> <div>Impact :</div> <div>Attackers could repeatedly exercise web site functionality attempting to exploit or defraud the system. An automated robot could potentially execute thousands of requests a minute, causing potential loss of performance or service.</div> <div>Recommendation :</div> <div>It is recommended to implement captcha. CAPTCHA should be perceived as a ratelimiting protection only. If it is implemented, the following considerations should be taken into account:</div> <div>No CAPTCHA information (except the image itself) should be stored on the client side.</div> <div>The client should have no "control" over the CAPTCHA content. CAPTCHA images should be always randomly generated without possibility to perform image preprocessing, segmentation and classification.</div> <div>CAPTCHA images should not be reused.</div> <div>Evidence/Proof Of Concept :</div> <div>Step 1: Captcha is not implemented for the application as shown below.</div> <div>clipboard-202404171603-4citj.png</div>			

History

#1 - 25/04/2024 11:54 PM - Karthik Daram

- Status changed from New to Resolved

#2 - 25/04/2024 11:55 PM - Karthik Daram

- Assignee set to Raju Kuthadi

#3 - 03/05/2024 05:24 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 - 30/09/2024 05:15 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171603-4citj.png	553 KB	17/04/2024	Kalyan Battula
----------------------------------	--------	------------	----------------