E-Arogya - Feature #268

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

[Security Audit Round 2] Cross Origin Resource Sharing (CORS) Misconfiguration

01/05/2024 01:06 PM - Kalyan Battula

Status:	Ready for Prod	**Start date:**	01/05/2024
Priority:	High	**Due date:**	
Assignee:	Vasu Malladi	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

Cross Origin Resource Sharing (CORS) Misconfiguration
observation : Repeated
CWE : CWE-642
Description :
The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.
Affected Path(s) :
/(WebServer)
Impact :
Any website can make XHR requests to your site and access the responses.
Evidence/Proof Of Concept :
Step 1: Cross Origin Resource Sharing (CORS) Misconfiguration as shown in below screenshot.

clipboard-202405011305-wrcjk.png
Recommendation :
It is recommended not to use Access-Control-Allow-Origin: *.
Instead use Access-Control-Allow-Origin header should contain the list of origins that can make CORS requests.
Reference Link:
https://cwe.mitre.org/data/definitions/942.htmlhttps://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny

History

#1 - 02/05/2024 09:18 PM - Vasudev Mamidi

- Assignee set to Vasu Malladi

#2 - 03/05/2024 04:23 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 05:27 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

Files

clipboard-202405011305-wrcjk.png	85.8 KB	01/05/2024	Kalyan Battula