E-Arogya - Bug #84

Feature # 65 (New): Security Audit

[Security Audit]19- Client side bypass / Improper server side validation

17/04/2024 04:01 PM - Kalyan Battula

Status:	Closed	**Start date:**	17/04/2024
Priority:	Normal	**Due date:**	
Assignee:	Pavan kumar Siddamsetti	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

19- Client side bypass / Improper server side validation
CWE : CWE-602
Description :
The software is composed of a server that relies on the client to implement a mechanism that is intended to protect the server.
Affected Path(s) :
https://earogya.satragroup.in/configuration/all_masterhttps://his-core-domainservice.satragroup.in/department-master *-Applicable to entire application
Impact :
When the server relies on protection mechanisms placed on the client side, an attacker can modify the client-side behavior to bypass the protection mechanisms resulting in potentially unexpected interactions between the client and server. The consequences will vary, depending on what the mechanisms are trying to protect.
Recommendation :
It is recommended to validate the user input at server side. It is recommended to enforce an application URL space white list and implement proper access control.
Evidence/Proof Of Concept :
Step 1: Login to the application with test2_fd credentials and navigate to the Department tab under the Masterdata dropdown. Observe that there are only options for "Yes" or "No" as shown in the screenshot below.
clipboard-202404171601-tiqhl.png

Step 2: Capture the above request and modify the value as depicted in the screenshot below. Observe Response Resource has been created successfully.
clipboard-202404171601-lcw2a.png

History

#1 - 17/04/2024 05:01 AM - Harish Beechani

- Status changed from New to In Progress

- Assignee set to Pavan kumar Siddamsetti

#2 - 24/04/2024 01:01 AM - Vasudev Mamidi

- Status changed from In Progress to Resolved

#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 05:16 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171601-tiqhl.png	73.6 KB	17/04/2024	Kalyan Battula