E-Arogya - Feature #278

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

[Security Audit Round 2] Sensitive Data Passed Through URL Parameters (Repeated)

01/05/2024 01:16 PM - Kalyan Battula

Status:	Ready for Prod	**Start date:**	01/05/2024
Priority:	High	**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

Sensitive Data Passed Through URL Parameters
observation : Repeated
CWE : CWE-598
Description :
The web application uses the HTTP GET method to process a request and includes sensitive information in the query string of that request.
Affected Path(s) :
https://his-healthidservice.satragroup.in/abdm/isAvailable/customHealthId/srinuks.1 *-Applicable to entire application
Impact :
This allows attackers to obtain sensitive data such as usernames, passwords, tokens (authX), database details, and any other potentially sensitive data. Simply using HTTPS does not resolve this vulnerability.
Evidence/Proof Of Concept :
Step 1: ABHA Username Passed Through URL as shown in below screenshot.
clipboard-202405011315-5lepq.png

Step 2: Functionality issue
clipboard-202405011316-jnjpt.png

Recommendation :
When sensitive information is sent, use the POST method (e.g. registration form, login form, etc.).

History

#1 - 03/05/2024 04:15 AM - Harish Beechani

- Assignee set to Pavan kumar Siddamsetti

#2 - 03/05/2024 04:15 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 07:19 AM - Harish Beechani

- Status changed from Resolved to Ready for Prod

Files

clipboard-202405011315-5lepq.png	35.6 KB	01/05/2024	Kalyan Battula
clipboard-202405011316-jnjpt.png	76.4 KB	01/05/2024	Kalyan Battula