E-Arogya - Bug #92

Feature # 65 (New): Security Audit

[Security Audit] 27 -Sensitive Data Passed Through URL Parameters

17/04/2024 04:10 PM - Kalyan Battula

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

27- Sensitive Data Passed Through URL Parameters
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.
Recommendation :
When sensitive information is sent, use the POST method (e.g. registration form, login
form, etc.).
Evidence/Proof Of Concept :
Step 1: ABHA Username Passed Through URL as shown in below screenshot.

clipboard-202404171610-2mfsz.png

History

#1 - 18/04/2024 11:39 PM - Pavan kumar Siddamsetti

- Assignee set to Pavan kumar Siddamsetti

#2 - 21/04/2024 08:44 PM - Pavan kumar Siddamsetti

- Status changed from New to In Progress

#3 - 24/04/2024 01:01 AM - Vasudev Mamidi

- Status changed from In Progress to Resolved

#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 05:13 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171610-2mfsz.png	40.2 KB	17/04/2024	Kalyan Battula