E-Arogya - Bug #75

Feature # 65 (New): Security Audit

[Security Audit]10 -Sensitive Information Disclosure

17/04/2024 03:46 PM - Kalyan Battula

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

Description

10- Sensitive Information Disclosure

CWE : CEW-200
Description :
Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker, including: (a) Data about other users, such as usernames or financial information (b) Sensitive commercial or business data (c) Technical details about the website and its infrastructure
Affected Path(s) :
https://earogya.satragroup.in/patient/search-update-patient *-Applicable to entire application
Impact :
The dangers of leaking sensitive user or business data are fairly obvious, but disclosing technical information can sometimes be just as serious. Although some of this information will be of limited use, it can potentially be a starting point for exposing an additional attack surface, which may contain other interesting vulnerabilities.
Recommendation :
It is recommended not to disclose any sensitive information to the end user. Incase of aadhaar: It is recommended to use Aadhaar vault service to store aadhaar numbers securely as per UIDAI guidelines. Mask Aadhaar numbers and display only last 4 digits.
Evidence/Proof Of Concept :
Step 1: Access the URL "https://earogya.satragroup.in/patient/search-update-patient" and it was observed that sensitive information like "Aadhar numbers" were disclosed in Plain text as shown in below screenshot.
clipboard-202404171545-ca3dd.png

History

#1 - 23/04/2024 02:15 AM - Deepika Valluri

- Status changed from New to In Progress

- Assignee set to Deepika Valluri

#2 - 26/04/2024 12:00 AM - Karthik Daram

- 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 05:21 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171545-ca3dd.png 62.6 KB 17/04/2024 Kalyan Battula