E-Arogya - Feature #245

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

[Security Audit Round 2] Insecure Data Storage (Reopened)

01/05/2024 12:37 PM - Kalyan Battula

Status:	Resolved	**Start date:**	01/05/2024
Priority:	High	**Due date:**	02/05/2024
Assignee:	Raju Kuthadi	**% Done:**	0%
Category:		**Estimated time:**	9:00 hours
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

Insecure Data Storage
observation : Repeated
CWE : CWE-312
Description :
Insecure data storage vulnerabilities occur when development teams assume that users or malware will not have access to a mobile device's file system and subsequent sensitive information in data-stores on the device. File systems are easily accessible.
Organizations should expect a malicious user or malware to inspect sensitive data stores. Usage of poor encryption libraries is to be avoided. Rooting or jailbreaking a mobile device circumvents any encryption protections. When data is not protected properly, specialized tools are all that is needed to view application data.
Affected Path(s) :
https://earogya.satragroup.in/frontdesk/dashboard *-Applicable to entire application
Impact :
Insecure data may result in the following business impacts: • Identity theft; • Privacy violation; • Fraud; • Reputation damage; • External policy violation (PCI); or • Material loss.
Evidence/Proof Of Concept :
Step 1: Login to the application, access the internal pages and click on logout. It is observed that even after the user get logged out, the JWT token was still saved in the cookie storage as shown below.

History

#1 - 01/05/2024 12:09 AM - Kalyan Battula

- File clipboard-202405011238-sk8oy.png added

- File clipboard-202405011239-tjtfi.png added

observation : Repeated
CWE : CWE-312
Description :
Insecure data storage vulnerabilities occur when development teams assume that users or malware will not have access to a mobile device's file system and subsequent sensitive information in data-stores on the device. File systems are easily accessible.
Organizations should expect a malicious user or malware to inspect sensitive data stores. Usage of poor encryption libraries is to be avoided. Rooting or jailbreaking a mobile device circumvents any encryption protections. When data is not protected properly, specialized tools are all that is needed to view application data.
Affected Path(s) :
https://earogya.satragroup.in/frontdesk/dashboard *-Applicable to entire application
Impact :
Insecure data may result in the following business impacts: • Identity theft; • Privacy violation; • Fraud; • Reputation damage; • External policy violation (PCI); or • Material loss.
Evidence/Proof Of Concept :
Step 1: Login to the application, access the internal pages and click on logout. It is observed that even after the user get logged out, the JWT token was still saved in the cookie storage as shown below.

clipboard-202405011238-sk8oy.png

Step 2: The JWT token reveals the sensitive information like username etc., as shown below.

clipboard-202405011239-tjtfi.png
Recommendation :
1. It is important to threat model your mobile app, OS, platforms and frameworks to understand the information assets the app processes and how the APIs handle those assets. It is crucial to see how they handle the following types of features :
1. URL caching (both request and response);
2. Keyboard press caching;
3. Copy/Paste buffer caching;
4. Application backgrounding;
5. Intermediate data
6. Logging;
7. HTML5 data storage;
8. Browser cookie objects;
9. Analytics data sent to 3rd parties.
2. Also, it is recommended to encrypt the user data in device internal storage.

#2 - 02/05/2024 03:45 AM - Uma Maheswarachari Melpati

- Assignee set to Raju Kuthadi

- Estimated time set to 9:00 h

#3 - 03/05/2024 04:04 AM - Raju Kuthadi

- Due date set to 02/05/2024

- Status changed from New 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 05:27 AM - Sivakanth Kesiraju

- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit

Files

clipboard-202405011238-sk8oy.png	101 KB	01/05/2024	Kalyan Battula
clipboard-202405011239-tjtfi.png	97.1 KB	01/05/2024	Kalyan Battula