

E-Arogya - Bug #79

Feature # 65 (New): Security Audit

[Security Audit] 14 -Improper Session Management / Session Expiration too longer

17/04/2024 03:55 PM - Kalyan Battula

Status:	Closed	Start date:	17/04/2024
Priority:	Normal	Due date:	
Assignee:	Vasu Malladi	% Done:	0%
Category:		Estimated time:	0:00 hour
Target version:	Security Audit	Spent time:	0:00 hour
Deployed In:		Category:	
Description 14- Improper Session Management / Session Expiration too longer CWE : CWE-613 Description : In this application a single fixed token is in use for single user, token expiry time also too longer. Affected Path(s) : https://earogya.satragroup.in/login *-Applicable to entire application Impact : It helps the attackers to submit without any authentication. Recommendation : It is recommended to maintain session id after login and destroy it after logout. Reference Link: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html Evidence/Proof Of Concept : Step 1: Login to the application with any user.And Capture the request.Here application using the JWT token for user token as shown as below screenshot. clipboard-202404171554-zb0b4.png Step 2: Now, observe the expiration token of the JWT token. It is noticed that expiration time of the token was too long as shown in below screenshot. clipboard-202404171555-wgpwd.png			

History

- #1 - 24/04/2024 12:53 AM - Vasudev Mamidi
- Assignee set to Vasu Malladi
- #2 - 24/04/2024 12:53 AM - Vasudev Mamidi
- Status changed from New to In Progress
- #3 - 25/04/2024 11:51 PM - Vasudev Mamidi
- Status changed from In Progress to Resolved
- #4 - 03/05/2024 05:24 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 05:20 PM - Gautam Kumar
- Status changed from Resolved to Closed

Files

clipboard-202404171554-zb0b4.png	109 KB	17/04/2024	Kalyan Battula
clipboard-202404171555-wgpwd.png	69.8 KB	17/04/2024	Kalyan Battula