E-Arogya - Bug #96

Feature # 65 (New): Security Audit

[Security Audit] 31 -Username and Password field with auto-complete

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

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

Description

31- Username and Password field with auto-complete
CWE : CWE-16
Description :
The Web form contains passwords or other sensitive text fields for which the browser auto-complete feature is enabled. Auto-complete stores completed form field and passwords locally in the browser, so that these fields are filled automatically when the user visits the site again.
Affected Path(s) :
https://earogya.satragroup.in/login *-Applicable to entire application
Impact :
Data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information.
Recommendation :
The autocomplete value can be configured in two different locations.
The first and most secure location is to disable the autocomplete attribute on the "form" HTML tag. This will disable autocomplete for all inputs within that form.
An example of disabling autocomplete within the form tag is:
"form autocomplete=off".
The second slightly less desirable option is to disable the autocomplete attribute for a specific "input" HTML tag. While this may be the less desired solution from a security perspective, it may be preferred method for usability reasons, depending on size of the form. An example of disabling the autocomplete attribute within a password input tag is
"input type=password autocomplete=off".
Evidence/Proof Of Concept :
Step 1: It was observed that 'Auto-complete=off' was not implemented in the username field as shown in below screenshot

clipboard-202404171615-hsytr.png

Step 2: It was observed that 'Auto-complete=off' was not implemented in password fields, as shown in below screenshot

clipboard-202404171616-iiynr.png

History

#1 - 17/04/2024 10:06 PM - Karthik Daram

- Status changed from New to In Progress

- Assignee set to Karthik Daram

#2 - 17/04/2024 10:22 PM - Karthik Daram

- Assignee changed from Karthik Daram to Uma Maheswarachari Melpati

#3 - 23/04/2024 03:02 AM - Uma Maheswarachari Melpati

- 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 05:27 AM - Sivakanth Kesiraju

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

#6 - 30/09/2024 04:33 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171615-hsytr.png	243 KB	17/04/2024	Kalyan Battula
clipboard-202404171616-iiynr.png	256 KB	17/04/2024	Kalyan Battula