

E-Arogya - Bug #81

Feature # 65 (New): Security Audit

[Security Audit ] 16- Weak Password Policy

17/04/2024 03:58 PM - Kalyan Battula

<b>Status:</b>	Closed	<b>Start date:</b>	17/04/2024
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Kranti Boddu	<b>% Done:</b>	0%
<b>Category:</b>		<b>Estimated time:</b>	0:00 hour
<b>Target version:</b>	Security Audit	<b>Spent time:</b>	0:00 hour
<b>Deployed In:</b>		<b>Category:</b>	
<b>Description</b> 16- Weak Password Policy CWE : CWE-521 Description : A weak password policy leaves sensitive data vulnerable to unauthorized access, increases the risk of security breaches, and can lead to non-compliance with regulations. It exposes organizations to reputational damage, financial losses, and undermines trust with stakeholders. Affected Path(s) : <a href="https://his-user-management-service.satragroup.in/changepassword">https://his-user-management-service.satragroup.in/changepassword</a> *-Applicable to entire application Impact : Not implementing a proper password policy, could allow the users to set very easy password that help the attackers to perform the dictionary attacks and gain access to the user accounts Recommendation : Implement a strong password policy that contains: 1. one capital letter 2. one number 3. Minimum 10 characters 4. One special character. Reference Links: 1. <a href="https://www.owasp.org/index.php/Testing_for_default_credentials_(OTGAUTHN-002)">https://www.owasp.org/index.php/Testing_for_default_credentials_(OTGAUTHN-002)</a> 2. <a href="https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTGAUTHN-007)">https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTGAUTHN-007)</a> 3. <a href="https://www.owasp.org/index.php/Testing_for_Weak_or_unenforced_username_policy_(OTG-IDENT-005)">https://www.owasp.org/index.php/Testing_for_Weak_or_unenforced_username_policy_(OTG-IDENT-005)</a> 4. <a href="https://www.us-cert.gov/ncas/alerts/TA13-175A">https://www.us-cert.gov/ncas/alerts/TA13-175A</a> Evidence/Proof Of Concept : Step 1: Password Policy not implemented as shown in below screenshot. clipboard-202404171558-4nevo.png			

History

- #1 - 17/04/2024 05:38 AM - Kranti Boddu
  - Status changed from New to In Progress
  - Assignee set to Kranti Boddu
- #2 - 25/04/2024 03:30 AM - Kranti Boddu
  - 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 05:19 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171558-4nevo.png	34.9 KB	17/04/2024	Kalyan Battula
----------------------------------	---------	------------	----------------