






Authentication security breach

 Attach  Add a child issue  Link issue  

Description • Unsaved changes


A user is allowed access to as many login attempts as he/she may wish. This can result in a security breach by allowing an attacker to gain access to a account credentials by using the brute force attack.

Steps to reproduce:

1. Open Chrome web browser version 108.0.5359.125 (Official Build) (64-bit) on a Windows 10 machine.
2. Access annacori.com website.
3. Click on 'Denis Handmade' button from the top menu.
4. Click on 'My Account' option from the top menu.
5. In the Email field, input danaarvinti@gmail.com
6. In the Password field, input 12345678
7. Click the 'Log In' button
8. Repeat step 6 and 7 in this order 10 times.

Actual result:

The website will still allow login attempts.

In Analysis 

Details

Assignee	 Dana Arvinti
Labels	None
Sprint	AN Sprint 1 
Reporter	 Dana Arvinti

Created 8 January 2023 at 19:57

Updated 2 hours ago

 Configure

The website will still allow login attempts.

Expected result:

The website should display a message in which it warns the user that the maximum login attempts was reached and for a specified amount of time the user will not be able to try login again.

Reference TC-4, Step 3

Severity Sev-3

Priority  High

Linked issues

blocks

 AC-6 Log in dialogue

  DONE ▾

Activity

Show: All Comments History

Newest first ▾

In Analysis ▾

Details

Assignee  Dana Arvinti

Labels None

Sprint AN Sprint 1 

Reporter  Dana Arvinti

Created 8 January 2023 at 19:57

Updated 2 hours ago

 Configure