Security test for brute force attack on Login page

The various scenarios to test for brute force attack on login page are as follows:

|  |
| --- |
| Test Scenario |
| Verify that there is a limit on the total number of unsuccessful login attempts |
| Verify that incase of incorrect credentials a message like ‘’incorrect username or password’’ should get displayed instead of an exact message pointing to the incorrect field |
| Verify that logging in involve a two-step verification |
| Verify that after the user has logged out, the user cannot access the account without logging in |
| Verify that the user use long and complex passwords |
| Validate whether the password fields in the Login page are following password complexity standards |
| Verify that the password field in the login page are toggled to hide its visibility |
| Verify the login session timeout duration |
| Verify that the account is locked out after multiple unsuccessful login attempts |

Brute force attack testing by OWASP ZAP tool

1. Installed and configured ZAP
2. Explored the application manually
3. Followed the below steps to manually explore the appliction:
4. Start ZAP and click on the Quick Start tab of the Workspace Window.
5. Click on the large Manual Explore button.
6. In the URL to explore text box, enter the full URL of the web application (https://www.tourradar.com/d/europe)
7. Select the browser
8. Click the Launch Browser

Below is the attached ZAP scan report of Tourradar

