List of found defects

LNU Scheduler

Defect 1. Incorrect state of the event template on the settings page

Description: While the selected event template is saved on the backend, the frontend does not update it correctly.

Reproduction:

1. Enter the website and log in with valid credentials.
2. Go to the Settings page.
3. Change the event template from default to any custom template.
4. Leave Settings page (e.g. go to the Schedules page).
5. Re-enter the Settings page.

Expected Result: A custom event template is selected and the page shows it correctly.

Actual Outcome: The default template is still seen as selected.

Defect 2. Session timeout inconsistencies

Description: User sessions do not consistently time out after the designated period of inactivity, posing a security risk.

Reproduction:

1. On test setup change the time out period to 1 minute.
2. Enter the website and log in with valid credentials.
3. Wait for a minute or two.
4. Make an action on the website (e.g. go to the Settings page)

Expected Result: The user is notified his session was timed out and is logged out.

Actual Outcome: The user can take any action he intends to do, without any time-out notification or log out. Can be reproduced each time.

Defect 3. Password restoration links do not timeout

Description: Links to restore passwords do not have a working expiration date, which is a serious security risk.

Reproduction:

1. Make the password restoration link either timeout immediately or in 1-2 minutes on the test setup.
2. Enter the website.
3. Access the login page.
4. Initiate the “Forgot Password” process.
5. Go to the used e-mail and locate the last message from a website about password restoration.
6. Open the link after it should’ve been expired.

Expected Result: The user is notified that the link has expired at a certain time.

Actual Outcome: The user can proceed with the password restoration process.

Defect 4. Mobile responsiveness issues on tablets

Description: The website does not correctly adjust to different tablet screen sizes, causing layout breaks and overlapping elements.

Reproduction:

1. Take any tablet and enter the website.

Expected Result: The layout was correctly adjusted and everything is properly visible on the screen.

Actual Outcome: Buttons and text labels are out of place and overlapping here and there.

Defect 5. Slow load times under high user load

Description: During peak traffic times, the website experiences slower load times than acceptable thresholds.

Reproduction:

1. Start a fake routine that imitates expected peak traffic.
2. Enter the website.
3. Measure the time it takes for the website to open.

Expected Result: The website loads in the expected threshold.

Actual Outcome: The website takes significantly more time to load.

Defect 6. Password reset function flaw

Description: Password reset process can be initiated multiple times without any limit.

Reproduction:

1. Enter the website.
2. Proceed to the login page.
3. Start the reset password process a dozen of times (for different e-mails, for the same e-mails).

Expected Result: After several tries the user is not allowed to initiate reset password anymore.

Actual Outcome: The user can initiate the reset password any amount of time he wants.

Defect 7. Overlapping text on mobile devices

Description: On smaller mobile screens, the text overlaps on the settings page.

Reproduction:

1. Enter the website on the smartphone.
2. Log in with valid credentials.
3. Enter the Settings page.

Expected Result: The text is properly aligned with all interactable components.

Actual Outcome: Text is overlapping some interactable components and other text on the page.

Defect 8. Incorrect login data message

Description: While trying to log in under a non-existent e-mail and/or username, the message displayed states that this user was not created. This

should be changed to the same message when the username/password does not match, otherwise, it will create a security risk and make it easier to brute-force accounts.

Reproduction:

1. Enter the website.
2. Proceed to the login screen.
3. Enter the wrong credentials with an incorrect username.
4. Observe the message.
5. Enter the wrong credentials with an incorrect password.
6. Observe the message.

Expected Result: The message is identical in both cases.

Actual Outcome: The message hints that the user is not created in one case and that the password is wrong in another case.

Defect 9. Brute-force attacks are possible

Description: There is no limit to trying to log into the account. Combined with previous defects that's a horrific security flaw.

Reproduction:

1. Enter the website.
2. Proceed to the login screen.
3. Start using the correct username but the wrong password as credentials.

Expected Result: The user can not initiate login after several tries.

Actual Outcome: The user can try to log in indefinitely.

Defect 10. Inconsistency on different browsers

Description: Pages do not render properly on Microsoft Edge and Internet Explorer.

Reproduction:

1. Enter the website on Google Chrome.

2. Enter the website on Microsoft Edge.
3. Enter the website on Internet Explorer.
4. Enter the website on Mozilla Firefox.

Expected Result: The website looks the same on all browsers.

Actual Outcome: While the website looks consistent on Chrome and Firefox, butt on Microsoft Edge and Internet Explorer a spider appears on the screen instead.