Explanation

I usually start with visual and manual testing of the login form, make sure UI looks good e.g., there is no text overlapping, the form doesn’t look broken all the buttons have correct names, there are no typos and translation errors. Using the basic functions of the login form I get to know the logic behind it and helps me choose testing tools for it.

As can be seen my primary choice is Test automation with Java Selenium. With it we covered all the functional and UI test scenarios. It became clear to me Boundary testing (min and max no of characters text fields accept) is unneeded when I realized min no of characters for username is 2 and 8 for password it's visible from the login form and I manually checked it, in addition to that I made password length Test that checks maximum No. of allowed characters and there is no limitation. I see the minimum no of username characters of 2 as a big lack of this website as it allowed me to block user with username: cy on the first day of testing. I think it would be much harder to accidentally guess other usernames if they were longer.

Other testing tools I would use: use Postman or developer tools network tab to see how the browser executes a POST request. When we try to login with valid credentials and what response do we get.

If we have access to a data base: using SQL to query the database to check user login is a common and effective method to verify the connection between the login form and the backend.

It allows us to validate whether the user-provided credentials match the records stored in the database, thus ensuring the authentication process is working as expected.

For performance testing: use JMeter for load test simulate multiple users logging in simultaneously to test the login form's performance under load, also measure the login time or use Lighthouse in developer tools (can't be used in this case).

Security testing: test the login form against SQL injection attack as it can be seen from the tests that username and password fields accept special characters. I suppose there is some other protection the website is using against the penetration attacks.