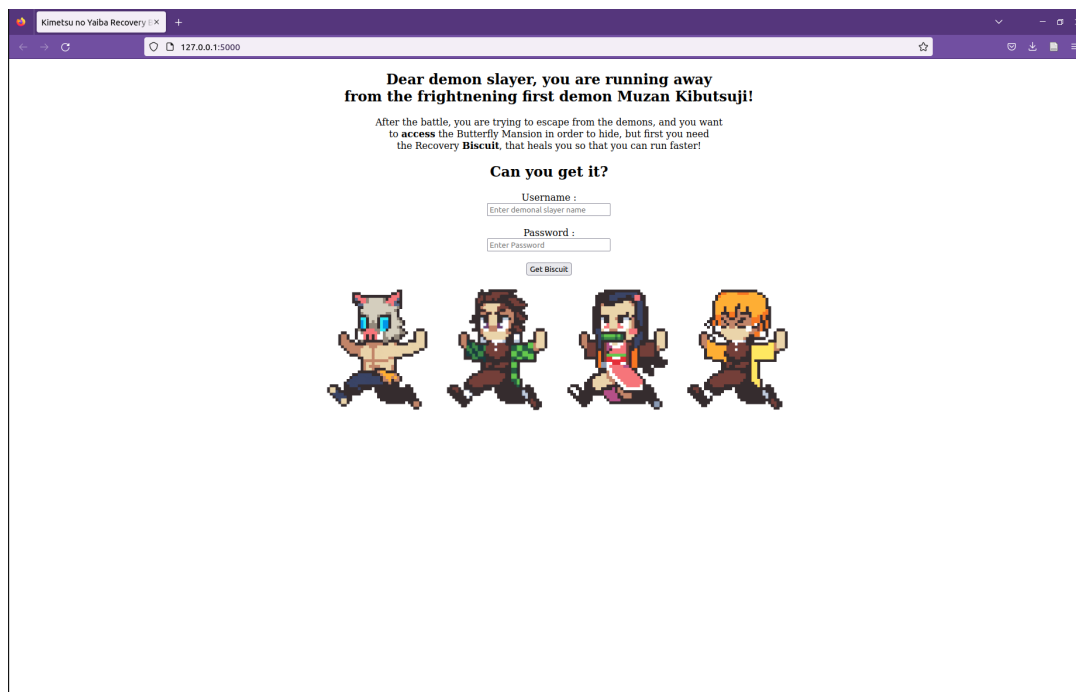
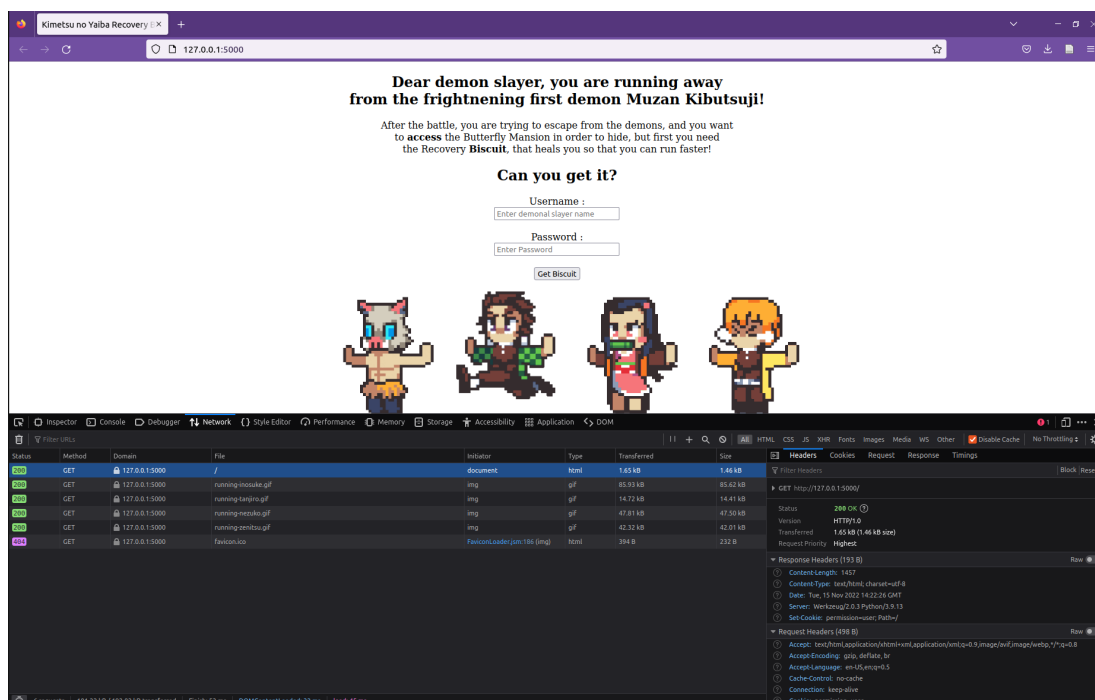


This challenge can be done using a python script (a little more advanced but you can directly take the flag from a terminal) or following this procedure through the browser inspector.

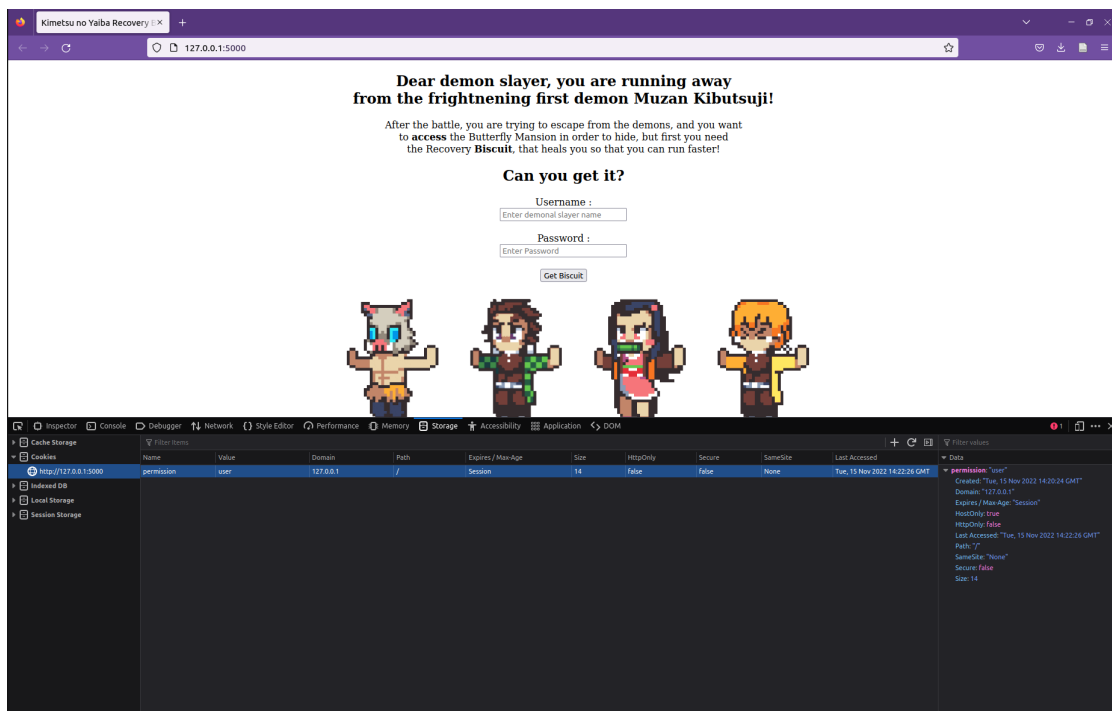
1. As the challenge hints, you need to do a (fake) login, but it requires a specific cookie (hinted by the biscuit request) in order to get the flag.



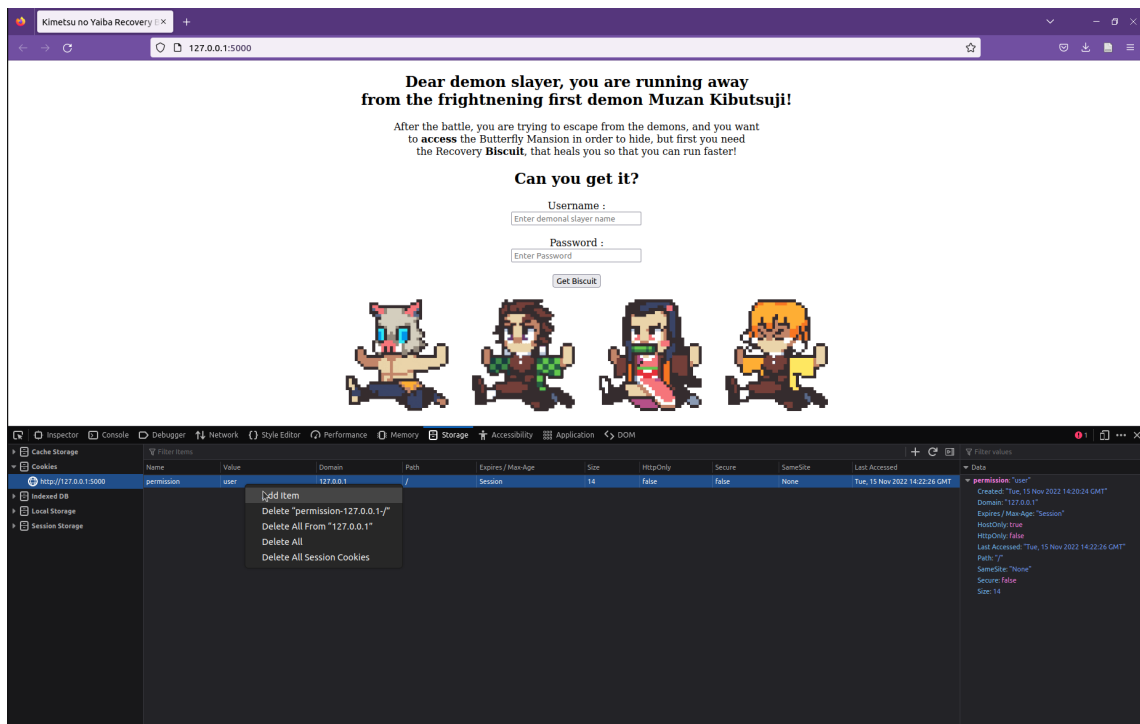
2. You can use the network inspector to look inside the GET request of the index page. You can notice the presence of the header “set-cookie” with the value “permission=user”.



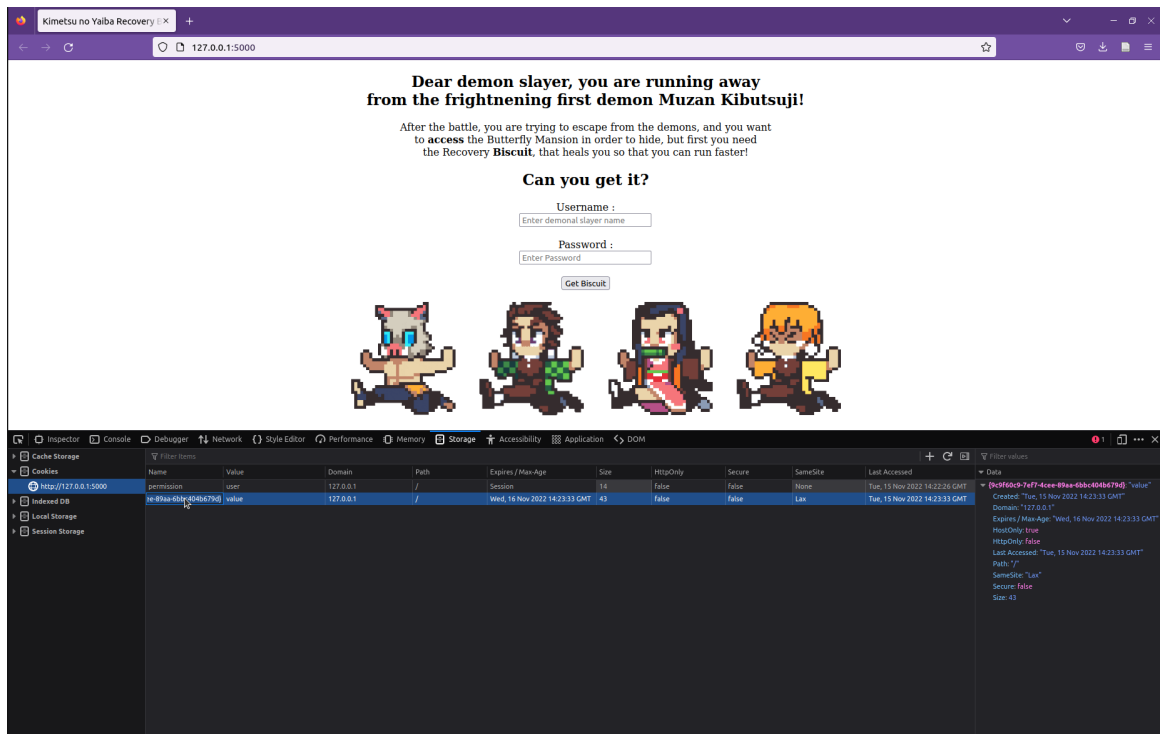
- Now you can try to guess the right cookie that the application wants to spit out the flag to you. To do that, you can check the cookie stored in the “Storage” window, at the “Cookie” folder. You can see the same cookie of the previous step.



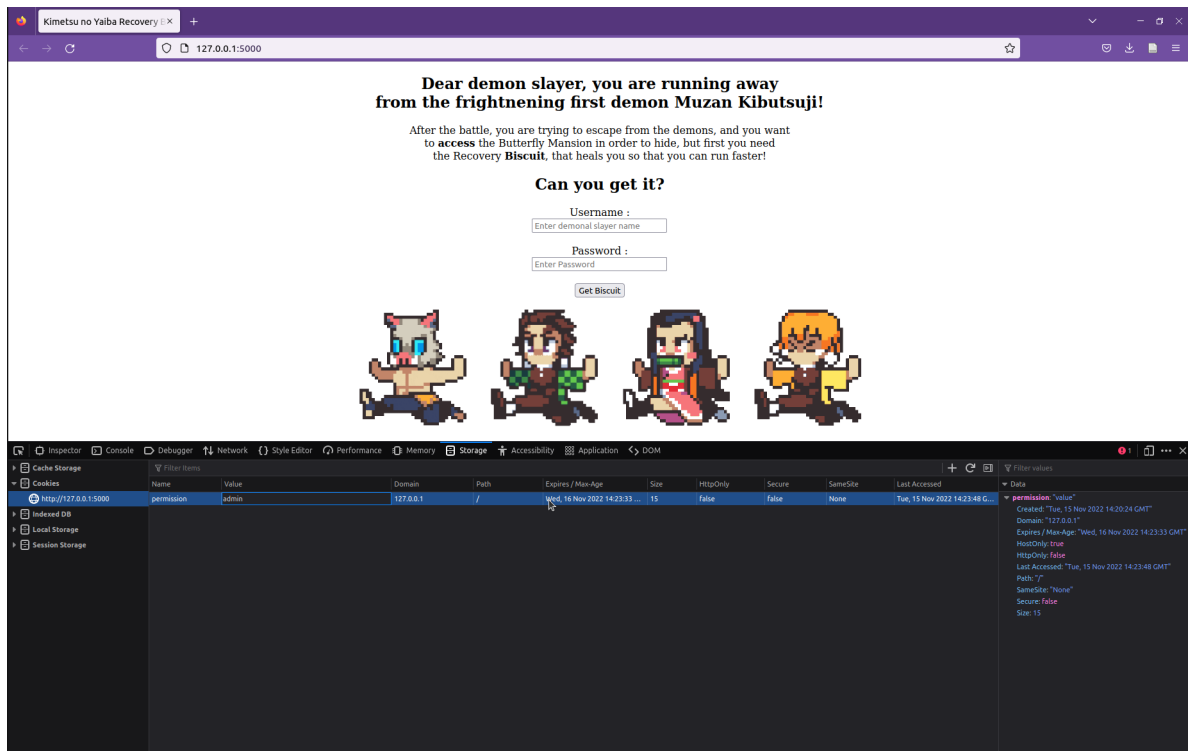
- The next step is to modify this cookie, creating a new one with the right-click on the cookie and selecting “Add item”.



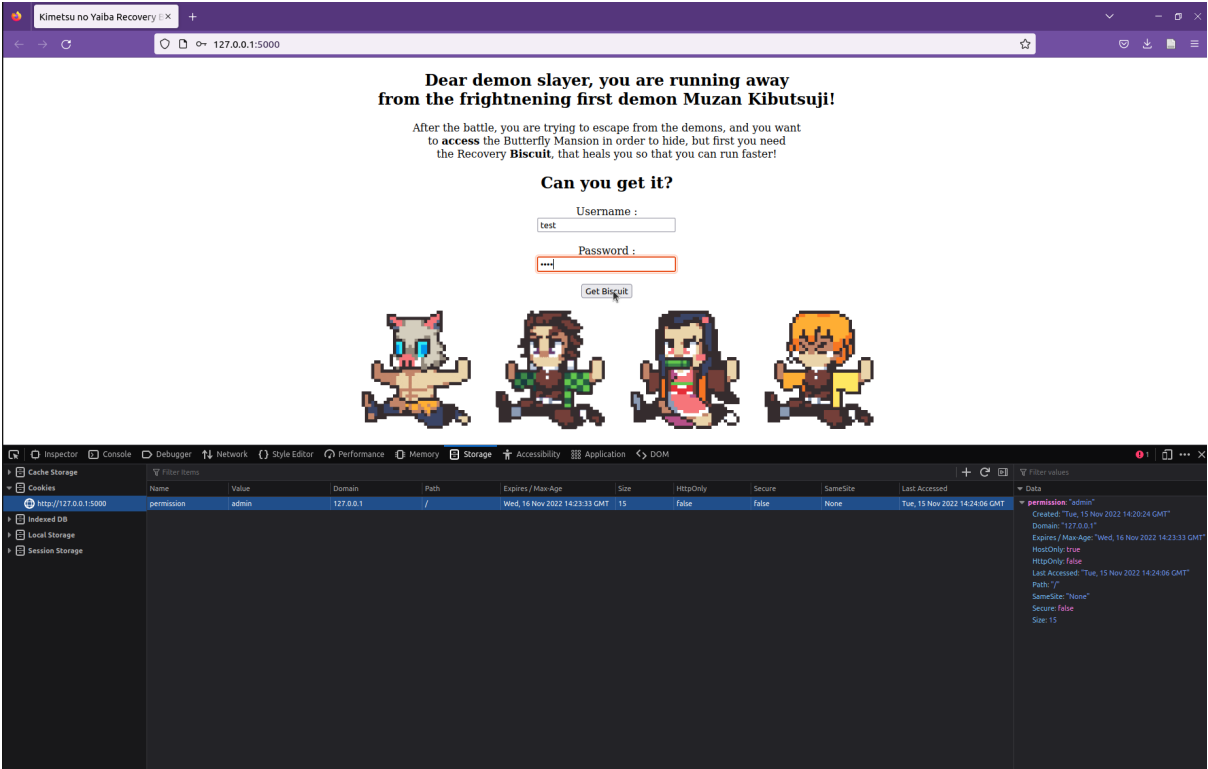
- Now you have a second cookie with a (not so) random name, you just modify the name to be the same as the older cookie and this will overwrite it with the new default value “value”



- Now we can change the cookie value to “admin” and see if it works, trying to login in the next step with a random username and password.



7. I used test/test as login, setting the cookie to admin



8. And it worked! Now I have the flag

