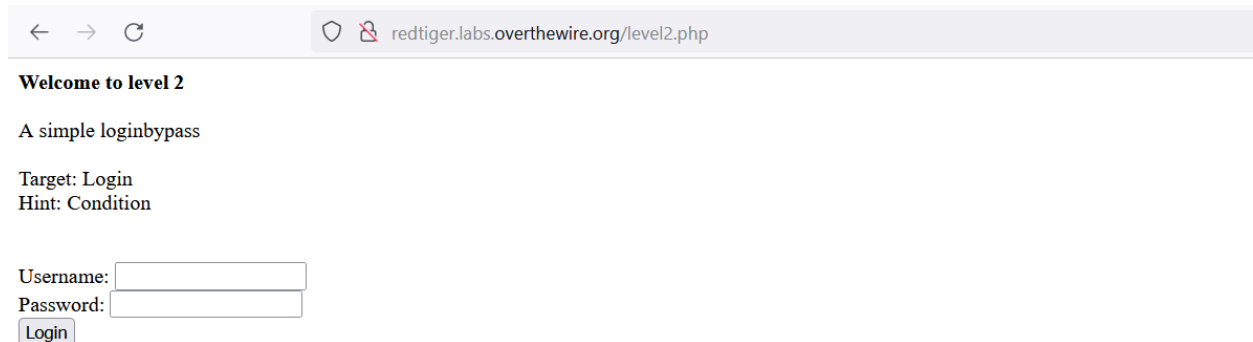


## Level 2 :- Simple login-bypass

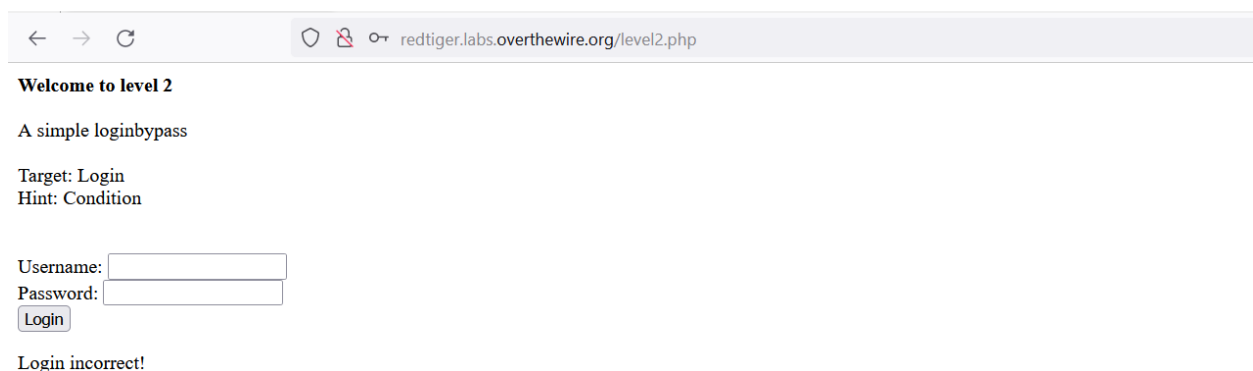
The lab at this level includes login functionality. Therefore, in order to complete the lab, we must circumvent the login functionality by utilising SQL Injection techniques.

So As you can see in Below Screenshot the there is a login page and as you can see in the Hint that there is “Condition” So from this we can conclude that the Condition for checking is differently executed.



The screenshot shows a web browser window with the address bar displaying 'redtiger.labs.overthewire.org/level2.php'. The page content includes the heading 'Welcome to level 2', a description 'A simple loginbypass', and the target 'Login' with a hint 'Condition'. Below this, there are input fields for 'Username:' and 'Password:', followed by a 'Login' button.

So let's try to log in with random credentials



This screenshot shows the same login page as before, but with an additional message at the bottom: 'Login incorrect!'. The browser address bar and the page content (heading, description, target, hint, and input fields) remain the same.

As you can see above I have entered the random credentials as we can see in the response it is displaying “Login incorrect!”

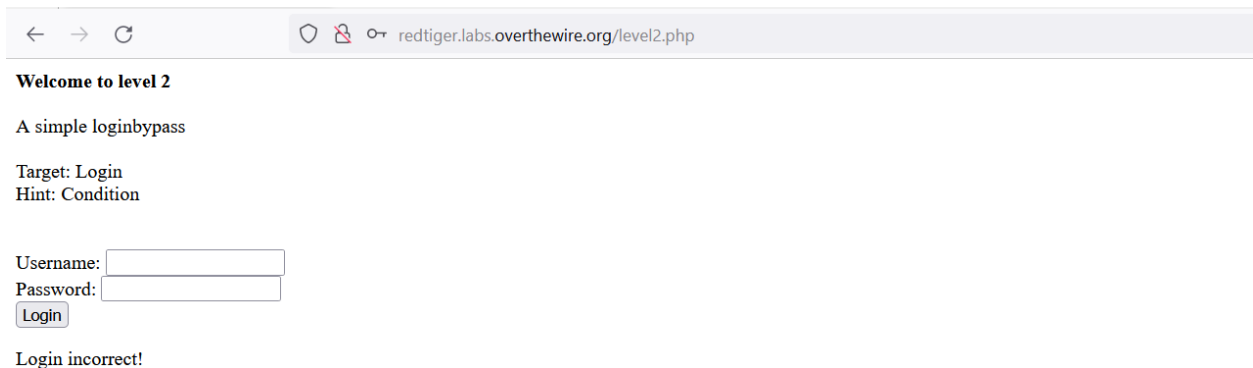
So now I am entering let's try Entering General payload from that we start testing the filter

So payload would be

A' or 1=1--

Due to our belief that all conditions following the username condition will be commented, let's enter the aforementioned payload into the username field and random characters into the password field.

Let's try that, then.



← → ↻ redtiger.labs.overthewire.org/level2.php

**Welcome to level 2**

A simple loginbypass

Target: Login  
Hint: Condition

Username:

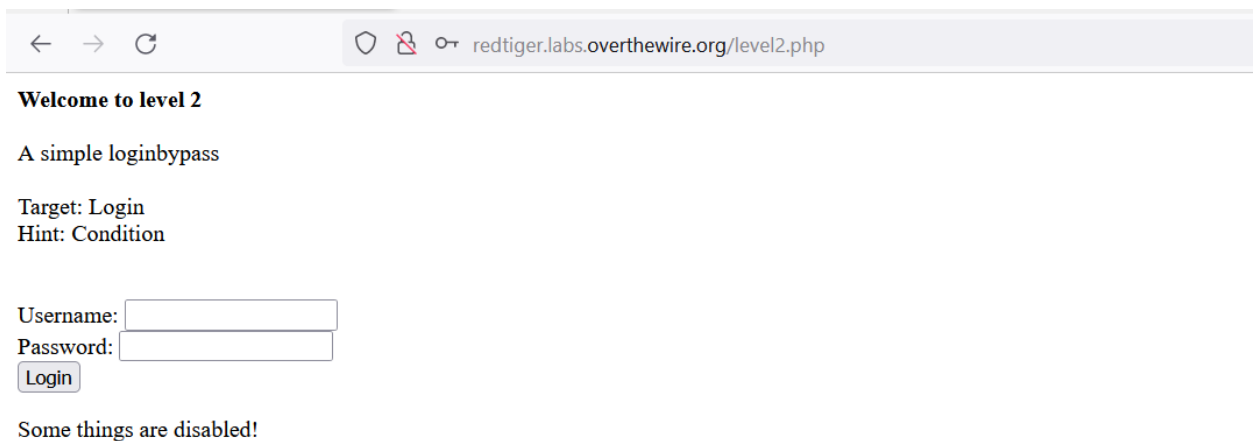
Password:

Login

Login incorrect!

However, after entering that, it is responding as stated above.

Therefore, let's try entering the aforementioned payload in both fields.



← → ↻ redtiger.labs.overthewire.org/level2.php

**Welcome to level 2**

A simple loginbypass

Target: Login  
Hint: Condition

Username:

Password:

Login

Some things are disabled!

We receive the message "Some things are disabled!" after entering the aforementioned payload in the response.

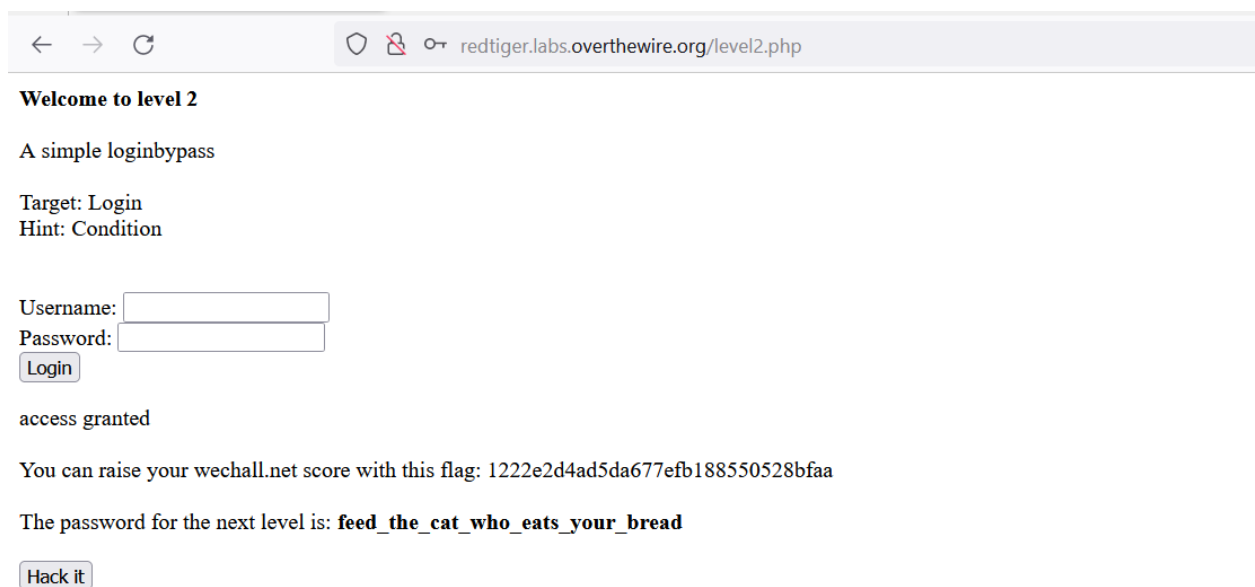
We can infer from the above response that something is being blocked from our payload.

So let's attempt to alter the payload in order to avoid the WAF.

Let's substitute "#" for the comment "--" so that the payload would be

A" OR 1=1-- -

Let's Execute the Payload in the Both field



← → ↻ redtiger.labs.overthewire.org/level2.php

**Welcome to level 2**

A simple loginbypass

Target: Login  
Hint: Condition

Username:

Password:

Login

access granted

You can raise your wechall.net score with this flag: 1222e2d4ad5da677efb188550528bfaa

The password for the next level is: **feed\_the\_cat\_who\_eats\_your\_bread**

Hack it

As you can see, we have the key to the subsequent level.

Thank you I hope you got to learn something out of it.