in robots.txt we see admin.phps are not allowed

we find three files

index.phps

cookie.phps

authentication.phps

we can use **gobuster dir -u [target ip] -w [wordlist]** for finding these pages

**gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php -u http://mercury.picoctf.net:2148**

these files contains mutiple php function

there is a deserialization vulnerability in these code



here we can see we can send a serialised object of access\_log class. As the object will not have the is\_guest() function it will call die() in catch

This will print $perm, the \_\_toString method of our access\_log object is called, which displays the content of whatever filename (the value of access\_log) was passed to it.

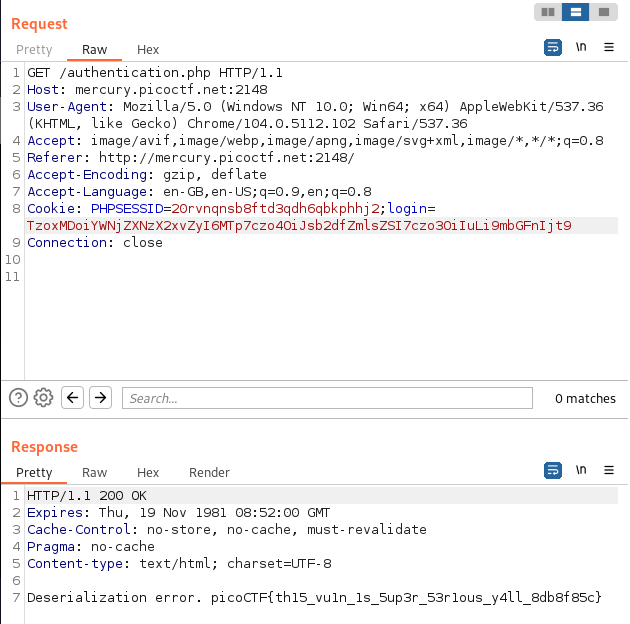
We will make a php object -

O:10:"access\_log":1:{s:8:"log\_file";s:7:"../flag";}

encode that to base64 and url encode

TzoxMDoiYWNjZXNzX2xvZyI6MTp7czo4OiJsb2dfZmlsZSI7czo3OiIuLi9mbGFnIjt9

Finally we will make the authentication request with login cookie as this



Flag: picoCTF{th15\_vu1n\_1s\_5up3r\_53r1ous\_y4ll\_8db8f85c}