

0CTF2018 Easy User Manager System writeup

原创

[1CHIGO](#) 于 2018-04-05 21:42:42 发布 373 收藏

分类专栏: [writeup WEB](#) 文章标签: [web ctf writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Jerryzhu369/article/details/79829192>

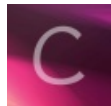
版权



[writeup](#) 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏



[WEB](#)

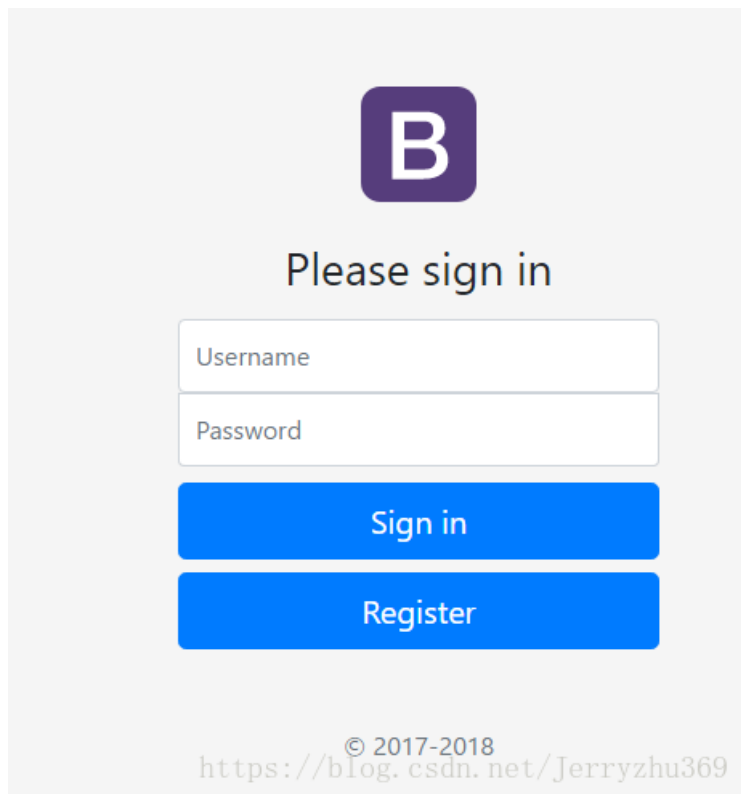
9 篇文章 0 订阅

订阅专栏

菜的不行, 比赛时进入了登录页面后要修改ip时完全没有思路, 只能水一水等比赛结束看师傅们的WP这样子, 我什么时候才能像师傅们一样优秀。

参考了<https://www.cnblogs.com/Mrsm1th/p/8719328.html>。

首先打开链接, 登录页面如下:



The image shows a login page for a system. At the top center is a purple square icon with a white letter 'B'. Below the icon, the text 'Please sign in' is displayed. There are two input fields: 'Username' and 'Password'. Below the input fields are two blue buttons: 'Sign in' and 'Register'. At the bottom of the page, there is a copyright notice: '© 2017-2018' and a URL: 'https://blog.csdn.net/Jerryzhu369'.

可知需要登录后才可以进行下一步。

首先注册, 发现服务器会向所填写的ip地址的80端口发送一条消息, 于是监听80端口

Register

Please use your ip instead of phone
We will send a http request to 80 port
with verify code!

Register

<https://blog.csdn.net/Jerryzhu369>

登陆一下，得到vcode:

```
root@vultr:~# nc -lp 80
HEAD /?2f5be42102054cafd25af005575de0b4 HTTP/1.1
Host: 108.61.212.230
Accept: */*
root@vultr:~# https://blog.csdn.net/Jerryzhu369
```

登陆一下，得知需要将ip地址变为8.8.8.8才可以的到flag。

Hello 1chig09(108.61.212.230)

You can change your phone [here](#).

If you make your phone to be 8.8.8.8, I will give you a flag.

<https://blog.csdn.net/Jerryzhu369>

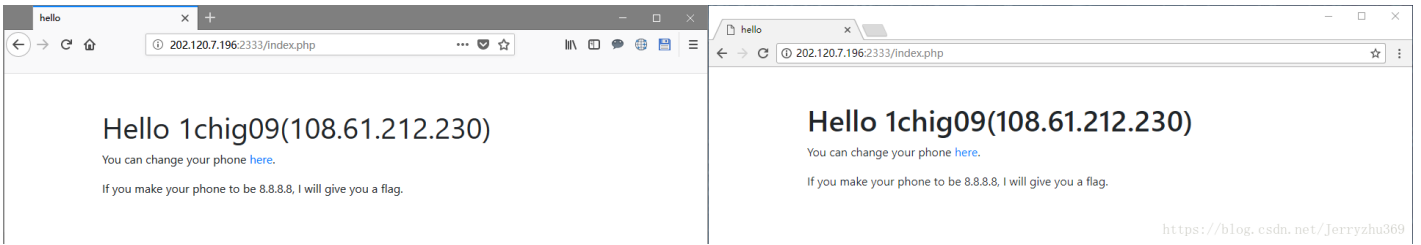
点开修改ip得到界面，知道要输入字符串，字符串的md5加密后的字符串的前六位与所给字符相一致。

可以用脚本跑一下

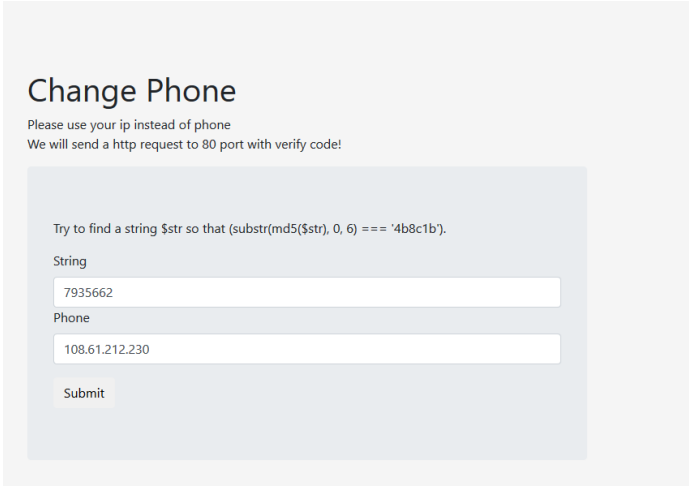
```
import hashlib
vcode_md5="113d07"
print(vcode_md5)
key=""
for i in range(1,999999999):
    md5_key=hashlib.md5(str(i).encode("utf-8")).hexdigest()
    #print(md5_key)
    first_md5=md5_key[0:6]
    #print(first_md5)
    if vcode_md5==first_md5:
        print(i)
        print(md5_key)
        key=str(i)
        break
```

以上是比赛时做到的，接下来是赛后看师傅们的wp得到的思路。

接下来打开两个浏览器分别登录刚刚注册成功的账号，



同时点开修改ip地址（phone），在其中一个浏览器中填写自己的ip地址，另一个填写8.8.8.8。

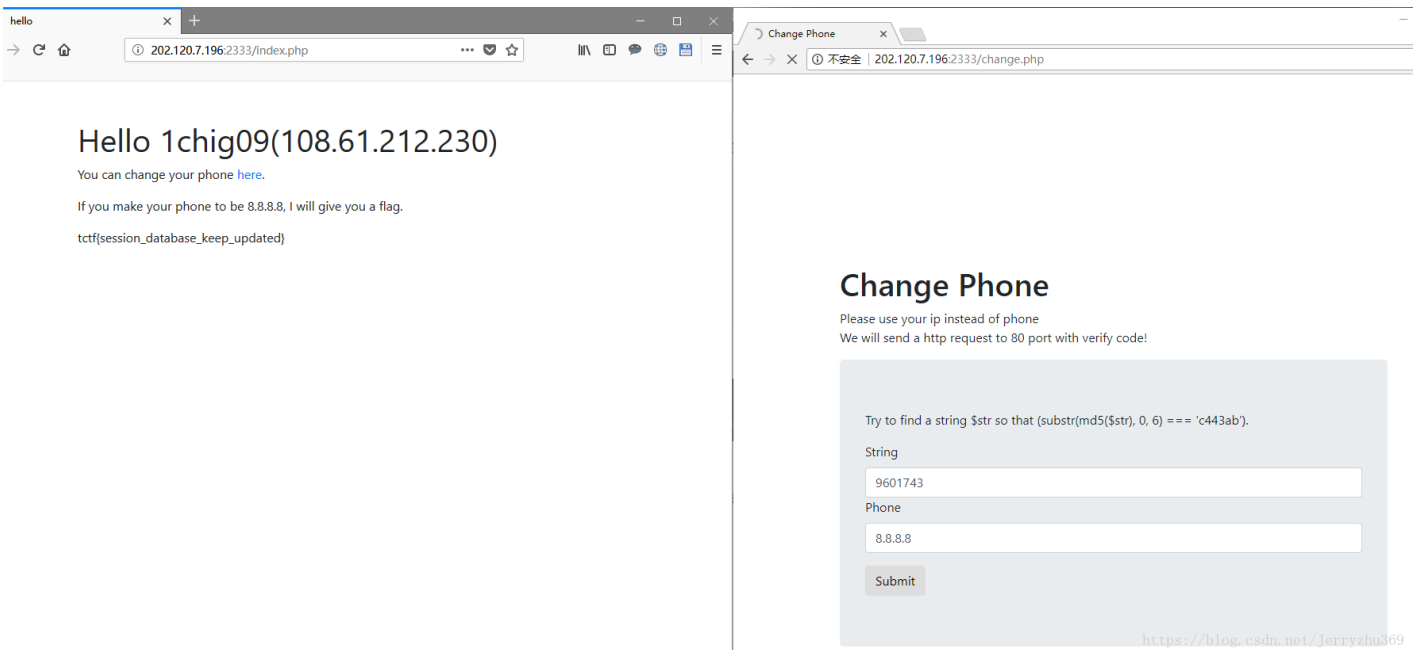


首先提交发送信息到本地ip的请求，得到vcode:

```
root@vultr:~# nc -lp 80
HEAD /?99e22eeb51f2782de4041770f2aec8fb HTTP/1.1
Host: 108.61.212.230
Accept: */*
tctf[session_database_keep_updated]
```

将得到的vcode输入，但是注意，此时不要提交。

将另一个浏览器即输入ip地址为8.8.8.8的请求提交，然后在其发送验证码之前转回另一浏览器将其提交，得到flag。



总结:

这里用到的是一个cookie混淆的漏洞，原理是在一个过程中(登录,密码重置)，可以使cookie相关联来达到欺骗服务器的效果。再甩出一篇大佬的博文：<http://www.freebuf.com/articles/web/162152.html>

大概就是这样子了。