

【bugku_writeup】web31 好像需要管理员

原创

kzaaa 于 2021-01-01 16:48:47 发布 262 收藏 2

分类专栏: [ctf_bugku_writeup](#)

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/kongzhian/article/details/112061433>

版权



[ctf_bugku_writeup](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

初识题目



Something error:

404 Not Found

No such file or directory.

Please check or [try again](#) later.

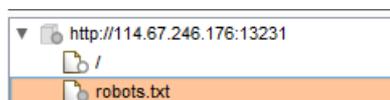
Generated by [kangle/3.5.5](#).

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

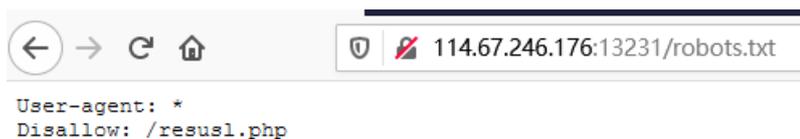
啥也没有, 点击try again也一样

解题思路

没什么思路, 有burpsuite的spider扫一下



有robots.txt, 打开看看



发现一个php文件, 打开看看

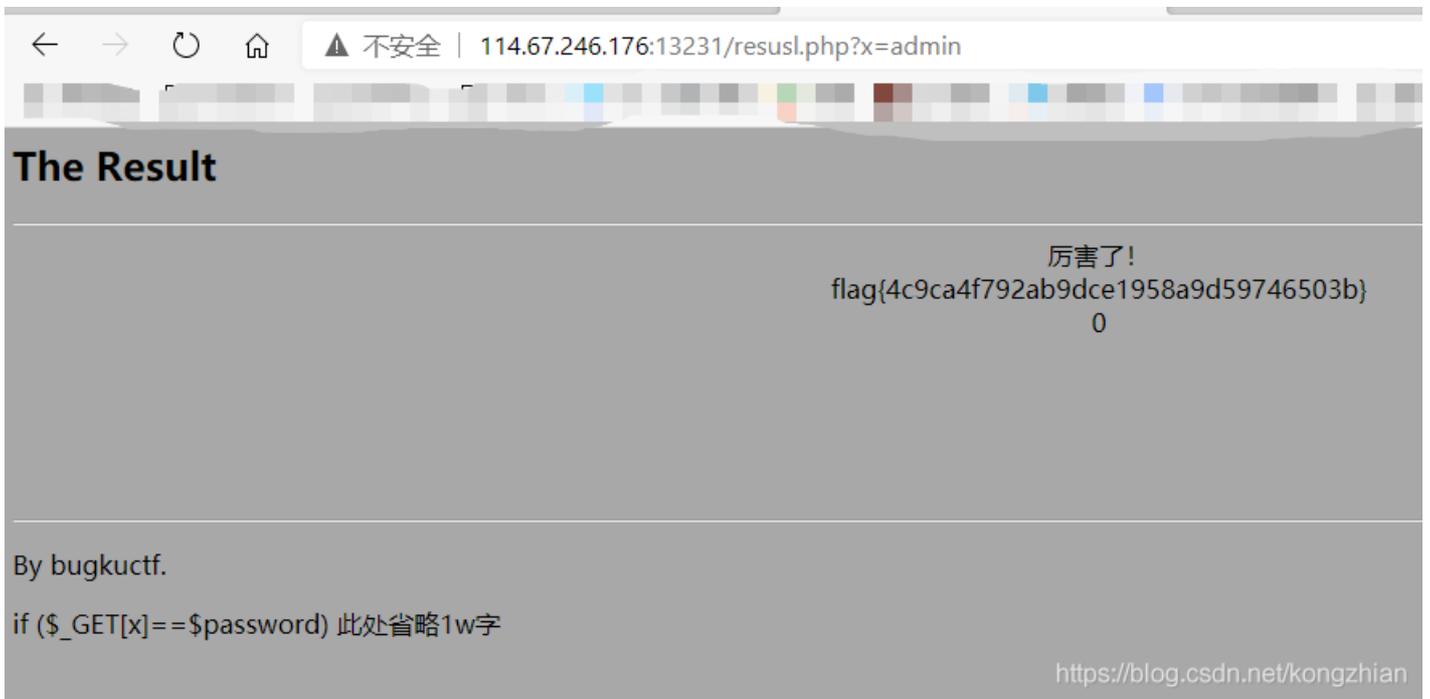


有点东西，其次还发现一个问题

```
<html>
  <head> </head>
  <body bgcolor="#A8A8A8">
    <h2>The Result</h2>
    <hr \="">
    <div align="center">
      <h3>warning:你不是管理员你的IP已经被记录到日志了</h3>
      <br>
      <h2>157.122.68.227</h2>
    </div>
    <br>
    <br>
    <br>
    <br>
    <br>
    <br>
    <hr \="">
    <p>By bugkuctf.</p>
    <p>if ($_GET[x]==$password) 此处省略1w字</p>
    <div id="cntvlive2-is-installed"></div>
  </body>
</html>
```

溢出是啥来的？当然，只在火狐上有溢出提示，先不管，其实也没什么作用

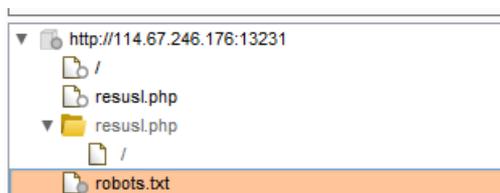
由于有if判断语句，目前没有设GET参数id，这个页面应该是不符合if正确的，由于有个x和password对比，猜测一下可能是判断是不是管理员，传参id=admin



就这??? (虽然太难的我也不会)

再提一句:

不过上面的resul.php不用通过robots.txt找到, 因为



当然, 我们应该知道利用robots.txt发现隐藏的页面