

BugkuCTF-web-前女友 writeup

原创

会下雪的晴天 于 2019-07-13 13:38:14 发布 442 收藏

分类专栏: [CTF做题记录](#)

会下雪的晴天

本文链接: https://blog.csdn.net/weixin_43578492/article/details/95743049

版权



[CTF做题记录](#) 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

题目描述

题目传送门: <http://123.206.31.85:49162/>



解题思路

打开链接一大段文字，，，没什么有用的，，，嗯，PHP是世界上最好的语言

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！”

它真的是链接。。。

“还记得你曾经说过.....”

PHP是世界上最好的语言 https://blog.csdn.net/weixin_43578492

老套路，先看看源码再说

```
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
```

https://blog.csdn.net/weixin_43578492

不看源码还真是看不出来这有个链接，打开这个隐蔽链接后得到：

```

<?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($v2)){//v1与v2的值要不一样，但是他们经过md5加密后又一样
        if(!strcmp($v3, $flag)){//strcmp() 函数比较两个字符串（区分大小写），相同则返回0
            echo $flag;
        }
    }
}
?>

```

- 因为md5不能处理数组，如果md5处理数组则为NULL，那么我们可以将v1,v2写成数组传入即可
- strcmp()函数,要想v3和flag相同，我们也可以将v3写成数组绕过

得到FLAG

综上，构造payload

```
http://123.206.31.85:49162/index.php?v1[]=1&v2[]=2&v3[]=3
```

The screenshot shows a web browser window with the URL `http://123.206.31.85:49162/index.php?v1[]=1&v2[]=2&v3[]=3`. The page content is a story:

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

SKCTF{Php_1s_th3_B3St_L4NgUag3}

Below the browser window, there is a tool interface with a 'Load URL' field containing the same URL and an 'Execute' button. The tool also has checkboxes for 'Post data', 'Referer', 'User Agent', and 'Cookies', and a 'Clear All' button.

END



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)