

[ACTF2020 新生赛]Upload(文件上传)

原创

[前方是否可导?](#)

于 2020-09-18 20:44:19 发布 482 收藏

分类专栏: [web](#)

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_44110537/article/details/108672641

版权



[web 专栏收录该内容](#)

20 篇文章 0 订阅

订阅专栏

先尝试直接上传一句话木马,发现果然不行。

一开始觉得可能只是后端进行检测,但是发现流量还没有发出去就提示上传的文件错误,说明在前端就进行了检测。

搜索 HTML

```
<body>
  <div class="sitemakers">
    <div class="wrap">
      <svg class="bulb" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px"
        y="0px" width="128px" height="128px" viewBox="0 0 128 128" enable-background="new 0 0 128 128" xml:space="preserve">
      </div>
      <div class="light">
        <span class="glow">
          <form enctype="multipart/form-data" method="post" onsubmit="return checkFile();" >
        </span>
        <span class="flare"></span>
      </div>
    </div>
  </div>
```

把检测的checkFile()函数删掉。

然后上传一个phtml后缀的一句话木马,通过蚁剑链接即可。

名称	日期	大小	属性
uev	2020-09-18 12:24:23	340 B	0755
etc	2020-09-18 12:24:23	66 B	0755
home	2018-10-20 10:40:06	6 B	0755
lib	2019-01-22 21:46:40	30 B	0755
lib64	2019-01-22 15:00:00	34 B	0755
media	2019-01-22 15:00:00	6 B	0755
mnt	2019-01-22 15:00:00	6 B	0755
opt	2019-01-22 15:00:00	6 B	0755
proc	2020-09-18 12:24:23	0 B	0555
root	2019-01-23 00:10:45	6 B	0700
run	2019-01-22 21:56:17	21 B	0755
sbin	2019-01-22 21:56:09	20 B	0755
srv	2019-01-22 15:00:00	6 B	0755
sys	2020-08-30 02:38:45	0 B	0555
tmp	2020-09-18 12:31:22	6 B	1777
usr	2019-01-22 15:00:00	19 B	0755
var	2019-01-22 21:56:12	17 B	0755
.dockerenv	2020-09-18 12:24:23	0 B	0755
flag	2020-09-18 12:24:24	43 B	0644