

Uploadddd

发表于 2021-01-04 分类于 [Challenge](#) , [2017](#) , [赛客夏令营](#) , [Web Challenge](#) | [2017](#) | [赛客夏令营](#) | [Web](#) | [Uploadddd](#)

[点击此处](#)获得更好的阅读体验

来源

本 WP 来自 spaceman 原创投稿

题目考点

- 目录扫描
- 源码审计

解题思路

尝试直接上传一句话木马，发现木马文件是可以上传，但是路径不知道

□

于是扫描了一下目录。发现 `index.php.swp`、`flag.php`，`swp` 文件需要恢复

```
1 vim -r index.php.swp
```

得出源码

```
1 <?php
2 if (isset($_POST['submit'])) {
3     $file_path = "uploads/";
4     $file_name = date("YmdHis") . rand(0,999) . ".php";
5     move_uploaded_file($_FILES["file"]["tmp_name"], $file_path . $file_name);
6     echo "上传成功!";
7 }
8 ?>
9 <!DOCTYPE html>
10 <html lang="en">
11 <head>
12     <meta charset="UTF-8">
13     <title>Web03</title>
14 </head>
15 <body>
16     <form action="index.php" method="post" enctype="multipart/form-data">
17         <input type="file" name='file'>
18         <input type="submit" name="submit" value="上传" />
19     </form>
20 </body>
21 </html>
```

可以看出上传的路径了 `uploads`，但是文件名更改为时间，还加了随机数，我本地搭建了一个，先尝试去掉随机的，可以发现是以时间命名，与提交的时间一样

□

再加上随机的，这次随机的数是900

□

这就一目了然了，随机数只能爆破了

□

时间 20200818141506+0-999 随机数.php，所以先写一个脚本生成字典

```
1 time = '20200818141506' #时间
2 s = ''
3 for i in range(1000):
4     s += time+str(i)+'.php'
5     s += '\n'
6     print (time+str(i)+'.php')
7 filename = 'dir.txt'
8 with open(filename,'a',encoding='utf-8') as f:
9     for i in s:
10         f.writelines(i)
```

然后再使用Bp跑

□

然后再复制字典粘贴上去，启动

□

最后跑完，排一下（It is ok！是我在一句话中自己添加的，为了方便确认上传是否成功）

□

蚁剑连接，html目录下拿到flag

□

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2017/赛客夏令营/Web/yKH6xziLNxoTpGiTt6Yfr.html>
- 版权声明：本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge # Web # 2017 # 赛客夏令营](#)
[beijing](#)
[无验证](#)