XCTF web Cat

原创

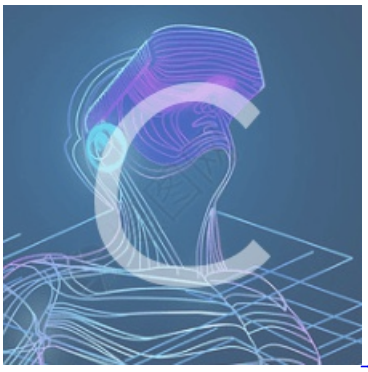
H4ppyD0g 于 2019-09-06 19:52:50 发布 392 收藏

分类专栏： CTF

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_42172261/article/details/100585526

版权



CTF 专栏收录该内容

45 篇文章 0 订阅

订阅专栏

题目提示输入loli.club，那就先输入，没有反应。

输入个127.0.0.1看看，报错，发现是执行ping命令

尝试使用管道进行命令执行127.0.0.1 && ls、127.0.0.0 || ls等等都不行。应该是行不通了。

然后发现每次输入都会在网址栏出现 **?url=...**

输入一个%79，结果被自动转换成y了，说明有url解码功能

输入%80看看，结果报错。

找到有一个目录路径：**/opt/api/dnsapi/views.py**

访问一下试试，没啥反应。

但是有一个**知识点**

使用@进行文件传递，对文件进行读取之后还会把内容传给url参数，如果像上面一样有超出解析范围的编码的时候就会得到错误信息。

加上@再次访问，又出现报错信息，搜索和和flag能有关系的关键字，最终database发现**database.sqlite3**

再访问这个目录，在搜索CTF即可。