BUUCTF系列 // Web ez题 Writeup

原创

Ga1axy_z 于 2020-09-28 17:53:26 发布 116 收藏

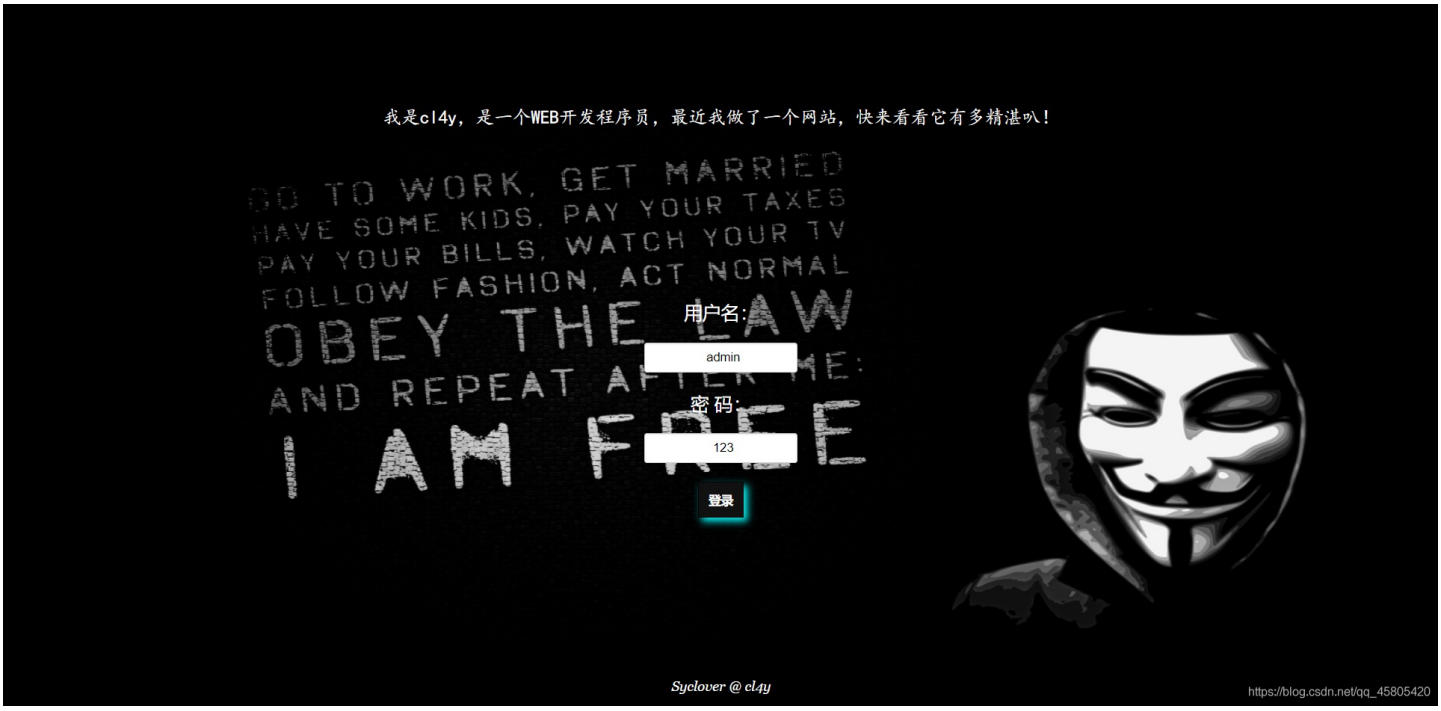
分类专栏： CTF

本文链接：https://blog.csdn.net/qq_45805420/article/details/108804093

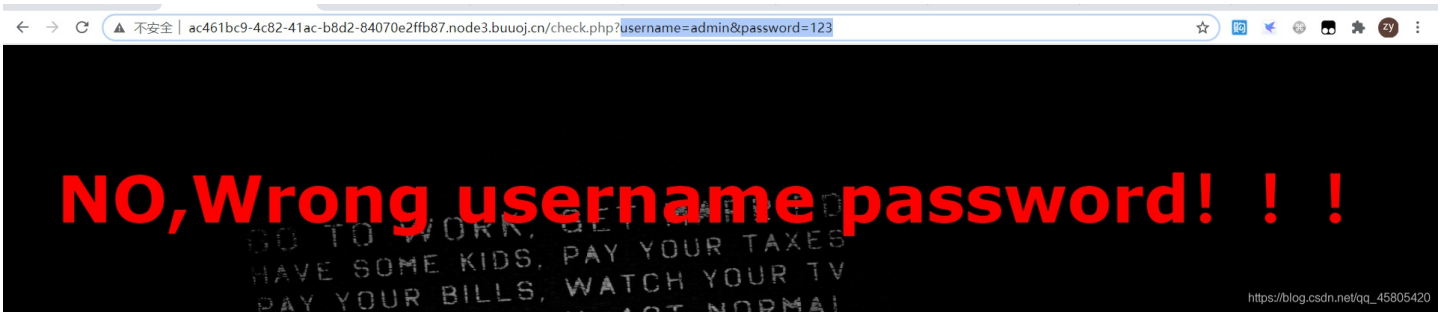
前言

本文主要包括 BUUCTF 里面一些比较简单的题

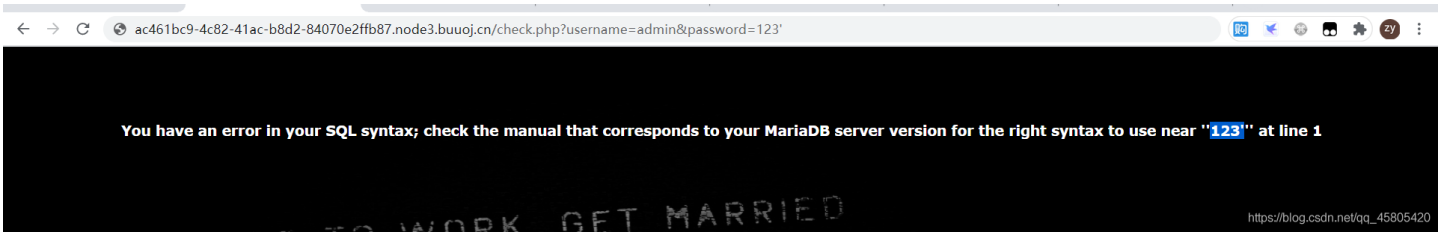
1` [极客大挑战 2019]EasySQL



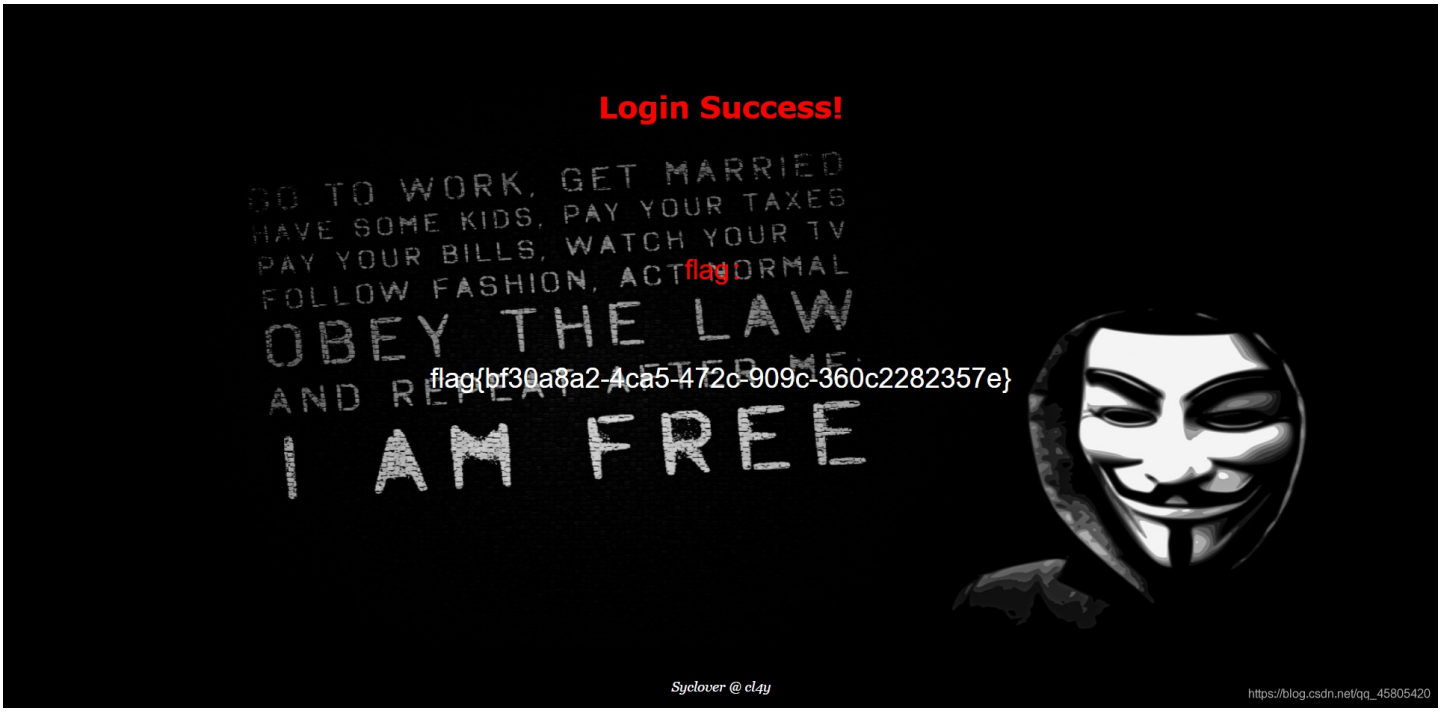
首先随便输个账号密码试试，发现回显只显示账号密码错误，没有得到什么有用的线索



接着尝试在密码后加上一个单引号，观察其回显



发现输入单引号后报错，由报错信息可知应该是字符型的注入，通过注释符号绕过即可得到 flag

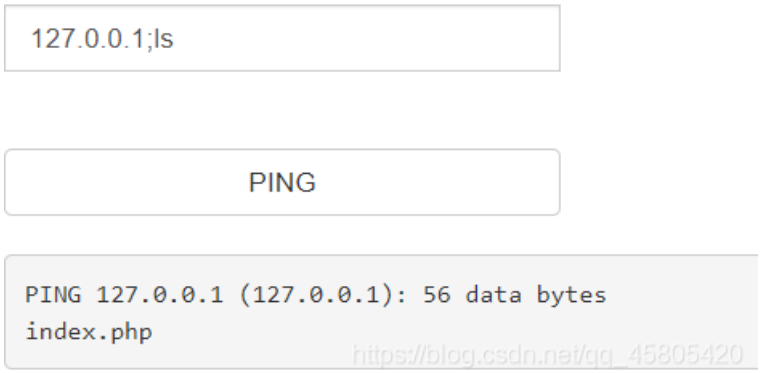


PS： 附上如何判断是字符型注入还是整形注入的 传送门

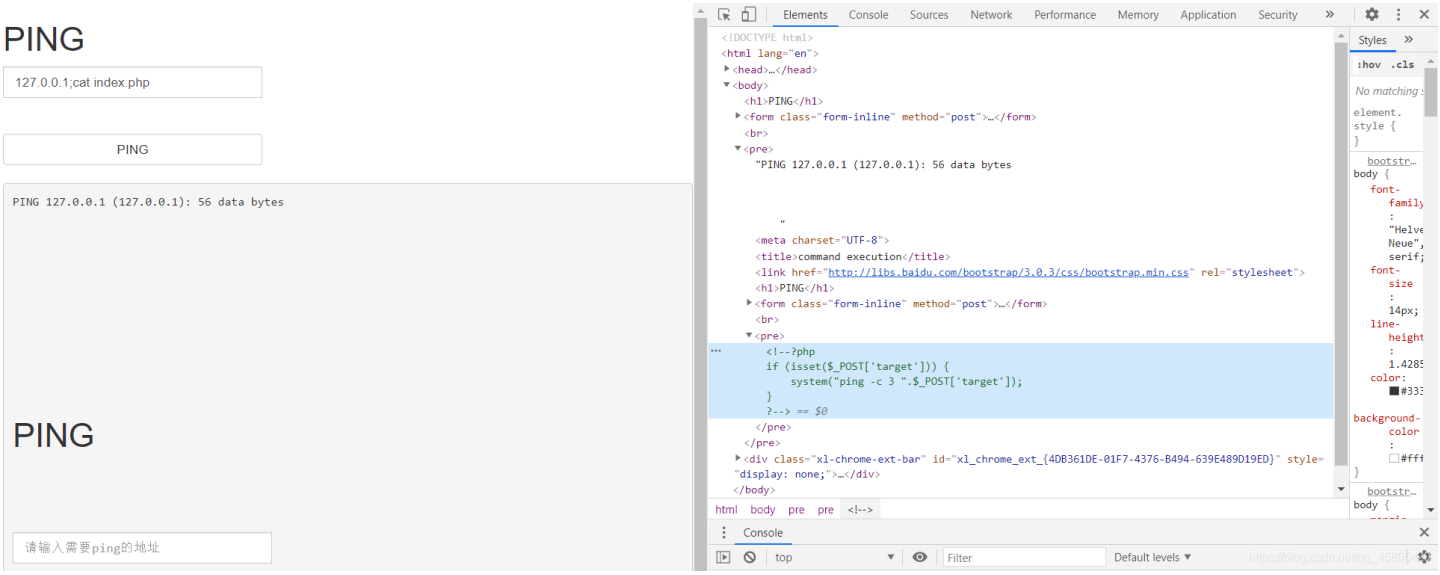
2` [ACTF2020 新生赛]Exec

打开题目，根据题型可以推测出本题应该是典型的命令执行漏洞

老规矩，先使用 ls 命令看看当前目录有没有什么提示



发现存在一个 ‘index.php’ 文件，不妨读取看看有没有什么线索



题目在该文件的源码注释中给出了后台执行命令的相关语句，可以看到题目没有对输入进行任何的过滤

除此之外该页面似乎是没有什么线索了，接着试试使用 ls 命令看看根目录下的文件

127.0.0.1;ls /

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

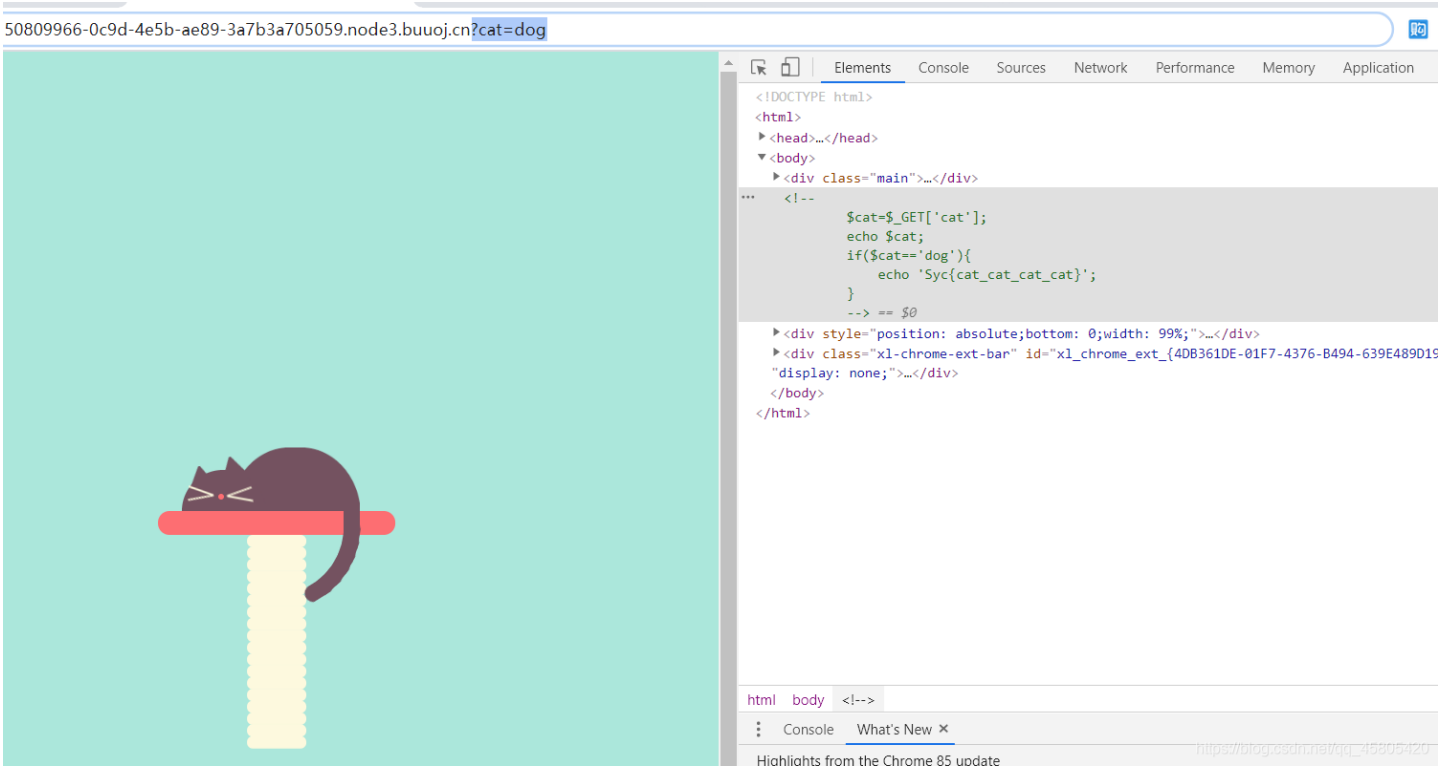

发现 flag 文件，使用 cat 命令读取即可得到 flag

127.0.0.1;cat /flag

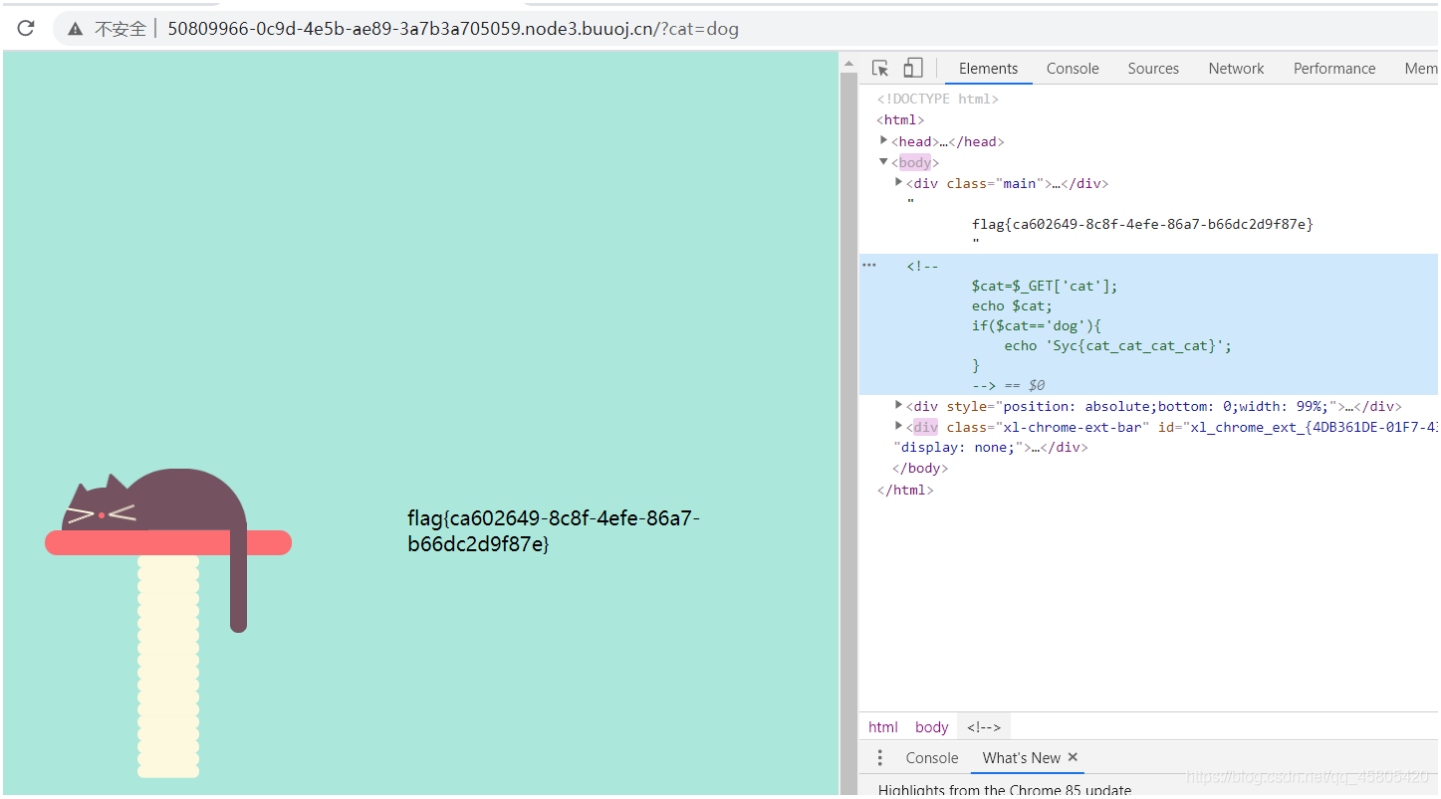
PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag{11152b38-bdef-4983-afaf-c57814c3f8bb}
```


3` [极客大挑战 2019]Havefun

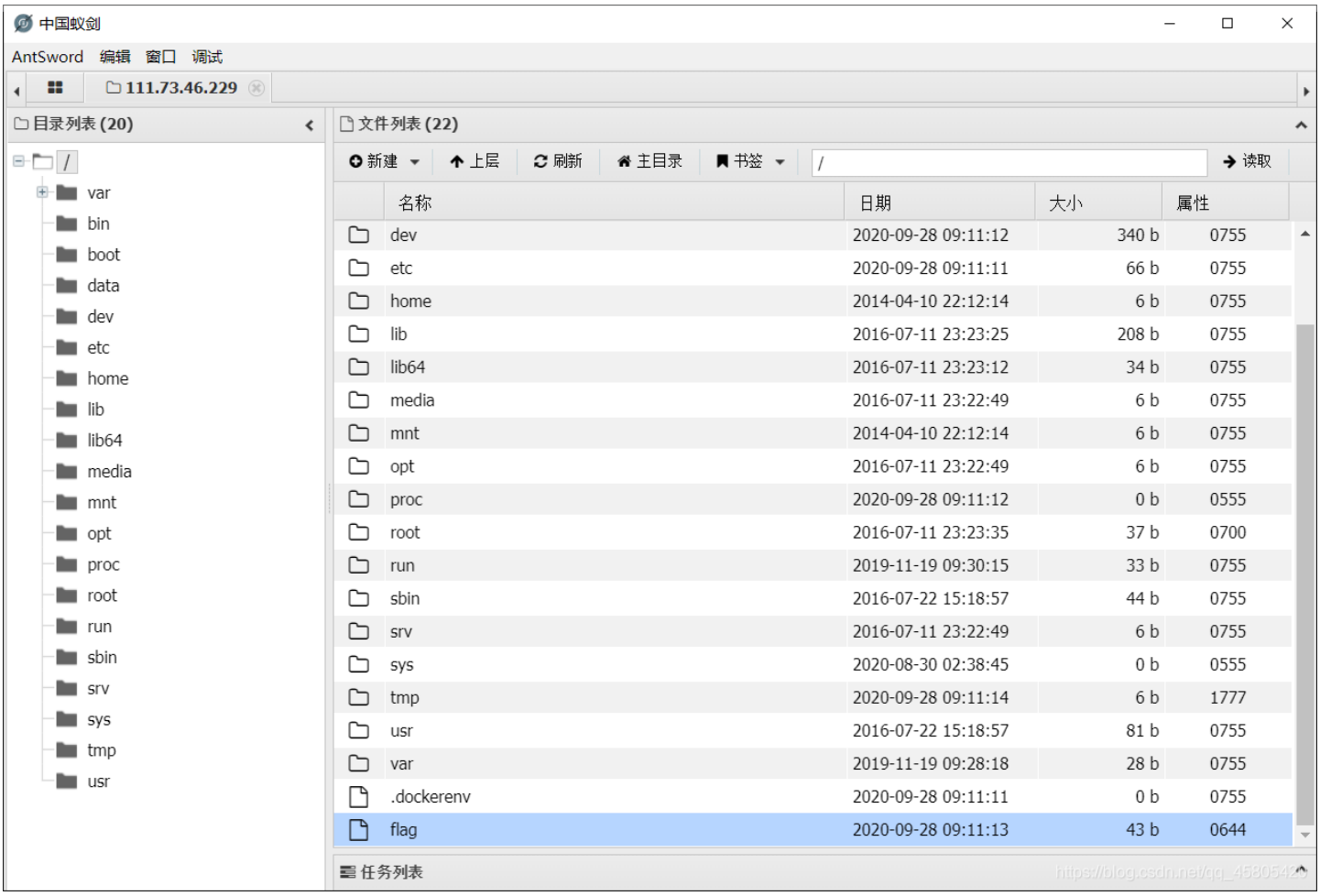


根据源码提示构造 URL 即可得到 flag

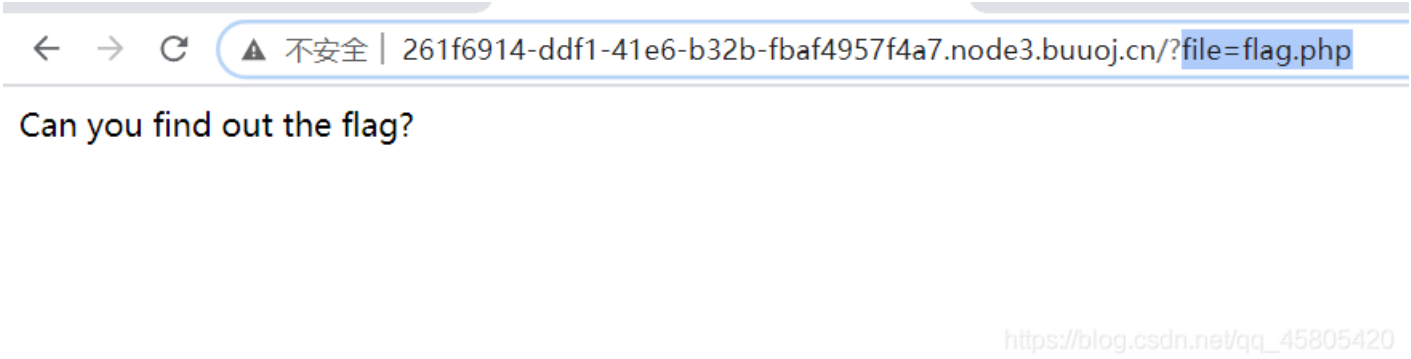


4` [极客大挑战 2019]Knife

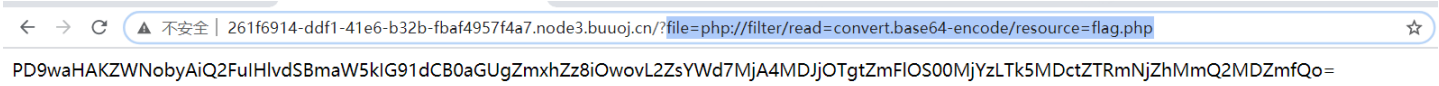
题目明显的提示是一句话木马，使用工具连接即可



5` [ACTF2020 新生赛]Include



结合题目名提示，考察点应该是文件包含漏洞，考虑到题目 URL 已经提示了 'flag.php' 文件，故尝试使用伪协议 `php://filter` 读取该文件内容



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MjA4MDJjOTgtZmFlOS00MjYzLTk5MDctZTRmNjZhMmQ2MDZmfQo=