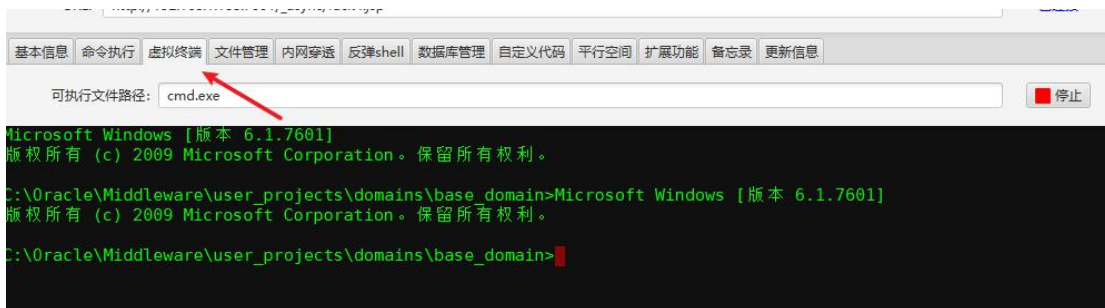
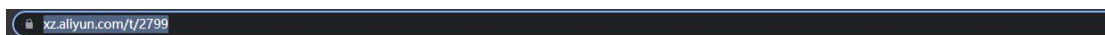


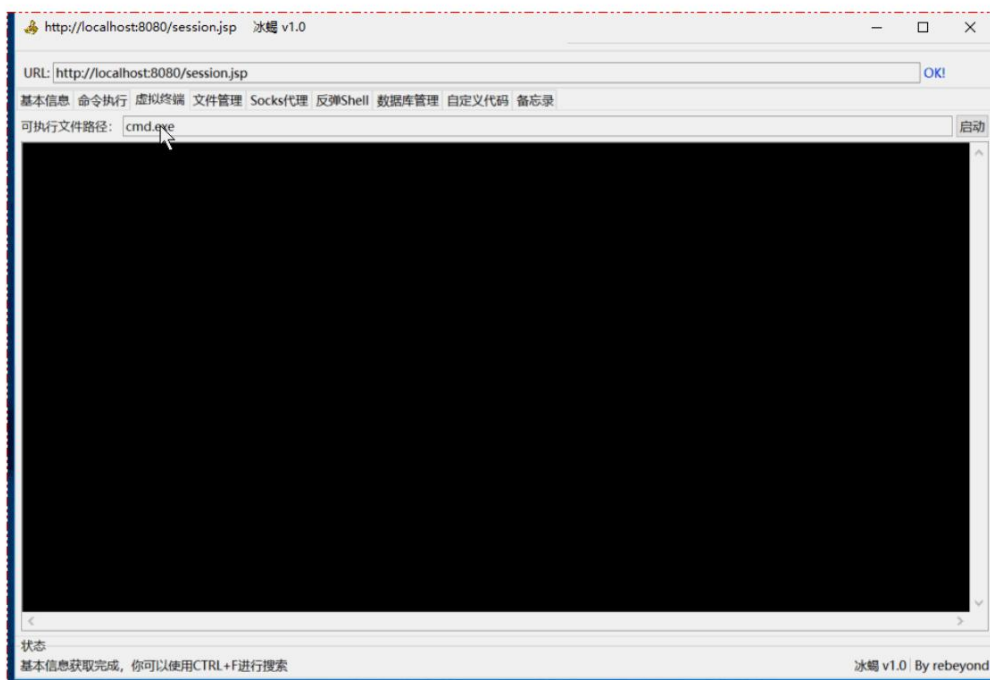
这里接《webserver 绕过 360 主动防御执行命令》这篇文章，顺带写一下冰蝎这个虚拟终端功能。



上次我说我猜测是他传了一个 cmd.exe，后来看了原作者 rebeyond 的文章，发现不是。
[//https://xz.aliyun.com/t/2799](https://xz.aliyun.com/t/2799)

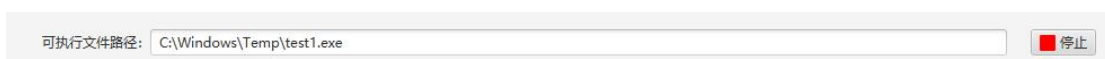


当然，如果你习惯powershell，也可以弹个powershell出来，如下图：



这里描述，可以弹 powershell，我就理解了，其实他就是直接调系统的接口，然后冰蝎这里把命令参数传进去。

这个 ，其实可以填写你想要的任何文件。
比如，我想执行我的马，那么填写上去。



然后这边直接上线了



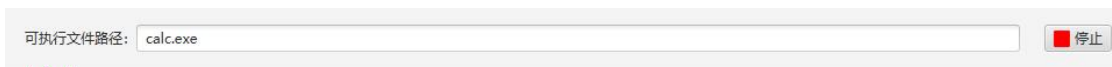
```
C:/Oracle/Middleware/user_projects/domains/base_domain/ >tasklist
```

映像名称	PID	会话名	会话#	内存使用
System Idle Process	0	Services	0	24 K
System	4	Services	0	368 K
smss.exe	264	Services	0	1,048 K
csrss.exe	348	Services	0	6,180 K
csrss.exe	400	Console	1	20,684 K
wininit.exe	408	Services	0	4,784 K
winlogon.exe	444	Console	1	5,652 K
services.exe	504	Services	0	9,308 K
lsass.exe	512	Services	0	15,016 K
lsm.exe	520	Services	0	6,184 K
svchost.exe	616	Services	0	9,560 K
vmacthlp.exe	676	Services	0	4,188 K
svchost.exe	720	Services	0	8,572 K
svchost.exe	800	Services	0	13,356 K
svchost.exe	856	Services	0	37,816 K
svchost.exe	896	Services	0	16,392 K
svchost.exe	940	Services	0	10,884 K
ZhuDongFangYu.exe	976	Services	0	27,680 K
svchost.exe	316	Services	0	17,840 K
svchost.exe	788	Services	0	13,308 K
spoolsv.exe	1172	Services	0	12,388 K
svchost.exe	1296	Services	0	9,216 K
sqlservr.exe	1540	Services	0	84,508 K
SMSvcHost.exe	1564	Services	0	24,868 K
ReportingServicesService.	1784	Services	0	73,288 K
sqlwriter.exe	1932	Services	0	6,684 K
VGAAuthService.exe	1980	Services	0	9,012 K
vmtoolsd.exe	2012	Services	0	21,216 K
svchost.exe	2040	Services	0	10,224 K
fdlauncher.exe	2164	Services	0	3,792 K
svchost.exe	2200	Services	0	7,696 K
svchost.exe	2244	Services	0	5,928 K
fdhost.exe	2296	Services	0	5,140 K
conhost.exe	2324	Services	0	2,704 K

主动防御是打开状态

通过这个虚拟终端的功能也可以绕 360，原理未知。

同理，也可以娱乐，比如



done

