Hack the ch4inrulz of Vulnhub

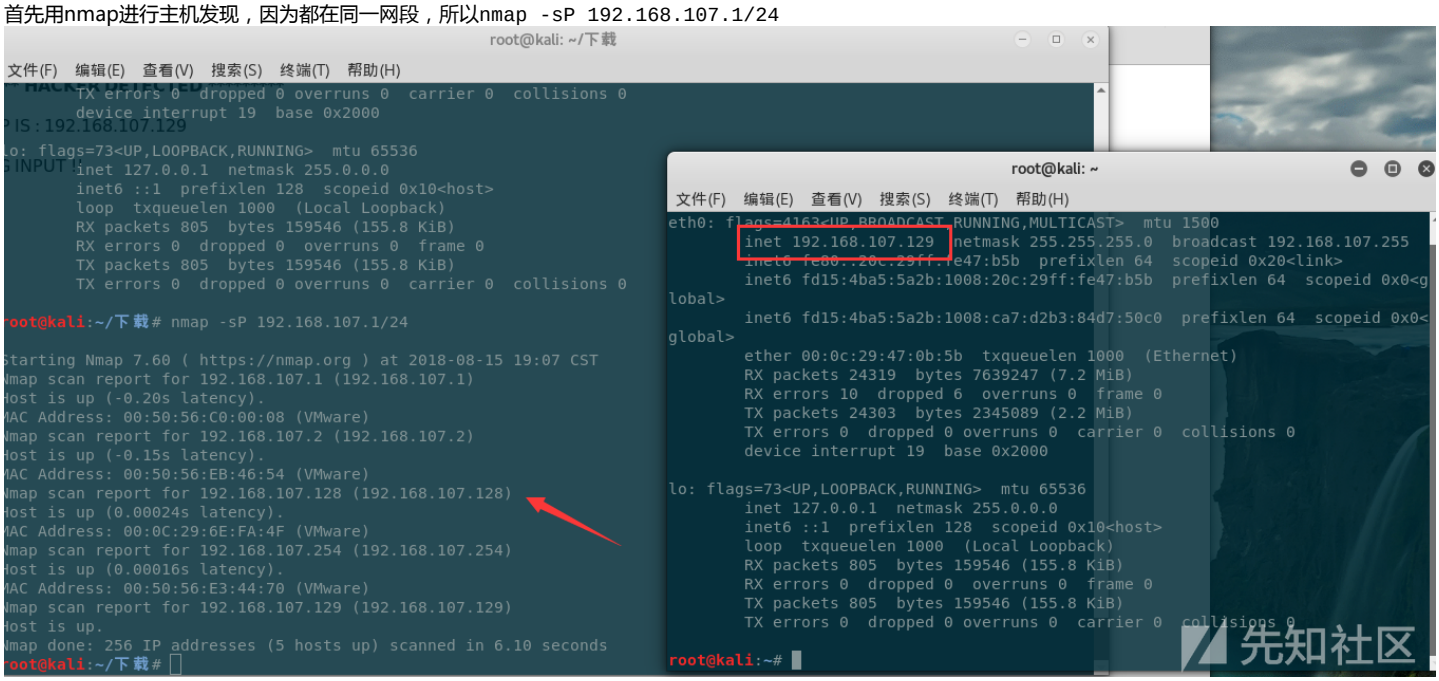
Hu3sky1 / 2018-08-17 11:27:34 / 浏览数 3682 技术文章 技术文章 顶(0) 踩(0)

环境说明

靶机环境 192.168.107.128
攻击机kali 192.168.107.129

主机发现

首先用nmap进行主机发现，因为都在同一网段，所以`nmap -sP 192.168.107.1/24`

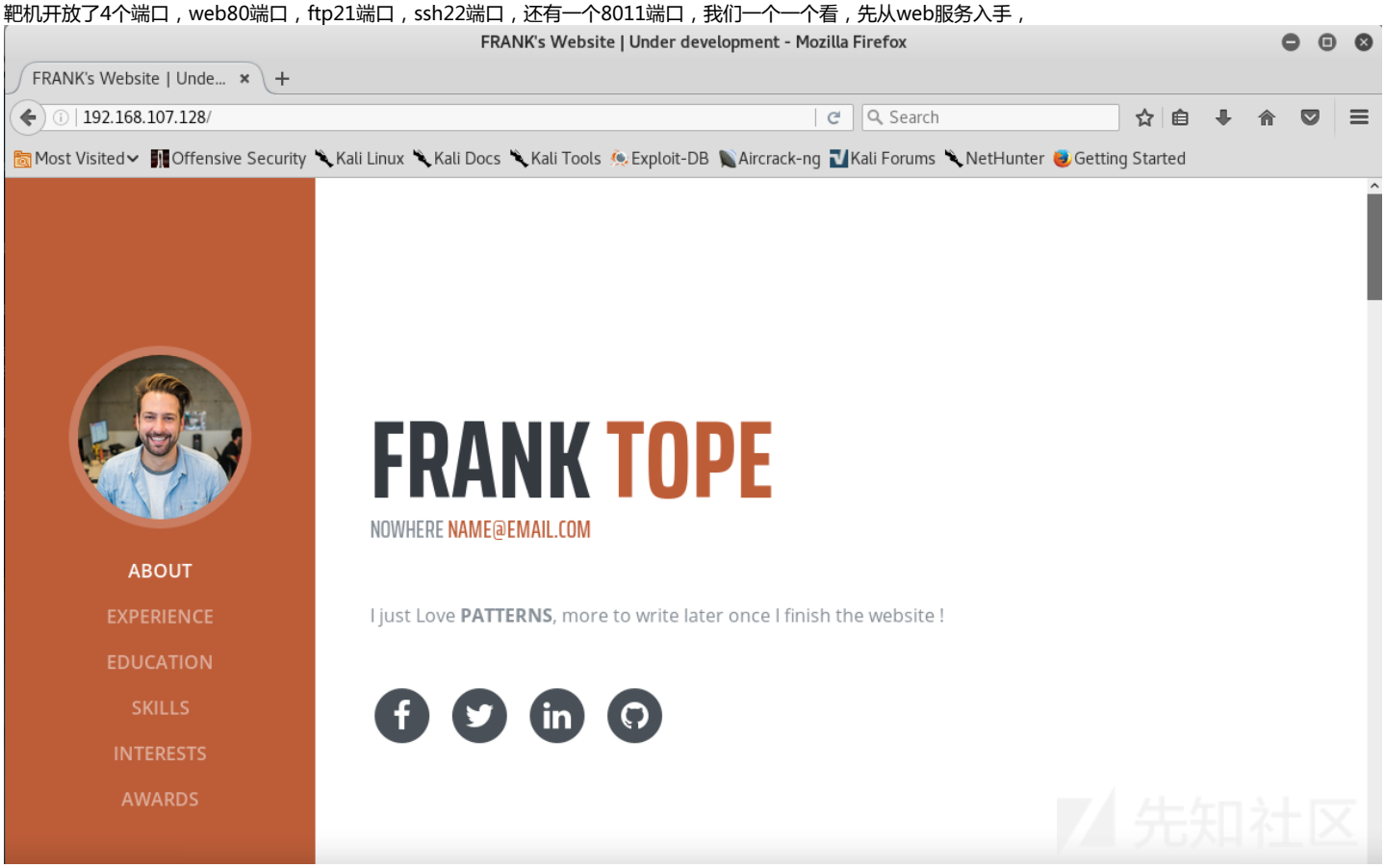


可以看到，本机ip是129，所以靶机自然就确定为192.168.107.128。

端口扫描

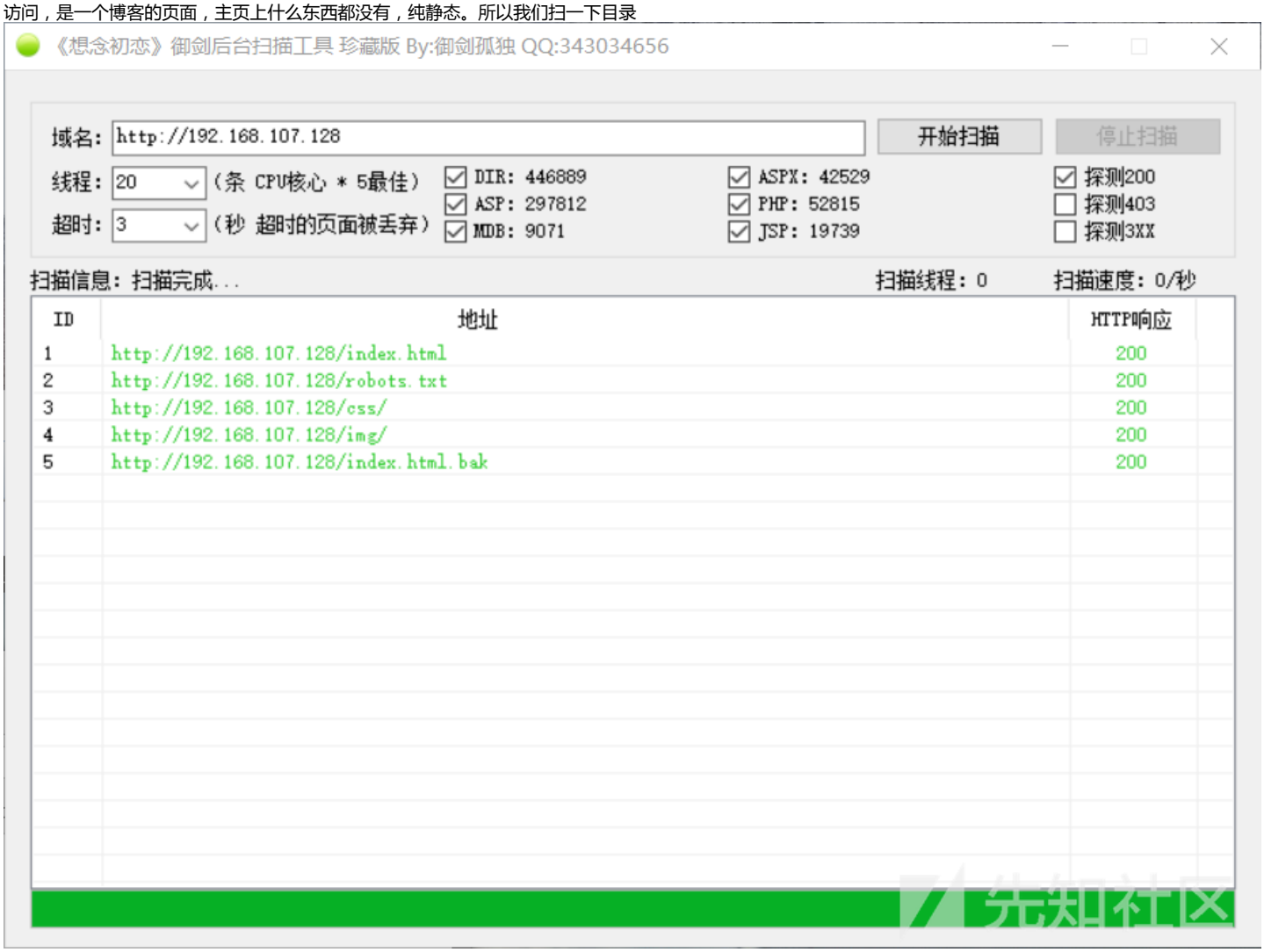
确定了靶机ip，就来确认一下开放的端口，使用nmap -sS -A 192.168.107.128

靶机开放了4个端口，web80端口，ftp21端口，ssh22端口，还有一个8011端口，我们一个一个看，先从web服务入手，

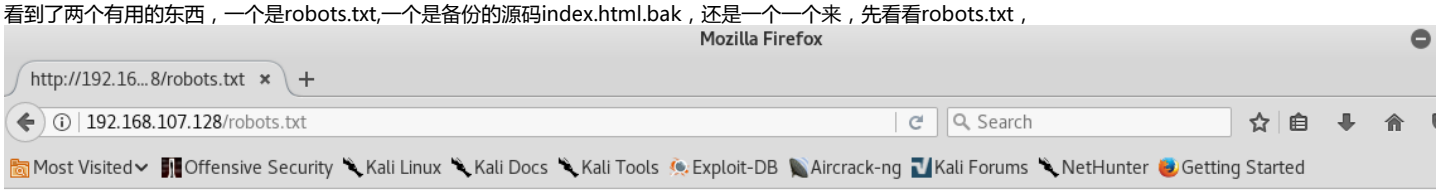


目录扫描

访问，是一个博客的页面，主页上什么东西都没有，纯静态。所以我们扫一下目录

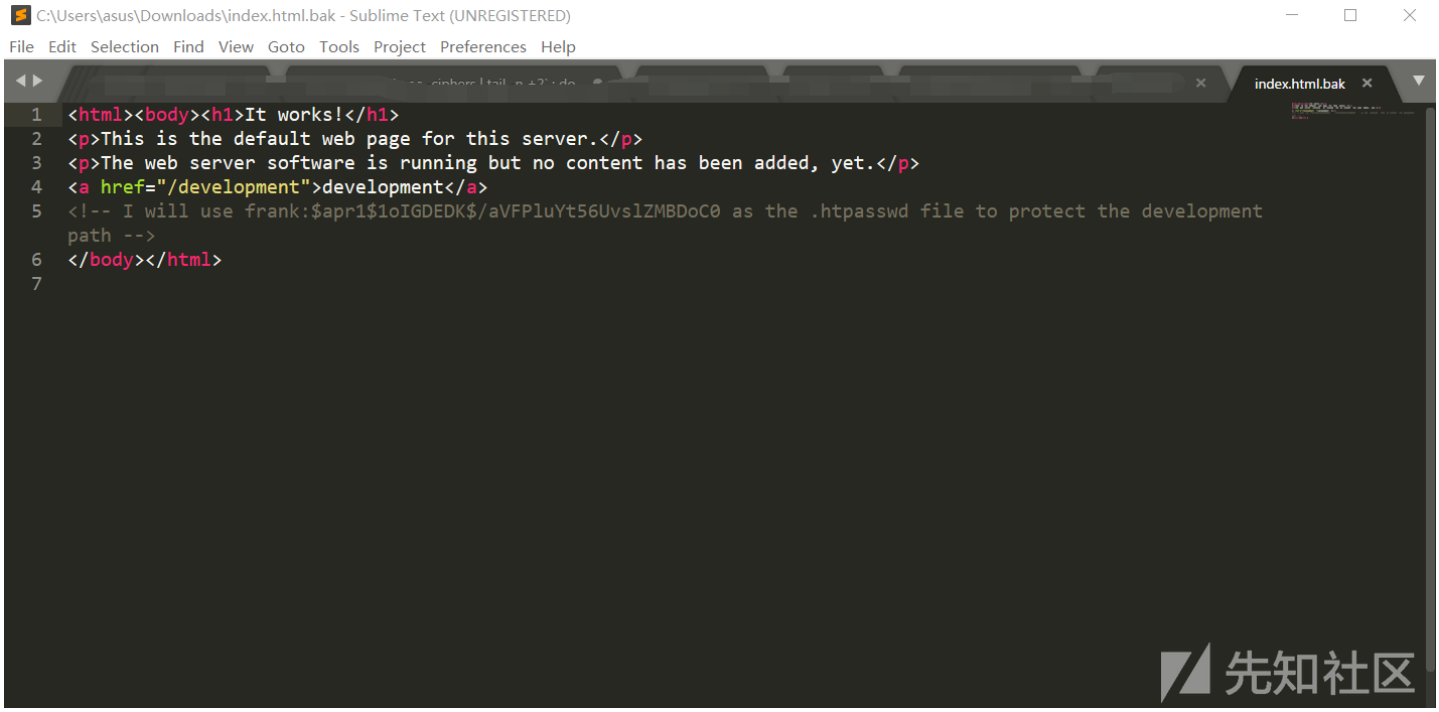


看到了两个有用的东西，一个是robots.txt,一个是备份的源码index.html.bak，还是一个一个来，先看看robots.txt，

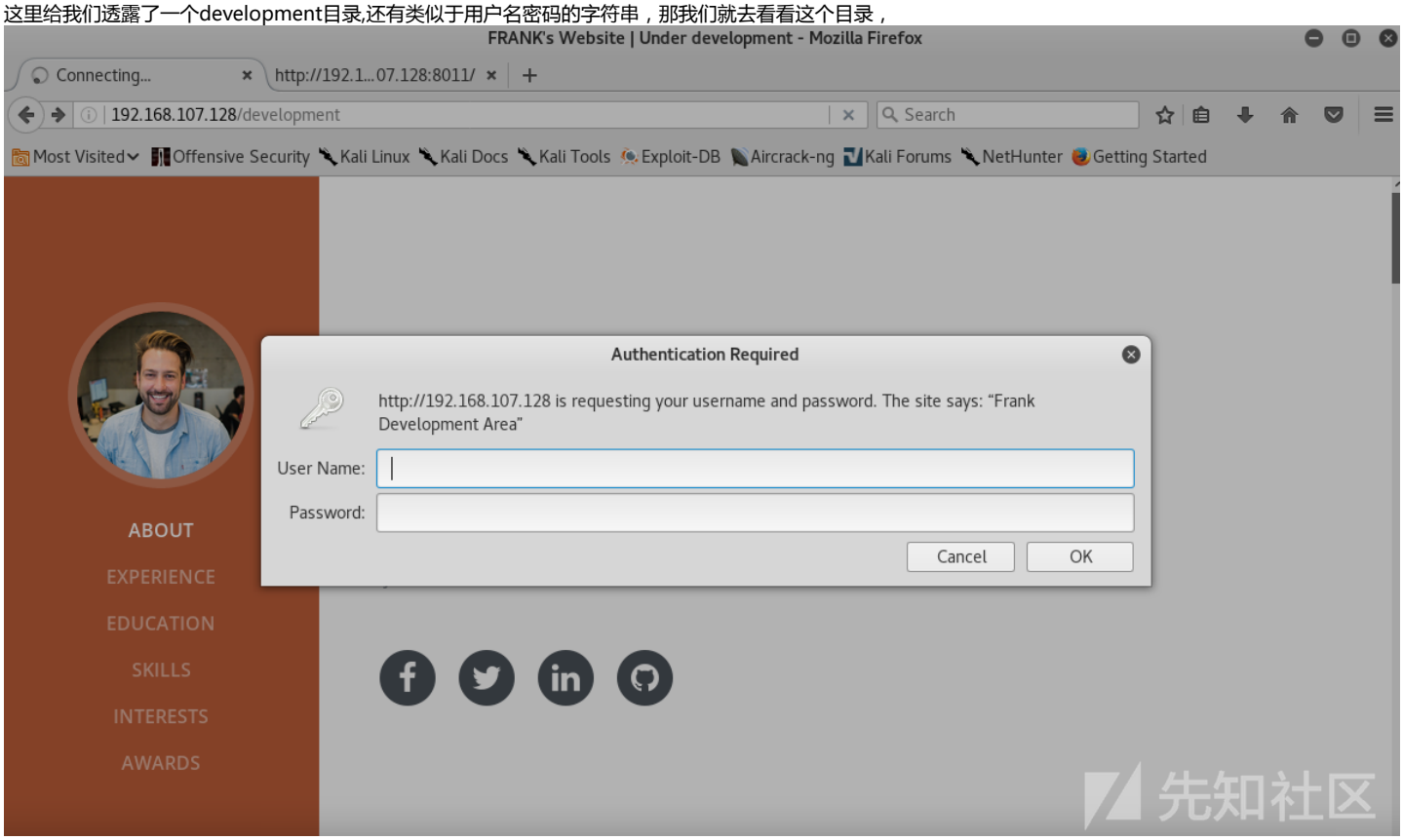


NOTHING here，yet！

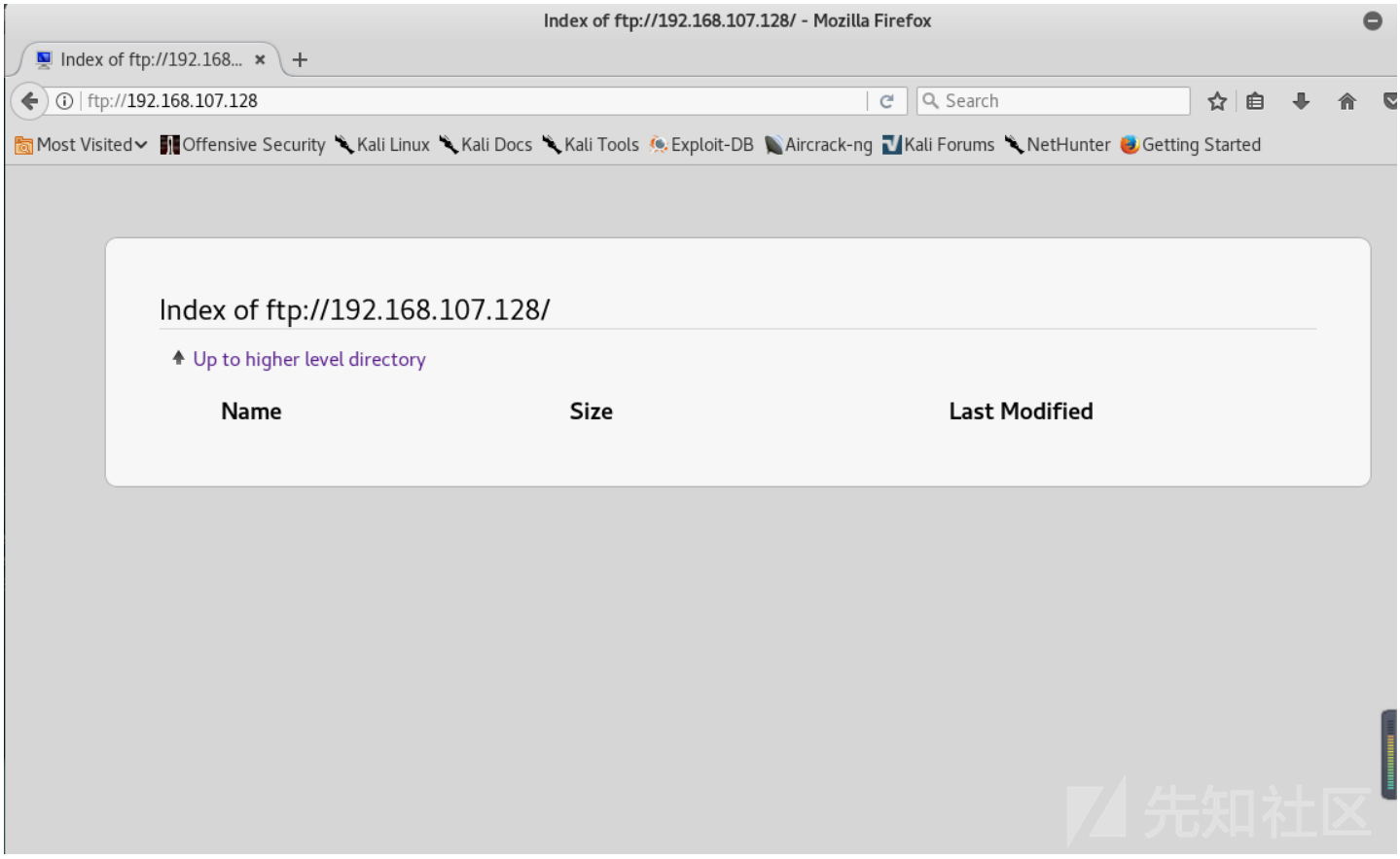
什么都没有，右键源码也是什么都没有，那就接着去看bak泄露的东西，下载下来，打开



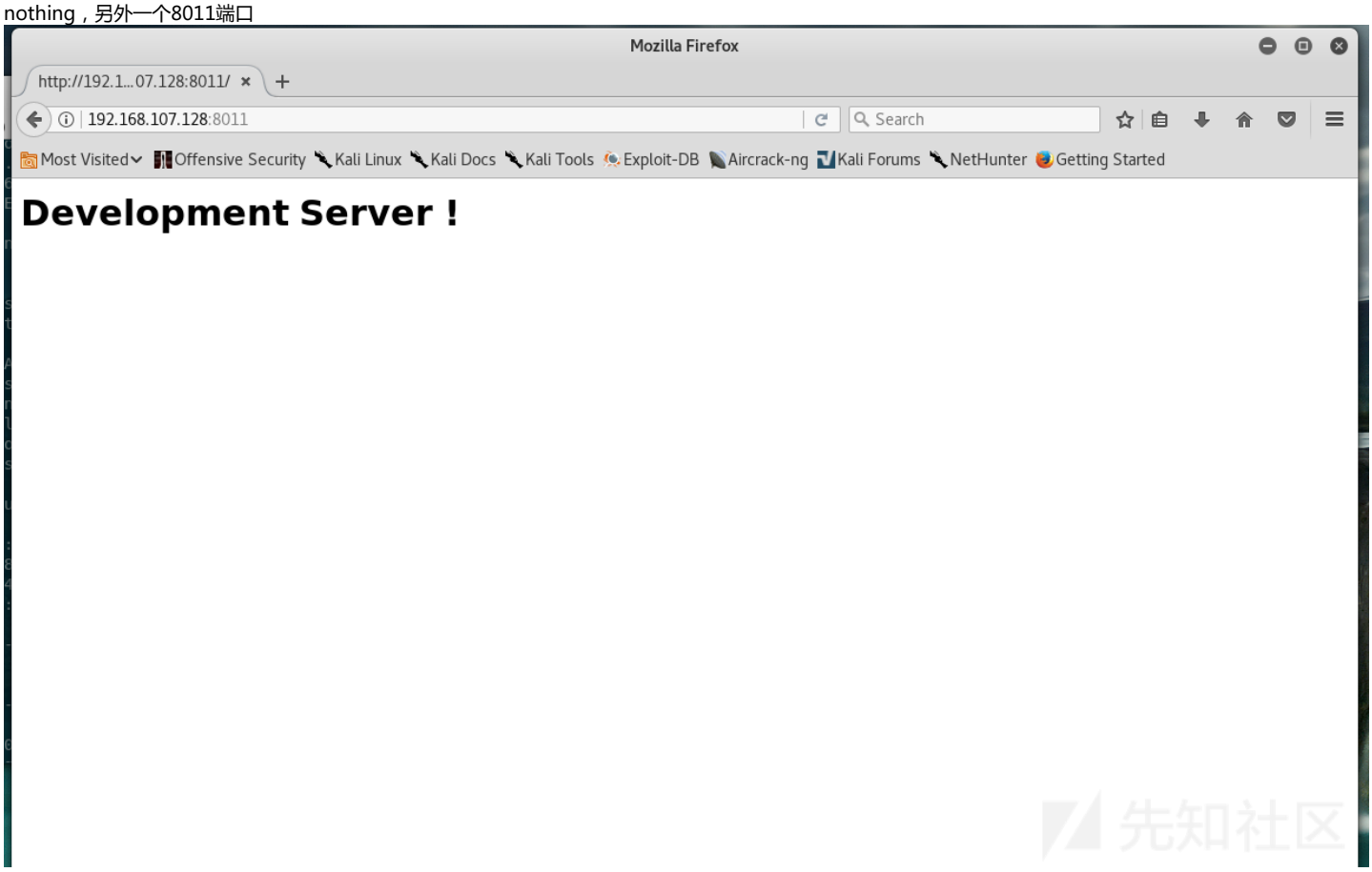
这里给我们透露了一个development目录,还有类似于用户名密码的字符串，那我们就去看看这个目录，



果然需要用户名和密码才能登陆，先放一放，看看其他入口，之前有个ftp端口开放了，看看有什么有用的文件，

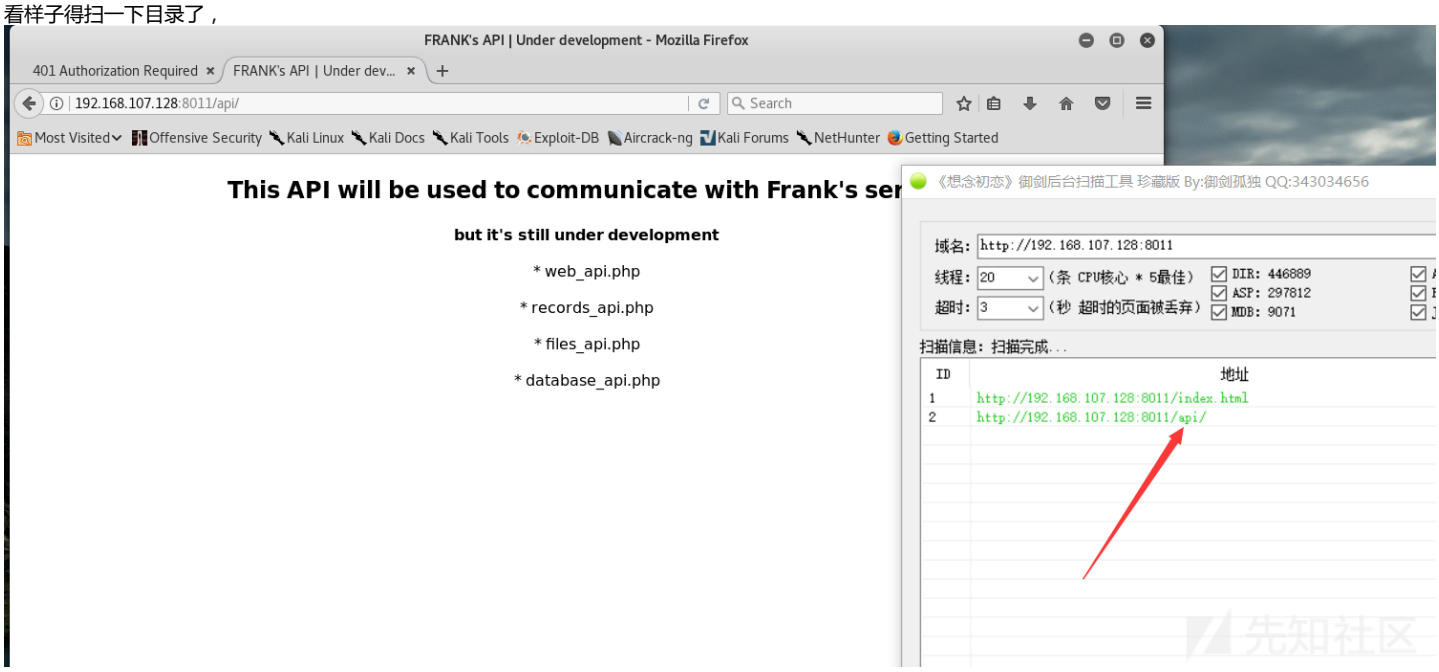


nothing，另外一个8011端口

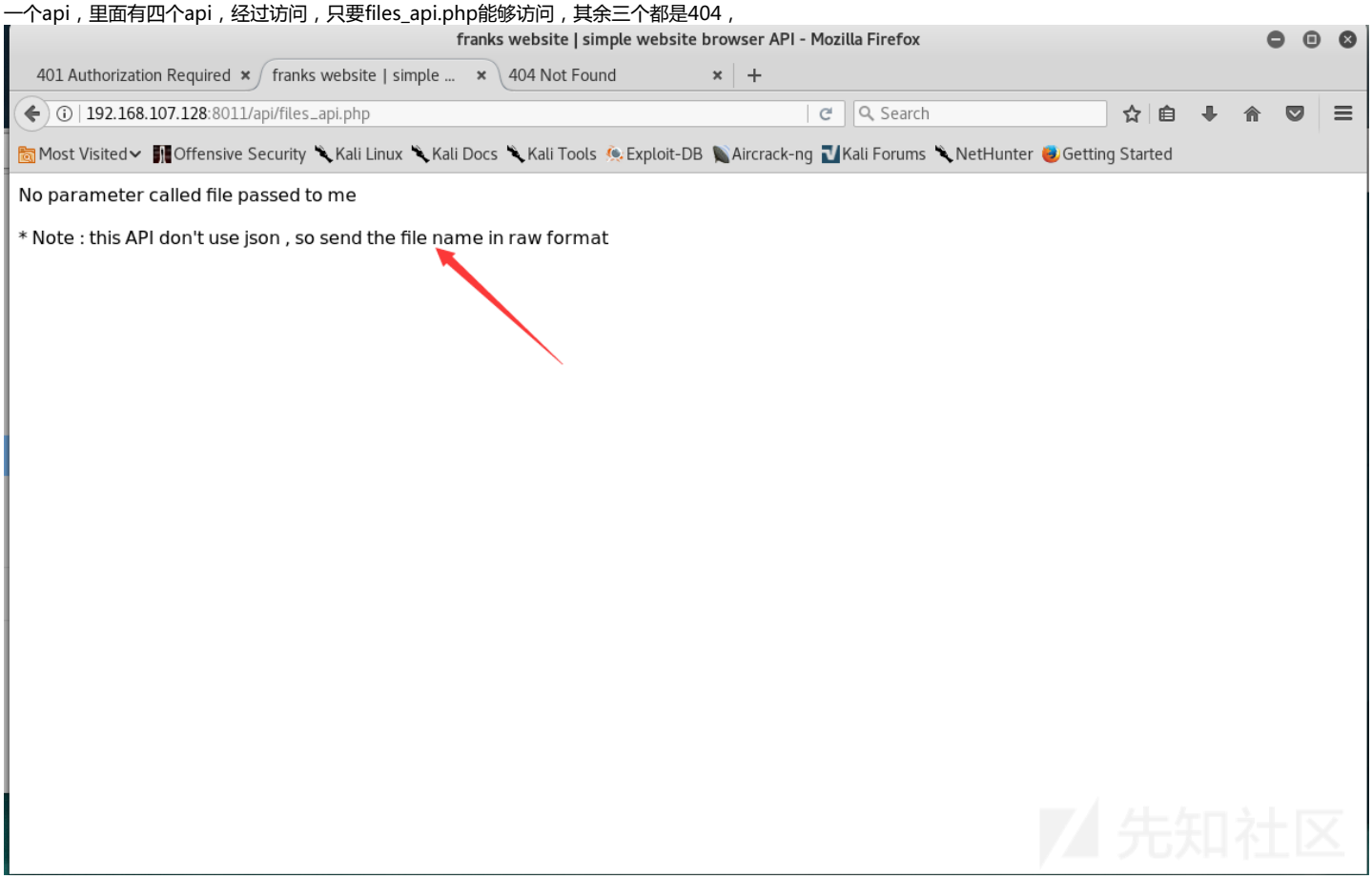


包含漏洞发现

看样子得扫一下目录了，



一个api，里面有四个api，经过访问，只要files_api.php能够访问，其余三个都是404，



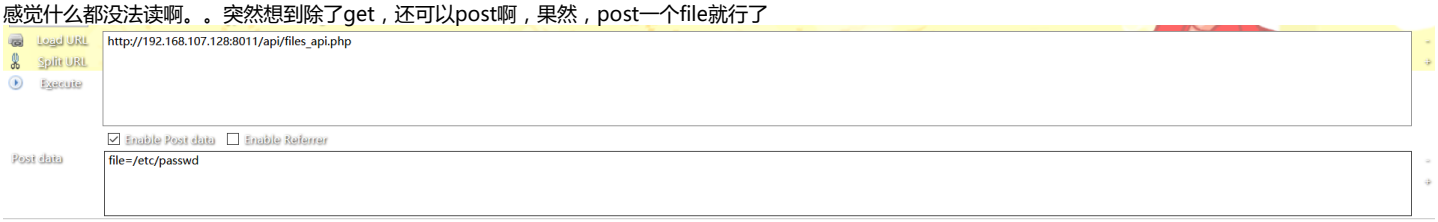
看样子是要让我们传入一个file参数，传入一个/etc/passwd结果发现是WRONG，难道说是过滤了什么？又试了其他的一些目录都是WRONG，

********* HACKER DETECTED *********

YOUR IP IS : 192.168.107.1

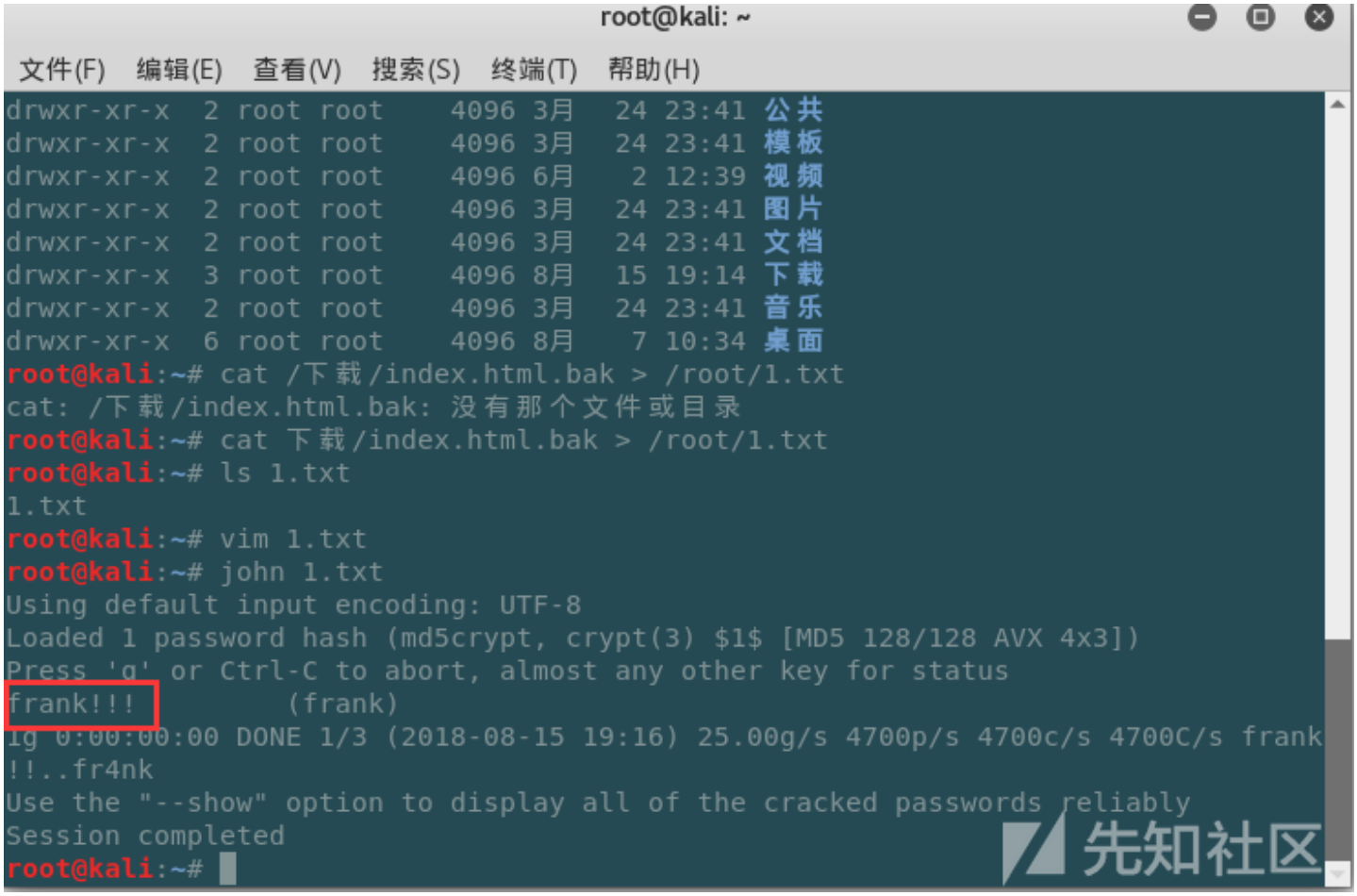
WRONG INPUT !!

感觉什么都没法读啊。。突然想到除了get，还可以post啊，果然，post一个file就行了



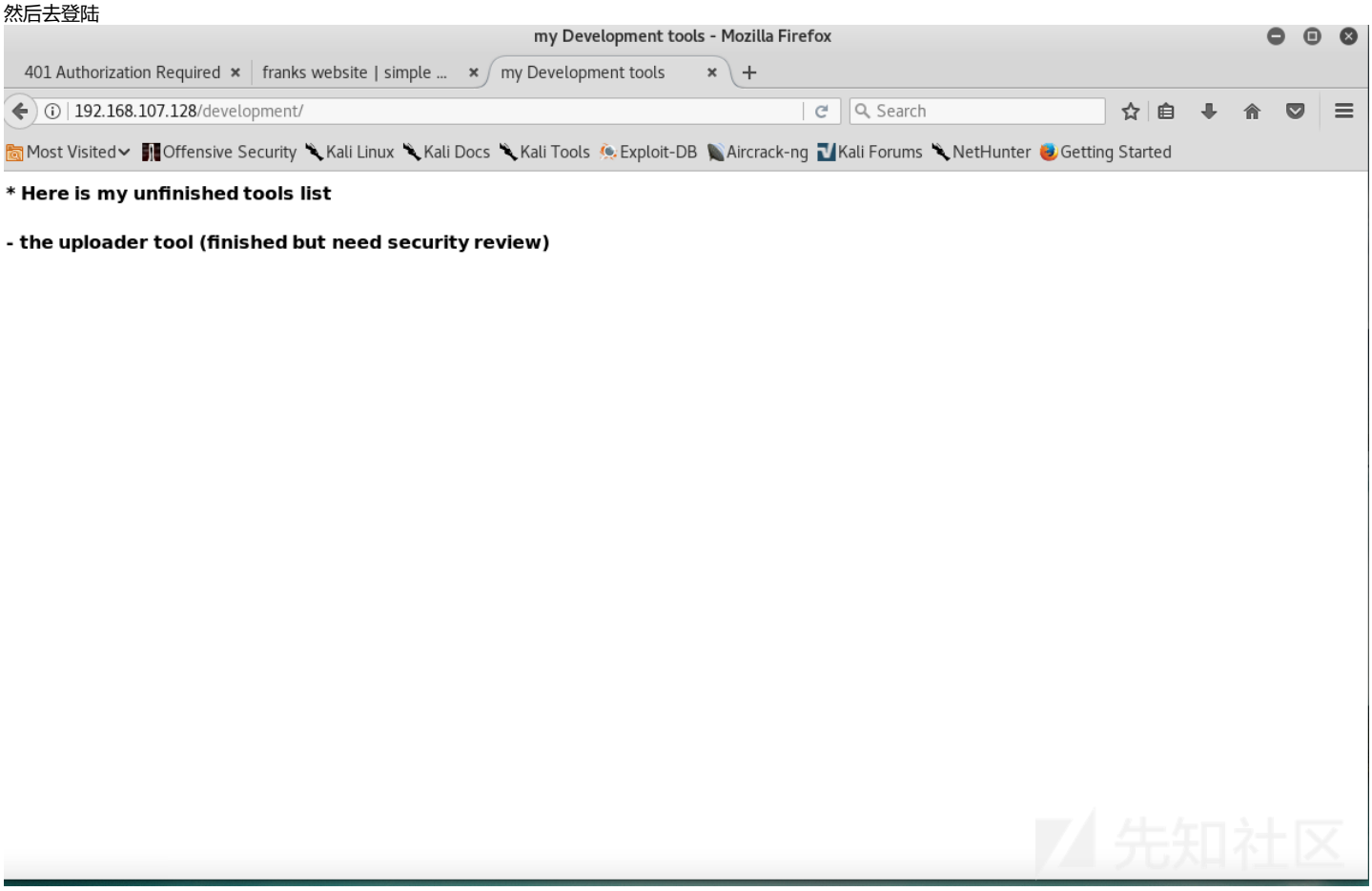
root:x:0:0:root:/root:/bin/bash bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:103::/home/syslog:/bin/false frank:x:1000:1000:frank,,,:/home/frank:/bin/bash sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin ftp:x:103:111:ftp daemon,,,:/srv/ftp:/bin/false

然后再来看我们之前的那串字符串，丢到kali下的john里解密，`john <filename>`。



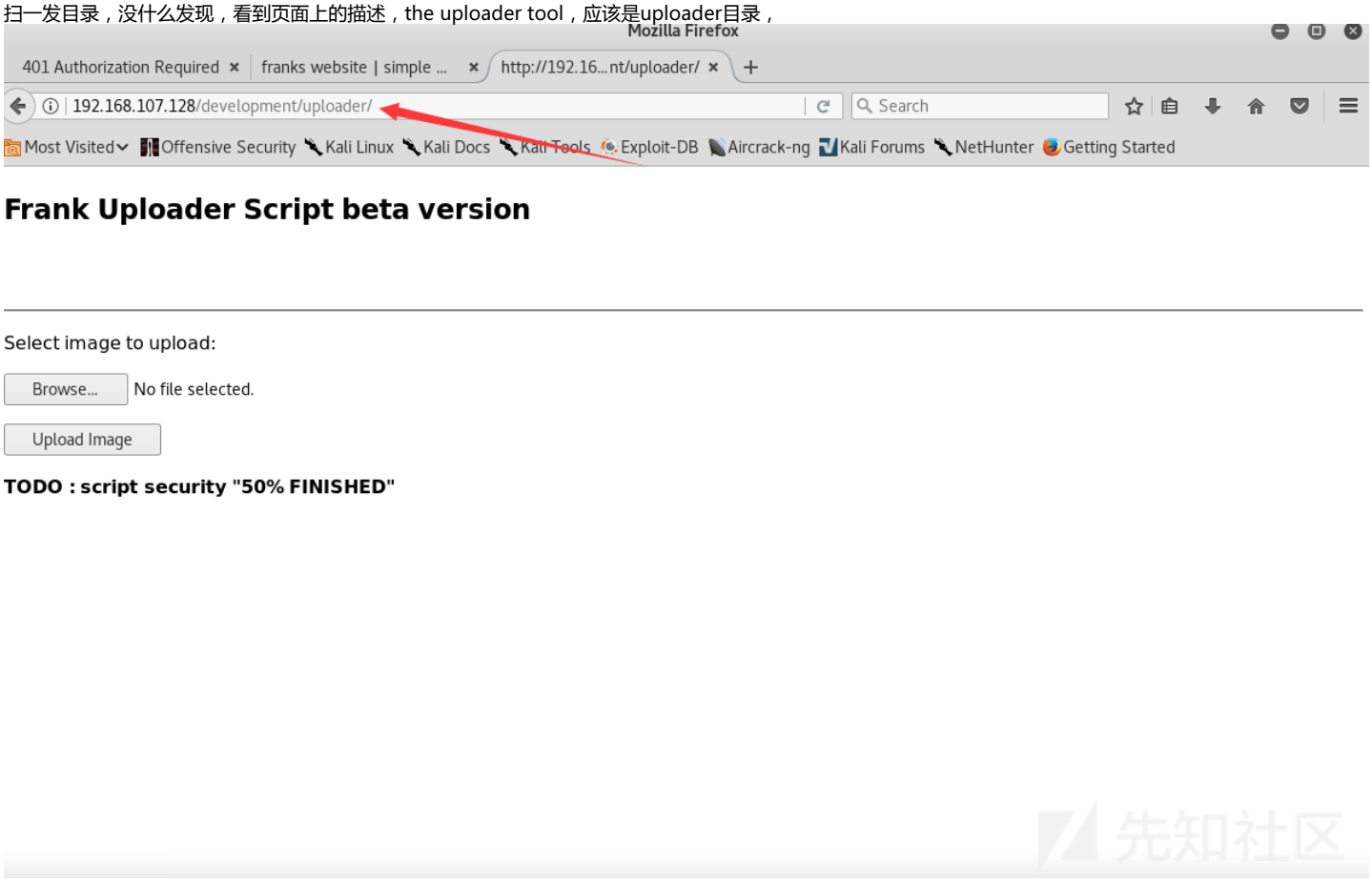
解密出来，密码是frank!!!。

然后去登陆

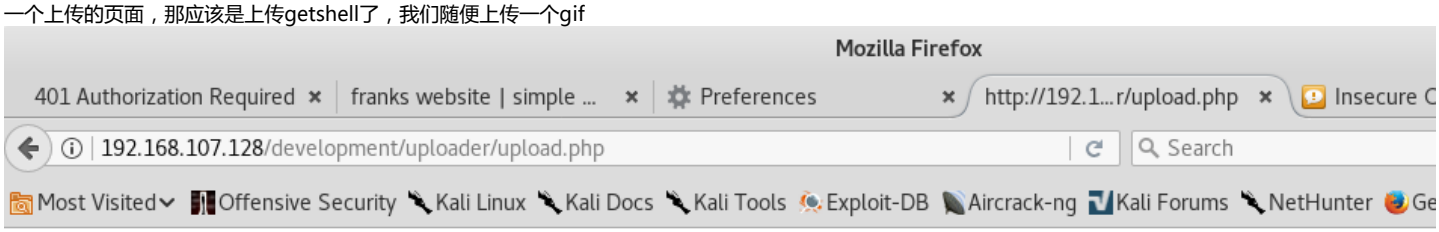


包含上传组合拳获取会话

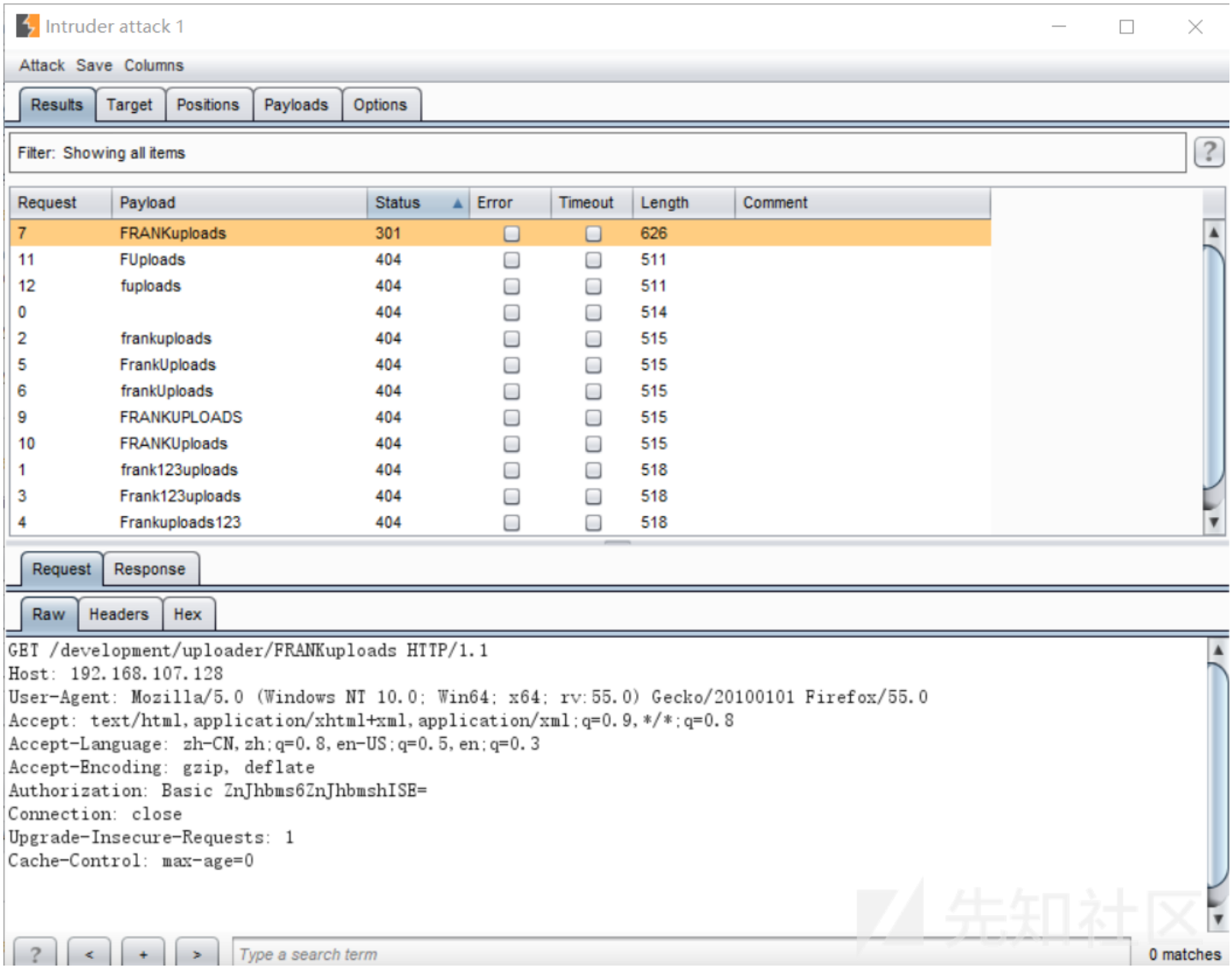
扫一发目录，没什么发现，看到页面上的描述，the uploader tool，应该是uploader目录，



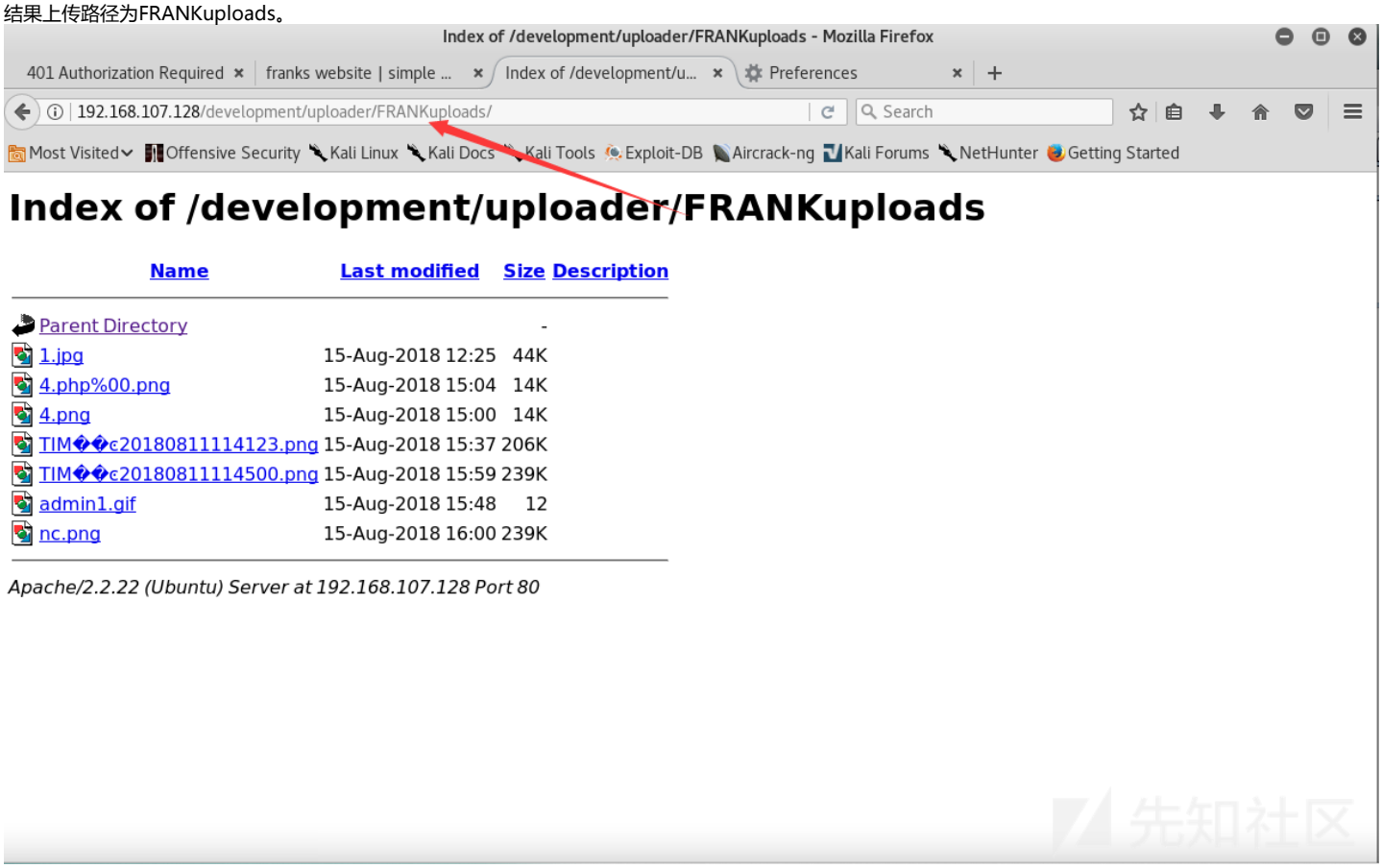
一个上传的页面，那应该是上传getshell了，我们随便上传一个gif



已经上传了，但是，我们找不到上传的路径，通过has been uploaded my uploads path，可以猜一猜上传路径，根据网站我写了个字典，Fuzz一下

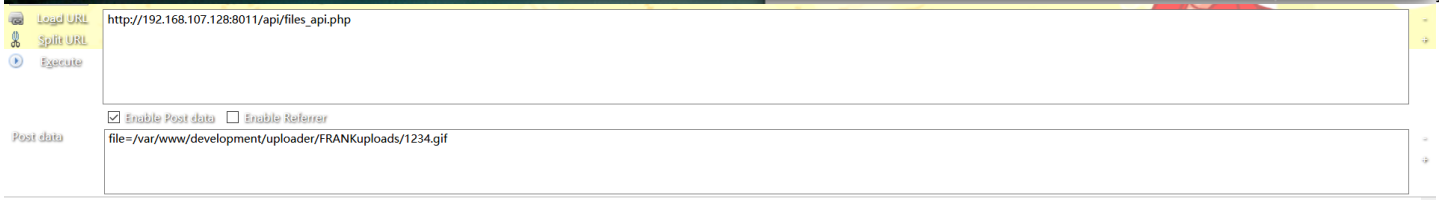


结果上传路径为FRANKuploads。



测试上传php，截断，等各种php都传不上去，这时候突然想到还有一个包含的漏洞，可以传一个gif文件里面插入一句话，然后再包含。我写了一个phpinfo().加个GIF98的

接着包含

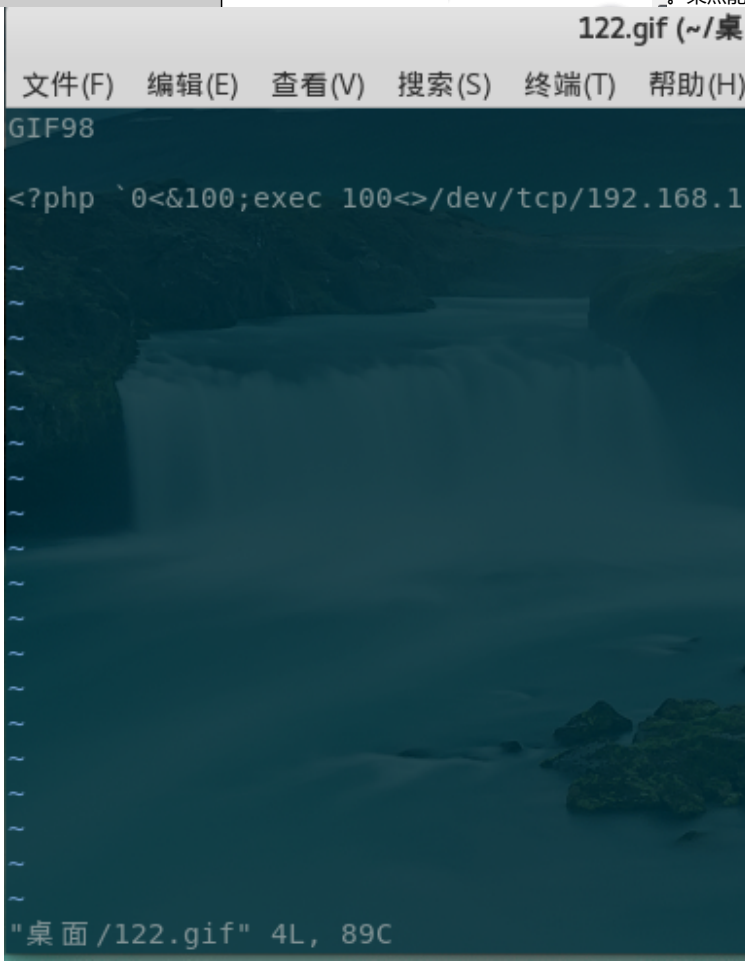


GIF98

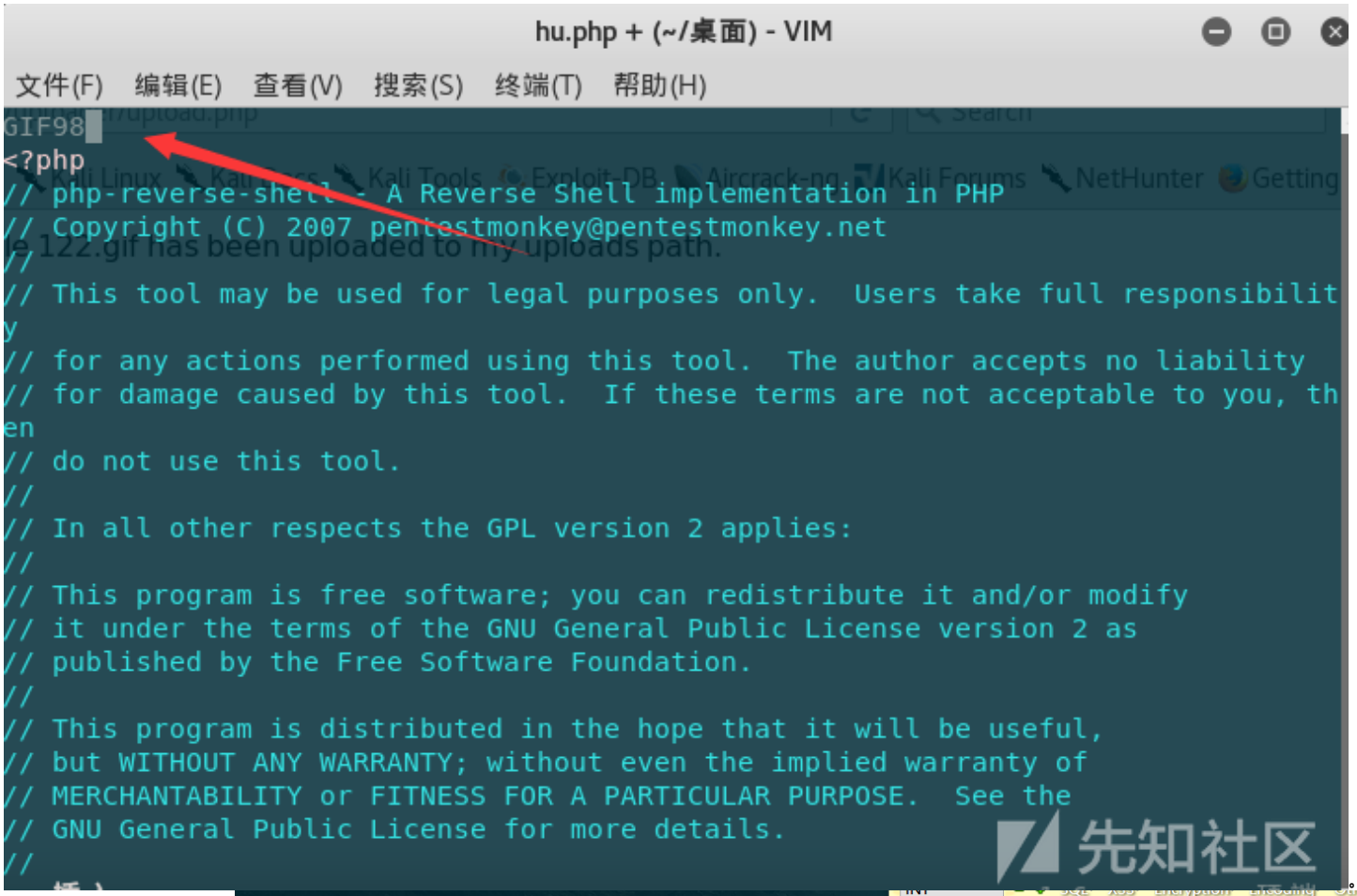
PHP Version 5.3.10-1ubuntu3.26

System	Linux ubuntu 2.6.35-19-generic #28-Ubuntu SMP Sun Aug 29 06:34:38 UTC 2010 x86_64
Build Date	Feb 13 2017 20:21:07
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/pdo.ini
PHP API	20090626
PHP Extension	20090626

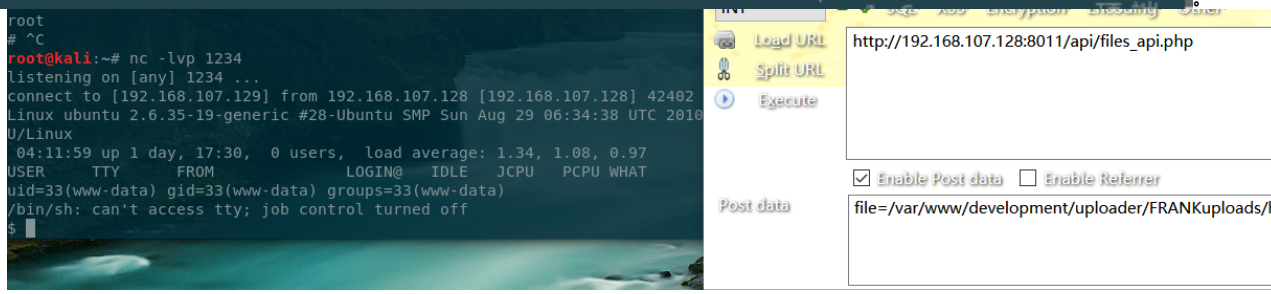
。果然能



4444。结果，没有任何反应，那应该是有什么过滤，接着我用msf生成了一个一句话，，依然弹不了shell，然后就在这，卡了一天。。查了资料，kali下有一个反弹shell的php文件，是/usr/share/webshells/php/php-reverse-shell.php，然后抱着试一试的心

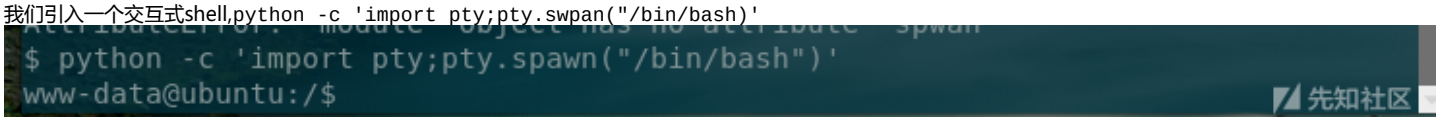


然后非常开心，居然成功了



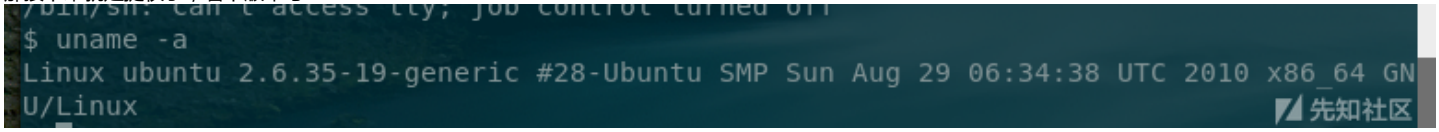
提升权限

我们引入一个交互式shell,`python -c 'import pty;pty.swpan("/bin/bash)'`



然后不能访问root，sudo需要密码

那接下来就是提权了，看下版本号



，谷歌一发，发现编号，把他放在kali web服务下

。然后靶机

这里注意

点击收藏 | 0 关注 | 2

上一篇：Sulley fuzzer lea... 下一篇：AdKoob数据窃贼将目标瞄准Fa...

1. 1 条回复

bin4xin 2019-05-06 22:04:42

您好！我想请问一下，我在弹SHELL的时候，POST页面显示"GIF98 WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111) "。请问该怎么办。。打扰！

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板