Ubuntu 18.04下搭建WooYun漏洞库

前言

自从wooyun关闭以后，网络安全人员缺少了一个学习平台，作为汇聚了大量前辈知识结晶的wooyun漏洞库、知识库对于搞安全行业的人员还是有很大的学习价值；目前互联网上也有很多人搭建了自己的wooyun平台，鉴于平台的稳定性以及后续使用的便利性，还是建议各位小伙伴自行搭建wooyun知识平台，本文主要以个人亲身经历为背景，基本ubuntu 18.04平台撰写了搭建手册，仅供有需要的小伙伴参考；

一、ubuntu系统下设置SSH密钥登陆步骤（可选项）

注：之所以使用密钥登陆，主要是为了提高安全性以及登陆的便捷性，可以根据实际情况选择紫荆喜欢的登陆方式；

1、首先登陆Ubuntu 18.04 生成密钥

- 我们先要生成一个密钥对，也就是公钥和私钥。生成密钥对需要**linux**操作系统。所以如果你在客户机上生成密钥对，你需要把公钥上传到服务器上。如果你在服务器上生成密钥对，你需要把私钥下载到客户机上。本人的客户机是**Windows10**，所以我选择在服务器上生成密钥对。
- 先通过ssh密码登陆服务器，然后：

```
ssh-keyge

Enter file in which to save the key (/root/.ssh/id_rsa):
//这句话的意思是你希望把生成的密钥对放在哪个位置，默认的是：/root/.ssh/id_rsa 默认就好，所以我们这里直接回车就好。

Enter passphrase (empty for no passphrase):
//这句话的意思是是否设置双重认证，就是为你的私钥添加一个密码，如果图方便，直接回车就好，如果为了更加安全，设置个简单密码就好。
//如果设置了双重认证，需要再一次确认密码
Your identification has been saved in /root/.ssh/id_rsa.

Your public key has been saved in /root/.ssh/id_rsa.pub.

The key fingerprint is:
aa:8b:61:13:38:ad:b5:49:ca:51:45:b9:77:e1:97:e1 root@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|     .o.         |
|     ..   . .    |
|   .  . . o o    |
| o.  . . o E     |
|o.=   . S .      |
|.*.+   .         |
|o.*   .          |
| . + .           |
|  . o.           |
+-----------------+
//完成
```

2、把密钥下载到客户机

id_rsa 是私钥 **id_rsa.pub**是公钥。我们只需要右键私钥，点击下载就好了。
这样，我们的客户机上就有钥匙了。后续就可以使用xshell使用密钥登陆设备了；

3、Ubuntu 18.04启用SSH密钥 禁用密码

```
:cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys //这一步是把生成的公钥导入到ssh的配置文件中

chmod 600 authorized_keys //以防万一，我们给予文件更高的权限
chmod 700 /root/.ssh

vim /etc/ssh/sshd_config //打开ssh配置文件

找到PubkeyAuthentication（在第37行）,默认的话，是被注释的，并且为no，我们把注释去掉，并且改为yes //开启密钥登陆

找到PasswordAuthentication（在第56行）,默认的话，是被注释的，并且为yes，我们把注释去掉，并且改为no //关闭密码登陆

service sshd restart //重启ssh服务
```

如图所示：

```
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
```


二、搭建LAMP环境

1、安装Apache

`apt install apache2 -y`

```
root@cqq-virtual-machine:/home/cqq# apt-get install apache2
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
将会同时安装下列软件:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
建议安装:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
下列【新】软件包将被安装:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
升级了 0 个软件包，新安装了 9 个软件包，要卸载 0 个软件包，有 432 个软件包未被升级。
需要下载 1,712 kB 的归档。
解压缩后会消耗 6,920 kB 的额外空间。
您希望继续执行吗？ [Y/n]
获取:1 http://cn.archive.ubuntu.com/ubuntu bionic/main amd64 libapr1 amd64 1.6.3-2 [
90.9 kB]
```

检查是否开启Apache，一般安装完会默认开启。

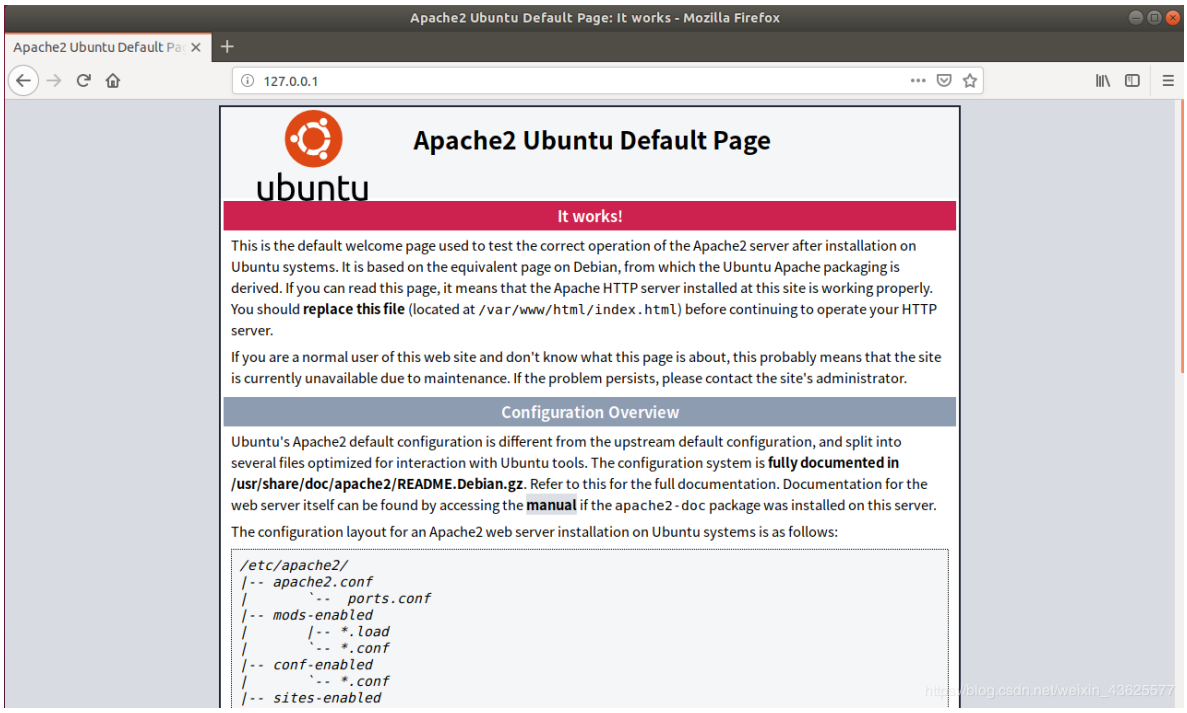
`systemctl status apache2`

```
root@cqq-virtual-machine:/home/cqq# systemctl status apache2
●apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enab
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Mon 2019-08-05 11:20:18 CST; 3min 21s ago
 Main PID: 13397 (apache2)
    Tasks: 55 (limit: 2290)
   CGroup: /system.slice/apache2.service
           ├─13397 /usr/sbin/apache2 -k start
           ├─13399 /usr/sbin/apache2 -k start
           └─13400 /usr/sbin/apache2 -k start

8月 05 11:20:18 cqq-virtual-machine systemd[1]: Starting The Apache HTTP Server...
8月 05 11:20:18 cqq-virtual-machine apachectl[13386]: AH00558: apache2: Could not re
8月 05 11:20:18 cqq-virtual-machine systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)
```


开启 、关闭和重启Apache服务器

```
systemctl start apache2      # 开启

systemctl stop apache2       # 关闭

systemctl restart apache2    # 重启
```

访问你的 Web 服务器，打开浏览器并输入Ubuntu18.04的IP地址，不出意外访问到Apache的默认信息页面。



2、数据库的安装，这里安装MySQL5.7

```
cqq@cqq-virtual-machine:~$ apt-get install mysql
E: 无法打开锁文件 /var/lib/dpkg/lock-frontend - open (13: 权限不够)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are y
ou root?
cqq@cqq-virtual-machine:~$ sudo passwd root
[sudo] cqq 的密码：
输入新的 UNIX 密码：
重新输入新的 UNIX 密码：
passwd：已成功更新密码
cqq@cqq-virtual-machine:~$ su root
密码：
root@cqq-virtual-machine:/home/cqq#
```


查看有没有安装MySQL：

`dpkg -l | grep mysql`

安装MySQL：

`apt install mysql-server -y`

```
root@cqq-virtual-machine:/home/cqq# dpkg -l | grep mysql
root@cqq-virtual-machine:/home/cqq# apt-get install mysql-server
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
将会同时安装下列软件：
  libaio1 libevent-core-2.1-6 libhtml-template-perl mysql-client-5.7 mysql-
client-core-5.7 mysql-common
  mysql-server-5.7 mysql-server-core-5.7
建议安装：
  libipc-sharedcache-perl mailx tinyca
下列【新】软件包将被安装：
  libaio1 libevent-core-2.1-6 libhtml-template-perl mysql-client-5.7 mysql-
client-core-5.7 mysql-common
  mysql-server mysql-server-5.7 mysql-server-core-5.7
升级了 0 个软件包，新安装了 9 个软件包，要卸载 0 个软件包，有 432 个软件包
未被升级。
需要下载 20.5 MB 的归档。
解压缩后会消耗 161 MB 的额外空间。
您希望继续执行吗？ [Y/n]
获取:1 http://cn.archive.ubuntu.com/ubuntu bionic/main amd64 mysql-common a
ll 5.8+1.0.4 [7,308 B]
```


安装完成之后可以使用如下命令来检查是否安装成功，如果看到有 mysql 的 socket 处于 LISTEN 状态则表示安装成功。

`netstat -tap | grep mysql`

```
root@cqq-virtual-machine:/home/cqq# netstat -pat | grep mysql
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN      15401/mysqld

root@cqq-virtual-machine:/home/cqq#
root@cqq-virtual-machine:/home/cqq# dpkg -l | grep mysql
ii  mysql-client-5.7                        5.7.27-0ubuntu0.18.04.1                 amd64
      MySQL database client binaries
ii  mysql-client-core-5.7                   5.7.27-0ubuntu0.18.04.1                 amd64
      MySQL database core client binaries
ii  mysql-common                            5.8+1.0.4                               all
      MySQL database common files, e.g. /etc/mysql/my.cnf
ii  mysql-server                            5.7.27-0ubuntu0.18.04.1                 all
      MySQL database server (metapackage depending on the latest version)
ii  mysql-server-5.7                        5.7.27-0ubuntu0.18.04.1                 amd64
      MySQL database server binaries and system database setup
ii  mysql-server-core-5.7                   5.7.27-0ubuntu0.18.04.1                 amd64
      MySQL database server binaries
root@cqq-virtual-machine:/home/cqq#
```


登录mysql数据库可以通过如下命令：

`mysql -u root -p`

> -u 表示选择登陆的用户名， -p 表示登陆的用户密码，全新安装的mysql数据库是没有密码的，Enter password: 处直接回车，就能够进入mysql数据库。然后通过 show databases; 就可以查看当前的所有数据库。

```
root@cqq-virtual-machine:/home/cqq# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.27-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.00 sec)
```


3、PHP的安装

PHP添加了支持动态网页的服务器端网页处理。

`apt install php -y`

```
root@cqq-virtual-machine:/home/cqq# apt install php
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
将会同时安装下列软件:
  libapache2-mod-php7.2 php-common php7.2 php7.2-cli php7.2-common php7.2-js
on php7.2-opcache php7.2-readline
建议安装:
  php-pear
下列【新】软件包将被安装:
  libapache2-mod-php7.2 php php-common php7.2 php7.2-cli php7.2-common php7.
2-json php7.2-opcache php7.2-readline
升级了 0 个软件包，新安装了 9 个软件包，要卸载 0 个软件包，有 432 个软件包未
被升级。
需要下载 3,863 kB 的归档。
解压缩后会消耗 17.2 MB 的额外空间。
您希望继续执行吗？ [Y/n]
获取:1 http://cn.archive.ubuntu.com/ubuntu bionic/main amd64 php-common all
1:60ubuntu1 [12.1 kB]
获取:2 http://cn.archive.ubuntu.com/ubuntu bionic-updates/main amd64 php7.2-
common amd64 7.2.19-0ubuntu0.18.04.1 [885 kB]
```


安装完成后，使用如下命令查看PHP的版本：php -v

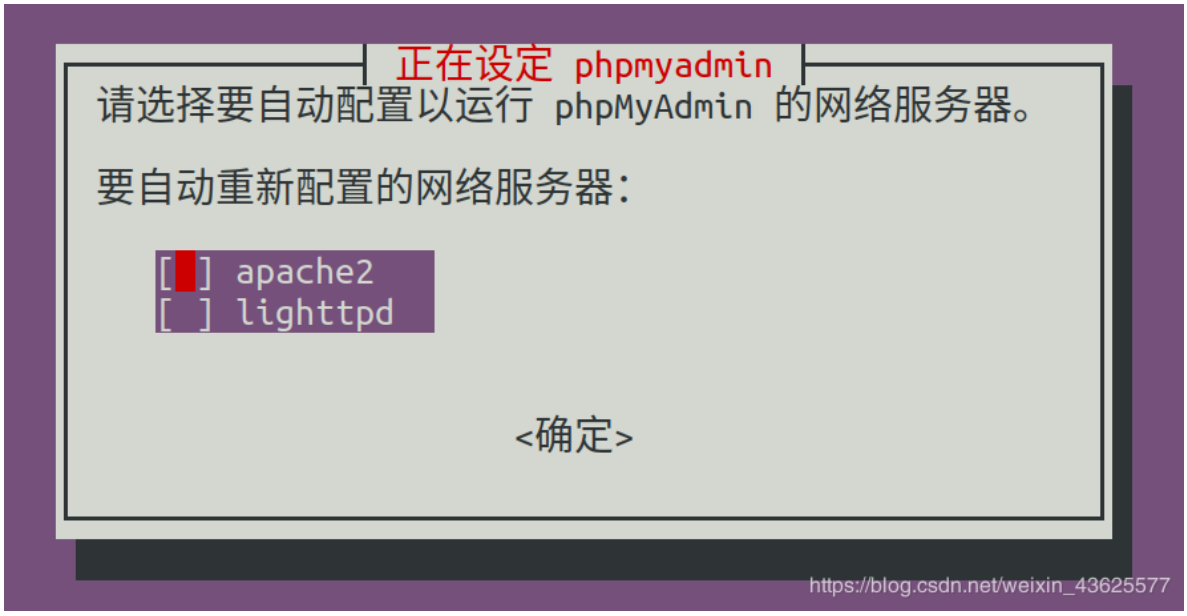
```
root@cqq-virtual-machine:/home/cqq# php -v
PHP 7.2.19-0ubuntu0.18.04.1 (cli) (built: Jun  4 2019 14:48:12) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
    with Zend OPcache v7.2.19-0ubuntu0.18.04.1, Copyright (c) 1999-2018, by
Zend Technologies
root@cqq-virtual-machine:/home/cqq#
```


4、phpMyAdmin 的安装（可选，主要是为了方便操作数据库，如比较倾向于命令行操作，可以不安装）

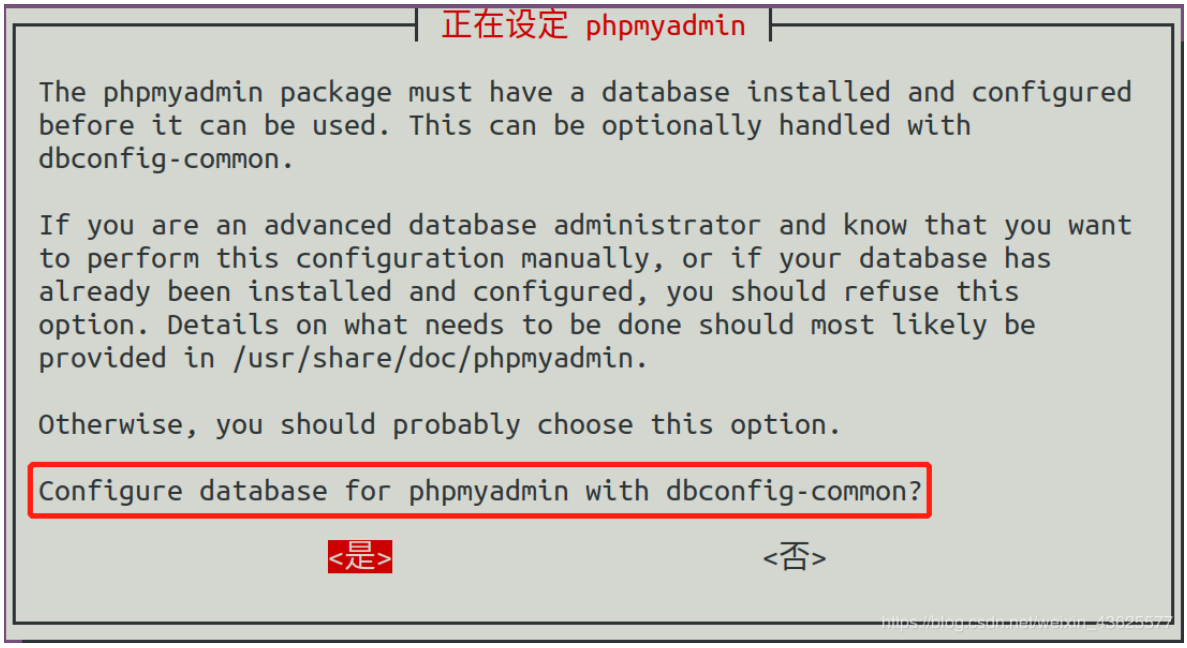
`apt install phpmyadmin -y`

```
root@cqq-virtual-machine:/home/cqq# apt install phpmyadmin
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
将会同时安装下列软件:
  dbconfig-common dbconfig-mysql javascript-common libcurl4 libjs-jquery
  libjs-sphinxdoc libjs-underscore libzip4 php-bz2 php-curl php-gd
  php-mbstring php-mysql php-pear php-php-gettext php-phpseclib php-tcpdf
  php-xml php-zip php7.2-bz2 php7.2-curl php7.2-gd php7.2-mbstring
  php7.2-mysql php7.2-xml php7.2-zip
建议安装:
  php-libsodium php-mcrypt php-gmp php-imagick
下列【新】软件包将被安装:
  dbconfig-common dbconfig-mysql javascript-common libcurl4 libjs-jquery
  libjs-sphinxdoc libjs-underscore libzip4 php-bz2 php-curl php-gd
  php-mbstring php-mysql php-pear php-php-gettext php-phpseclib php-tcpdf
  php-xml php-zip php7.2-bz2 php7.2-curl php7.2-gd php7.2-mbstring
  php7.2-mysql php7.2-xml php7.2-zip phpmyadmin
升级了 0 个软件包，新安装了 27 个软件包，要卸载 0 个软件包，有 432 个软件包未被升级。
需要下载 14.1 MB 的归档。
解压缩后会消耗 55.1 MB 的额外空间。
您希望继续执行吗？ [Y/n]
获取:1 http://cn.archive.ubuntu.com/ubuntu bionic/main amd64 dbconfig-common all 2.0.9
```

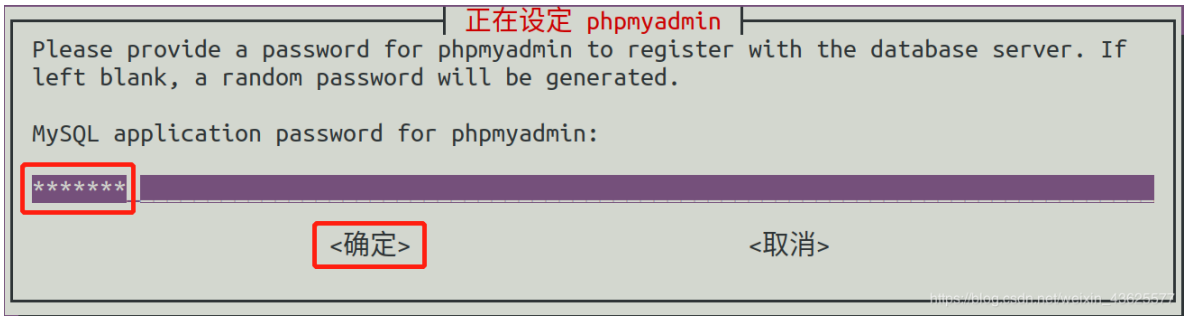
选择 Apache2 并点击确定。（以下的选择用TAB键）



点击确定来配置 phpMyAdmin 管理的数据库。



指定 phpMyAdmin 向数据库服务器注册时所用的密码。（由于mysql初始化安装以后是没有设置密码的，这里可以不写或者写准备作为作为mysql的密码）



再次确认密码。

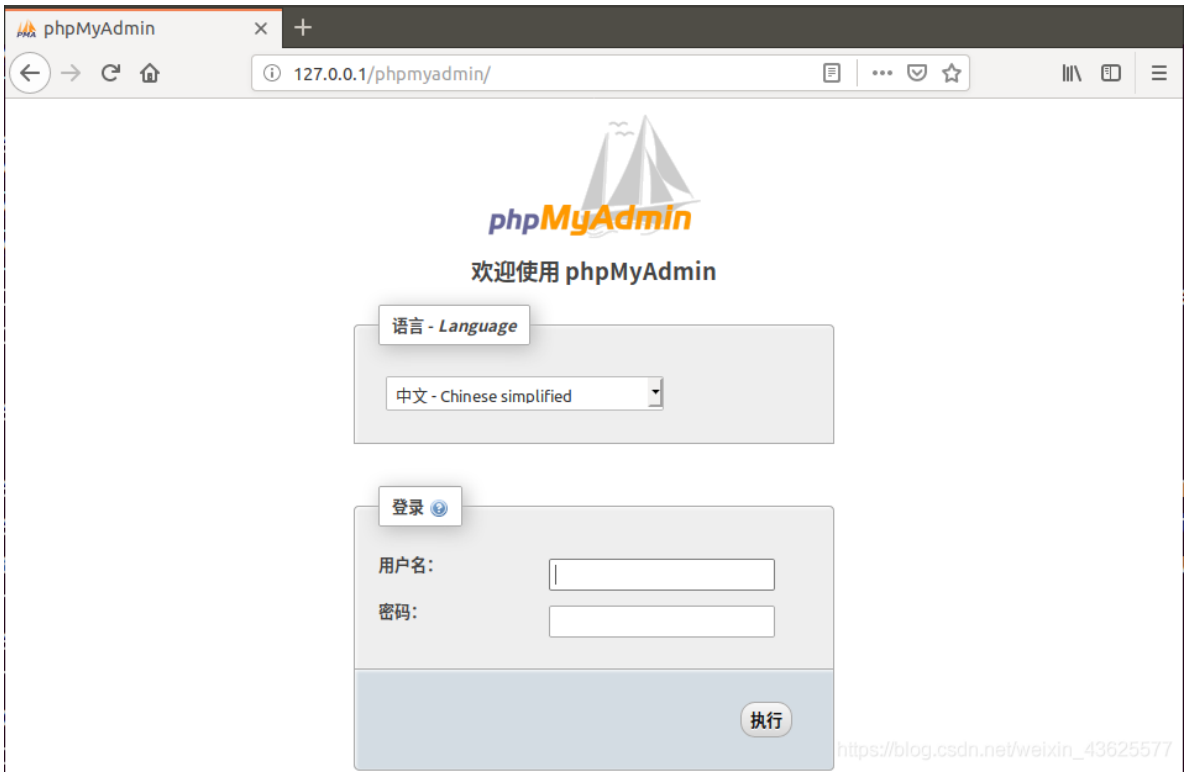
出现如下图所示，就表示phpMyAdmin安装完毕了。

```
Determining localhost credentials from /etc/mysql/debian.cnf: succeeded.
dbconfig-common: writing config to /etc/dbconfig-common/phpmyadmin.conf

Creating config file /etc/dbconfig-common/phpmyadmin.conf with new version

Creating config file /etc/phpmyadmin/config-db.php with new version
checking privileges on database phpmyadmin for phpmyadmin@localhost: user creation needed.
granting access to database phpmyadmin for phpmyadmin@localhost: success.
verifying access for phpmyadmin@localhost: success.
creating database phpmyadmin: success.
verifying database phpmyadmin exists: success.
populating database via sql...  done.
dbconfig-common: flushing administrative password
正在处理用于 libapache2-mod-php7.2 (7.2.19-0ubuntu0.18.04.1) 的触发器 ...
root@cqq-virtual-machine:/home/cqq#
root@cqq-virtual-machine:/home/cqq#
root@cqq-virtual-machine:/home/cqq# ln -s /usr/share/phpmyadmin /var/www/html/phpmyadmin
root@cqq-virtual-machine:/home/cqq#
```


安装完成后，创建phpMyAdmin的软链接到Apache的根目录下（我的是/var/www/html/）

```
ln -s /usr/share/phpmyadmin /var/www/html/phpmyadmin
```

现在开始尝试访问phpMyAdmin，打开浏览器并输入：IP地址/phpmyadmin



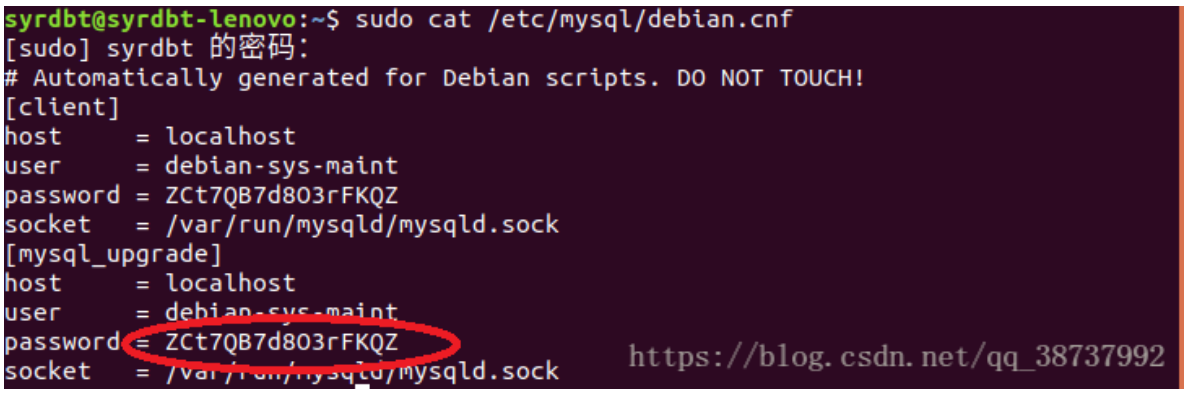
phpMyAdmin 是一个以PHP为基础，以Web-Base方式架构在网站主机上的MySQL的数据库管理工具，让管理者可用Web接口管理MySQL数据库。借由此Web接口可以成为一个简易方式输入繁杂SQL语法的较佳途径，尤其要处理大量资料的汇入及汇出更为方便。其中一个更大的优势在于由于phpMyAdmin跟其他PHP程式一样在网页服务器上执行，但是您可以在任何地方使用这些程式产生的HTML页面，也就是于远端管理MySQL数据库，方便的建立、修改、删除数据库及资料表。也可借由phpMyAdmin建立常用的php语法，方便编写网页时所需要的SQL语法正确性。

5、针对首次登录mysql未设置密码或忘记密码解决方法

1：首先输入以下指令：

```
sudo cat /etc/mysql/debian.cnf
```

运行截图如下：

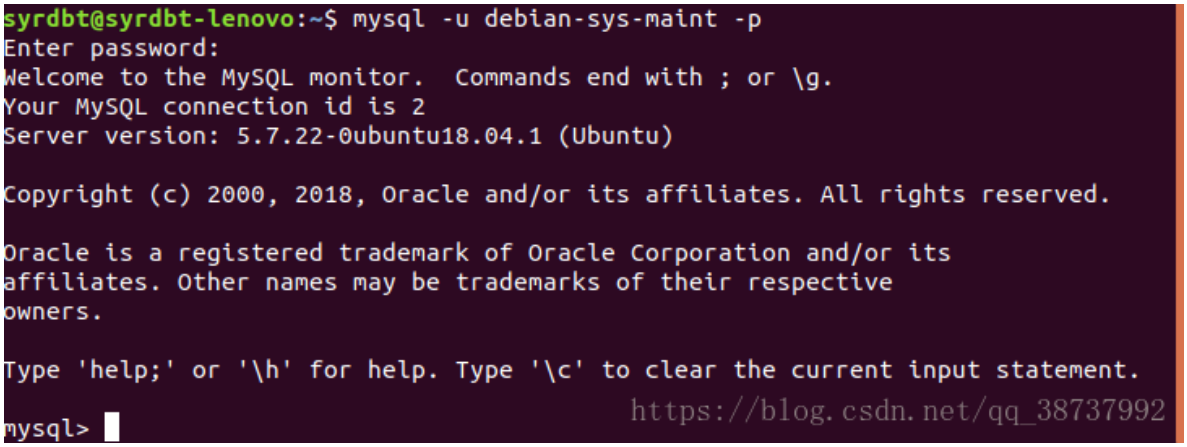


2： 再输入以下指令：

```
mysql -u debian-sys-maint -p

//注意!
//这条指令的密码输入是输入第一条指令获得的信息中的 password = ZCt7QB7d8O3rFKQZ 得来。
//请根据自己的实际情况填写!
```

运行截图如下：**(注意! 这步的密码输入的是 ZCt7QB7d8O3rFKQZ，密码是由第一条指令获得的信息中的**

password = ZCt7QB7d8O3rFKQZ 得来，每个人不一样，请根据自己的实际情况输入，输入就可以得到以下运行情况)



3. 修改密码，本篇文章将密码修改成 root , 用户可自行定义。

```
use mysql;

update mysql.user set authentication_string=password('root') where user='root'
and Host ='localhost';

update user set plugin="mysql_native_password";

flush privileges;
quit;
```

```
mysql> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> update mysql.user set authentication_string=password('root') where user='
root' and Host ='localhost';
Query OK, 0 rows affected, 1 warning (0.00 sec)
Rows matched: 1  Changed: 0  Warnings: 1

mysql> update user set plugin="mysql_native_password";
Query OK, 0 rows affected (0.00 sec)
Rows matched: 4  Changed: 0  Warnings: 0

mysql> flush privileges;
Query OK, 0 rows affected (0.01 sec)

mysql> quit;
Bye
```


4： 重新启动mysql:

```
sudo service mysql restart

mysql -u root -p // 启动后输入已经修改好的密码：root
```

```
syrdbt@syrdbt-lenovo:~$ sudo service mysql restart
```

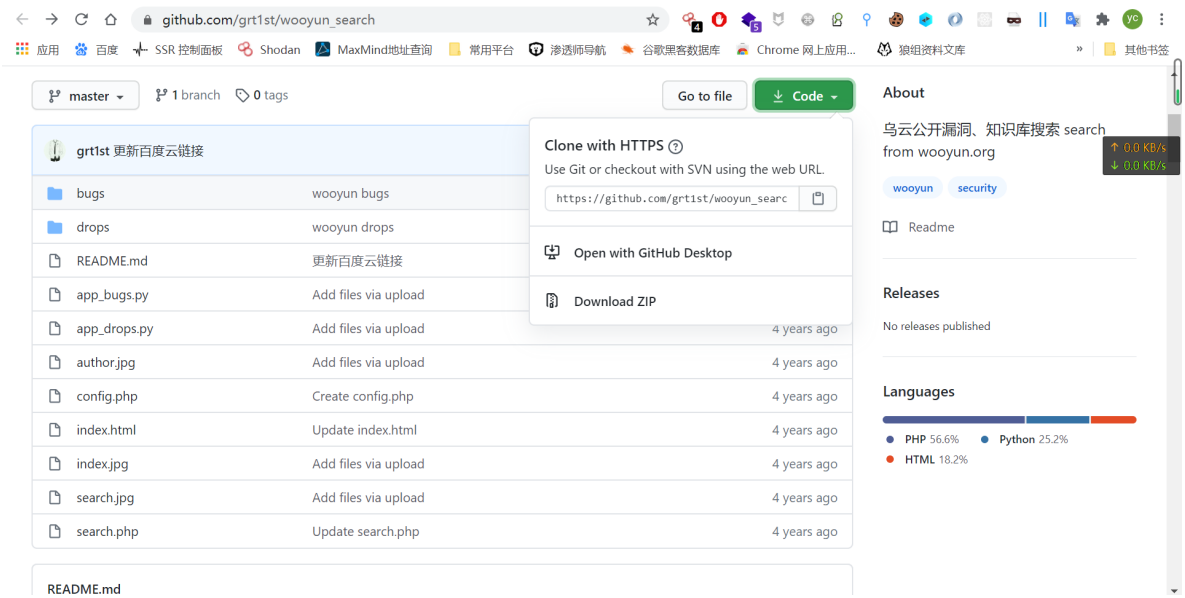
```
syrdbt@syrdbt-lenovo:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.22-0ubuntu18.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```


5：至此，mysql初始化完成；

三、搭建WooYun漏洞库

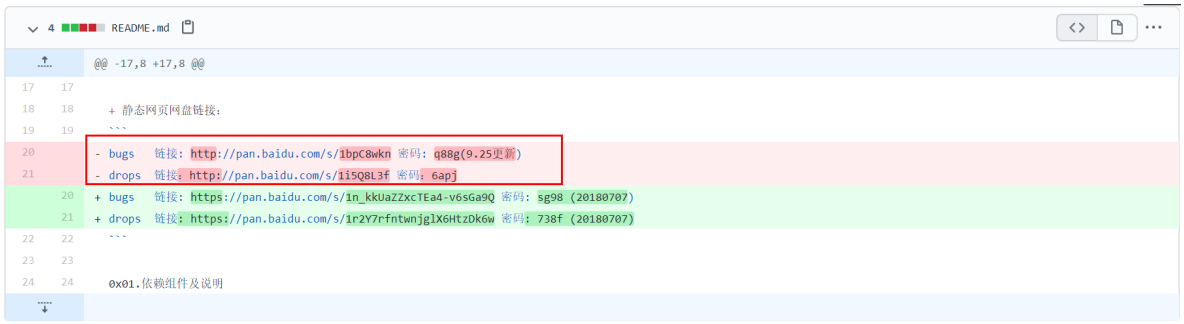
1、下载资源

访问https://github.com/grt1st/wooyun_search，下载所需文件。



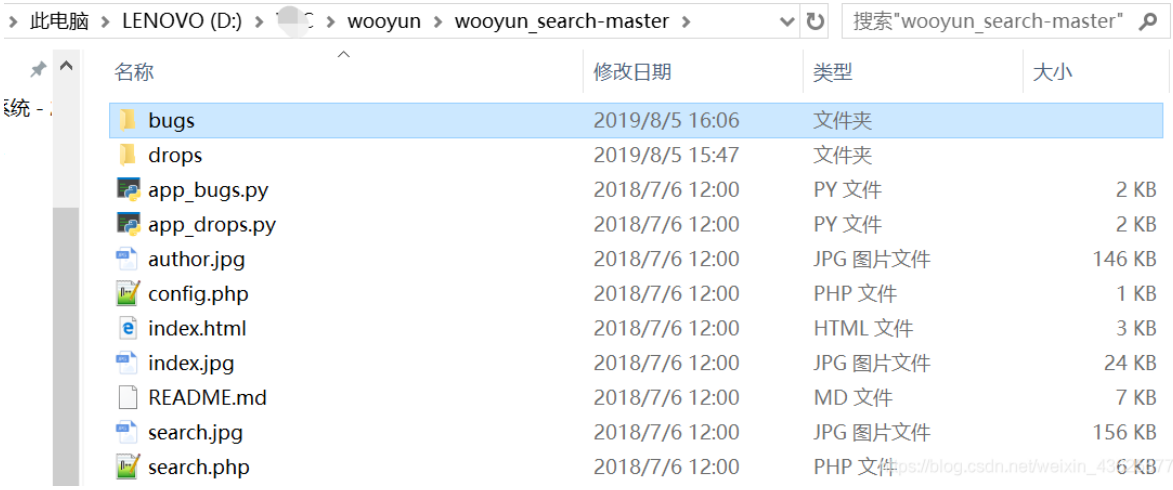
使用git克隆代码(文件名为：wooyun_search-master)，其中文件bugs和drops内容为空，需另外下载，下载链接如下所示：

bugs 链接: http://pan.baidu.com/s/1bpC8wkn 密码: q88g(9.25更新)		
drops 链接：http://pan.baidu.com/s/1i5Q8L3f 密码：6apj		



下载好WooYun_Bugs(漏洞库)、WooYun_Drops(知识库)之后，需对里面的压缩文件进行解压。

注意：只需分别对文件WooYun_Bugs(漏洞库)、WooYun_Drops(知识库)中的一个压缩文件进行彻底解压即可。解压成功后，分别将这两个文件中的内容放到对应的bugs、drops文件中。



接下来就是将文件wooyun_search-master放进先前搭建好的web服务器目录下(/var/www/html)，并将文件wooyun_search-master重命名为wooyun，方便后面进行搜索。

```
root@VM-0-4-ubuntu:/var/www/html/wooyun# ls -al
total 380
drwxr-xr-x 5 root root   4096 Aug  6 16:15 .
drwxr-xr-x 3 root root   4096 Aug  6 16:09 ..
-rw-r--r-- 1 root root   1545 Aug  6 16:14 app_bugs.py
-rw-r--r-- 1 root root   1357 Aug  6 16:15 app_drops.py
-rw-r--r-- 1 root root 149210 Aug  6 16:09 author.jpg
drwxr-xr-x 2 root root   4096 Aug  6 16:09 bugs
-rw-r--r-- 1 root root    573 Aug  6 16:09 config.php
drwxr-xr-x 2 root root   4096 Aug  6 16:09 drops
drwxr-xr-x 8 root root   4096 Aug  6 16:09 .git
-rw-r--r-- 1 root root   2076 Aug  6 16:09 index.html
-rw-r--r-- 1 root root  24480 Aug  6 16:09 index.jpg
-rw-r--r-- 1 root root   6805 Aug  6 16:09 README.md
-rw-r--r-- 1 root root 159495 Aug  6 16:09 search.jpg
-rw-r--r-- 1 root root   5904 Aug  6 16:09 search.php
root@VM-0-4-ubuntu:/var/www/html/wooyun#
```

文件说明：

app_bugs.py	bugs的索引，依赖lxml
app_drops.py	drops的索引，依赖lxml
index.html	搜索的主页
search.php	执行搜索的页面
config.php	php配置文件
./bugs	bugs静态文件的目录
./drops	drops静态文件的目录

> app_bugs.py为建立bugs索引的脚本，app_drops.py为建立drops索引的脚本。
>
> 因为python脚本中open()函数打开的文件名不能为中文，建议将drops目录下的中文文件名改为英文(例如，安全运维-xxxx.html=>safe-xxxx.html)

2、安装依赖组件

> - python 2.7和pip
> - python依赖：MySQLdb，lxml(推荐)

提示：以下操作均在root权限下进行（每个人搭建过程中遇到的问题会不一样，本文不保证能解决所有问题，个别问题需自己去手动查搜索。）

2.1 安装Python

```
apt install python
```

2.2 安装pip

```
root@cqq-virtual-machine:/home/cqq# apt install python-pip
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
将会同时安装下列软件:
  build-essential cpp cpp-7 dpkg-dev fakeroot g++ g++-7 gcc gcc-7 gcc-7-base
  gcc-8-base libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libasan4 libatomic1 libc-dev-bin libc6-dev libcc1-0
  libcilkrts5 libexpat1 libexpat1-dev libfakeroot libgcc-7-dev libgcc1 libgomp1
  libitm1 liblsan0 libmpx2 libpython-all-dev libpython-dev libpython2.7-dev
  libquadmath0 libssl1.1 libstdc++-7-dev libstdc++6 libtsan0 libubsan0
  linux-libc-dev make manpages-dev python-all python-all-dev python-asn1crypto
  python-cffi-backend python-crypto python-cryptography python-dbus python-dev
  python-enum34 python-gi python-idna python-ipaddress python-keyring
  python-keyrings.alt python-pip-whl python-pkg-resources python-secretstorage
  python-setuptools python-six python-wheel python-xdg python2.7-dev
建议安装:
  cpp-doc gcc-7-locales debian-keyring g++-multilib g++-7-multilib gcc-7-doc
  libstdc++6-7-dbg gcc-multilib autoconf automake libtool flex bison gcc-doc
```


安装时若出现询问框，按默认的安装就行。安装完成后，可输入如下命令进行版本查询。

```
root@cqq-virtual-machine:/home/cqq# pip --version
pip 9.0.1 from /usr/lib/python2.7/dist-packages (python 2.7)
root@cqq-virtual-machine:/home/cqq#
root@cqq-virtual-machine:/home/cqq# python --version
Python 2.7.15+
root@cqq-virtual-machine:/home/cqq#
```

2.3 安装MySQLdb

> MySQLdb — Python 连接 MySQL 的模块。

pip install mysql-python

```
root@cqq-virtual-machine:/home/cqq# pip install mysql-python
Collecting mysql-python
  Downloading https://files.pythonhosted.org/packages/a5/e9/51b544da85a36a68debe7a7
091f068d802fc515a3a202652828c73453cad/MySQL-python-1.2.5.zip (108kB)
    100% |                                | 112kB 186kB/s
    Complete output from command python setup.py egg_info:
    sh: 1: mysql_config: not found
    Traceback (most recent call last):
      File "<string>", line 1, in <module>
      File "/tmp/pip-build-VNHVIW/mysql-python/setup.py", line 17, in <module>
        metadata, options = get_config()
      File "setup_posix.py", line 43, in get_config
        libs = mysql_config("libs_r")
      File "setup_posix.py", line 25, in mysql_config
        raise EnvironmentError("%s not found" % (mysql_config.path,))
    EnvironmentError: mysql_config not found

    ----------------------------------------
Command "python setup.py egg_info" failed with error code 1 in /tmp/pip-build-VNHVI
W/mysql-python/                                    https://blog.csdn.net/weixin_43625577
```

使用pip安装，若出现以上异常 — EnvironmentError: mysql_config not found，需安装另一个依赖 apt-get install libmysqld-dev

```
root@cqq-virtual-machine:/home/cqq# apt-get install libmysqld-dev
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
将会同时安装下列软件:
  libaio-dev libmysqlclient-dev libmysqlclient20 libnuma-dev libnuma1 zlib1g-dev
下列【新】软件包将被安装:
  libaio-dev libmysqlclient-dev libmysqlclient20 libmysqld-dev libnuma-dev
  zlib1g-dev
下列软件包将被升级:
  libnuma1
升级了 1 个软件包，新安装了 6 个软件包，要卸载 0 个软件包，有 418 个软件包未被升级
。
需要下载 8,736 kB 的归档。
解压缩后会消耗 60.7 MB 的额外空间。
您希望继续执行吗？ [Y/n]
获取:1 http://cn.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libnuma1 amd64
 2.0.11-2.1ubuntu0.1 [22.0 kB]                    https://blog.csdn.net/weixin_43625577
```

再次安装pip install mysql-python，安装成功之后，进入到python环境确认— import MySQLdb

```
root@cqq-virtual-machine:/home/cqq# pip install mysql-python
Collecting mysql-python
  Using cached https://files.pythonhosted.org/packages/a5/e9/51b544da85a36a68debe7a
7091f068d802fc515a3a202652828c73453cad/MySQL-python-1.2.5.zip
Building wheels for collected packages: mysql-python
  Running setup.py bdist_wheel for mysql-python ... done
  Stored in directory: /root/.cache/pip/wheels/07/d2/5f/314860e4cb53a44bf0ee0d051d4
b34465e4b4fbe9de6d42f42
Successfully built mysql-python
Installing collected packages: mysql-python
Successfully installed mysql-python-1.2.5
root@cqq-virtual-machine:/home/cqq#                https://blog.csdn.net/weixin_43625577
```

```
root@cqq-virtual-machine:/home/cqq# python
Python 2.7.15+ (default, Nov 27 2018, 23:36:35)
[GCC 7.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import MySQLdb
>>>
```

2.4 安装lxml

> lxml是python的一个解析库，支持HTML和XML的解析，支持XPath解析方式，而且解析效率非常高。

安装依赖 — apt-get install libxml2-dev libxslt-dev

```
root@cqq-virtual-machine:/home/cqq# apt-get install libxml2-dev libxslt-dev
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
注意，选中 'libxslt1-dev' 而非 'libxslt-dev'
下列软件包是自动安装的并且现在不需要了：
  python-bs4 python-chardet python-html5lib python-webencodings
使用'apt autoremove'来卸载它(它们)。
将会同时安装下列软件：
  gir1.2-harfbuzz-0.0 icu-devtools libglib2.0-0 libglib2.0-bin libglib2.0-dev
  libglib2.0-dev-bin libgraphite2-dev libharfbuzz-dev libharfbuzz-gobject0
  libicu-dev libicu-le-hb-dev libicu-le-hb0 libiculx60 libpcre16-3
  libpcre3-dev libpcre32-3 libpcrecpp0v5 libxslt1.1 pkg-config
  python3-distutils python3-lib2to3
建议安装：
  libglib2.0-doc libgraphite2-utils icu-doc
下列【新】软件包将被安装：
  gir1.2-harfbuzz-0.0 icu-devtools libglib2.0-dev libglib2.0-dev-bin
  libgraphite2-dev libharfbuzz-dev libharfbuzz-gobject0 libicu-dev
```


安装lxml —— apt-get install python-lxml 或 pip install lxml

```
root@cqq-virtual-machine:/home/cqq# apt-get install python-lxml
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
建议安装：
  python-lxml-dbg python-lxml-doc
下列【新】软件包将被安装：
  python-lxml
升级了 0 个软件包，新安装了 1 个软件包，要卸载 0 个软件包，有 415 个软件包未被升级。
需要下载 0 B/1,075 kB 的归档。
解压缩后会消耗 4,135 kB 的额外空间。
正在选中未选择的软件包 python-lxml:amd64。
(正在读取数据库 ... 系统当前共安装有 138328 个文件和目录。)
正准备解包 .../python-lxml_4.2.1-1ubuntu0.1_amd64.deb  ...
正在解包 python-lxml:amd64 (4.2.1-1ubuntu0.1) ...
正在设置 python-lxml:amd64 (4.2.1-1ubuntu0.1) ...
```


3、索引配置

3.1 修改py文件

打开终端，切到/var/www/html/wooyun目录下，分别在脚本app_bugs.py、app_drops.py中修改如下语句，更改参数如主机、端口号、用户名、密码(将光标定位到需要更改的位置，输入i，即可进行添加)。

```
cqq@cqq-virtual-machine:/var/www/html/wooyun$ su root
密码：
root@cqq-virtual-machine:/var/www/html/wooyun# vi app_bugs.py
root@cqq-virtual-machine:/var/www/html/wooyun#
root@cqq-virtual-machine:/var/www/html/wooyun# vi app_drops.py
root@cqq-virtual-machine:/var/www/html/wooyun#
```

3.2 创建数据库、表

在mysql中建立数据库wooyun，数据表bugs、drops，分别建立字段title、dates、author、type、corp、doc与title、dates、author、type、doc。

```
CREATE DATABASE `wooyun` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci;

create table bugs(title VARCHAR(500),dates DATETIME, author CHAR(255),type
CHAR(255),corp CHAR(255),doc VARCHAR(200) PRIMARY KEY);

create table drops(title VARCHAR(500),dates DATETIME, author CHAR(255),type
CHAR(255),doc VARCHAR(200) PRIMARY KEY);
```

注意mysql编码如下，需要为utf-8（character_set_server不为utf-8要修改mysql配置文件）

```
use wooyun;

show variables like 'character%'; #查看编码

+--------------------------+----------------------------+


| Variable_name            | Value                      |


+--------------------------+----------------------------+


| character_set_client     | utf8                       |


| character_set_connection | utf8                       |


```

```
| character_set_database   | utf8                       |

| character_set_filesystem | binary                     |

| character_set_results    | utf8                       |

| character_set_server     | utf8                       |

| character_set_system     | utf8                       |

| character_sets_dir       | /usr/share/mysql/charsets/ |

+--------------------------+----------------------------+
```

以下是修改character_set_server的编码的方法。修改完之后，记得重启mysql服务。

```
root@cqq-virtual-machine:~# vi /etc/mysql/mysql.conf.d/mysqld.cnf
root@cqq-virtual-machine:~#
root@cqq-virtual-machine:~# systemctl restart mysql
root@cqq-virtual-machine:~#
```

```
[mysqld]
#
# * Basic Settings
#
character-set-server=utf8

user            = mysql
pid-file        = /var/run/mysqld/mysqld.pid
socket          = /var/run/mysqld/mysqld.sock
port            = 3306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
lc-messages-dir = /usr/share/mysql
skip-external-locking
```


3.3 建立索引

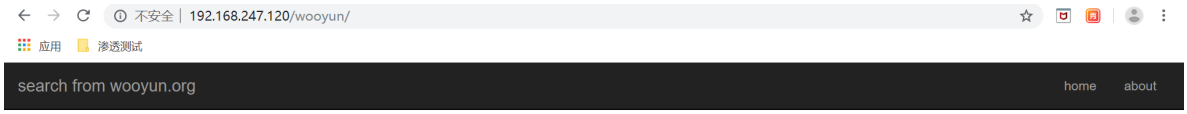
切换到/var/www/html/wooyun目录下，分别执行app_bugs.py、app_drops.py文件

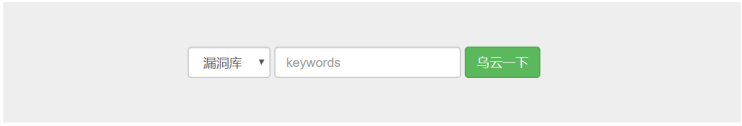
```
python ./app_bugs.py

python ./app_drops.py
```

执行完后在mysql中进行查询，bugs数目为40280，drops数目为1264

```
use wooyun;

select count(*) from bugs;

select count(*) from drops;
```

在浏览器中输入"Web服务器http://ip/wooyun"，便可以进入到WooYun查询页面。





提交时间	标题	漏洞类型	提交者
2016-05-27	APP安全之趣网APP存在XSS与SQL注入漏洞	SQL注射漏洞	我在不想理你
2016-05-11	APP安全之鱼泡泡无效xss杀入俩后台系统操控80万用户	XSS 跨站脚本攻击	小龙
2016-05-09	暴风墨镜某站存储型xss漏洞可获取超级管理员权限	XSS 跨站脚本攻击	蓝①依
2016-05-05	腾讯又一XSS被广泛用于黑产	XSS 跨站脚本攻击	%2e
2016-05-04	暴风魔镜多处漏洞打包（撞库/xss/Getshell）	成功的入侵事件	干机
2016-05-03	discuz某插件漏洞导致qq域名xss	XSS 跨站脚本攻击	弥生
2016-05-03	新浪某地区分站Flash逆向分析存安全隐患可进行XSS利用	XSS 跨站脚本攻击	chengable
2016-05-03	我是如何利用组合拳一步步攻陷匹克内网的(XSS配合CSRF/利用DNS配合SQL注入获取数据等等)	未授权访问/权限绕过	Mr.Q
2016-04-28	APP安全之朋友印象一处无效xss爆破导致www后台被登录(100万设备/150万用户/1000万微信用户/核心功能可修改用户密码)	XSS 跨站脚本攻击	小龙
2016-04-27	点开我的链接就上了你的QQ mail（非xss）	敏感信息泄露	he1renyagao
2016-04-26	华夏航空某系统存储型XSS漏洞(已登录系统)	XSS 跨站脚本攻击	jianFen