

网站搭建-LAMP

Kali Linux实际上内置了Apache、Nginx、PHP和MySQL，满足LAMP和LNMP环境，省得我们再去部署

我们这里使用LAMP作为生产力环境

首先我们安装Apache PHP模块，用下面命令来安装

```
sudo apt install libapache2-mod-php
```

我们通过下面命令来重启Apache，此时，Linux会向你索要系统密码

```
sudo systemctl restart apache2
```

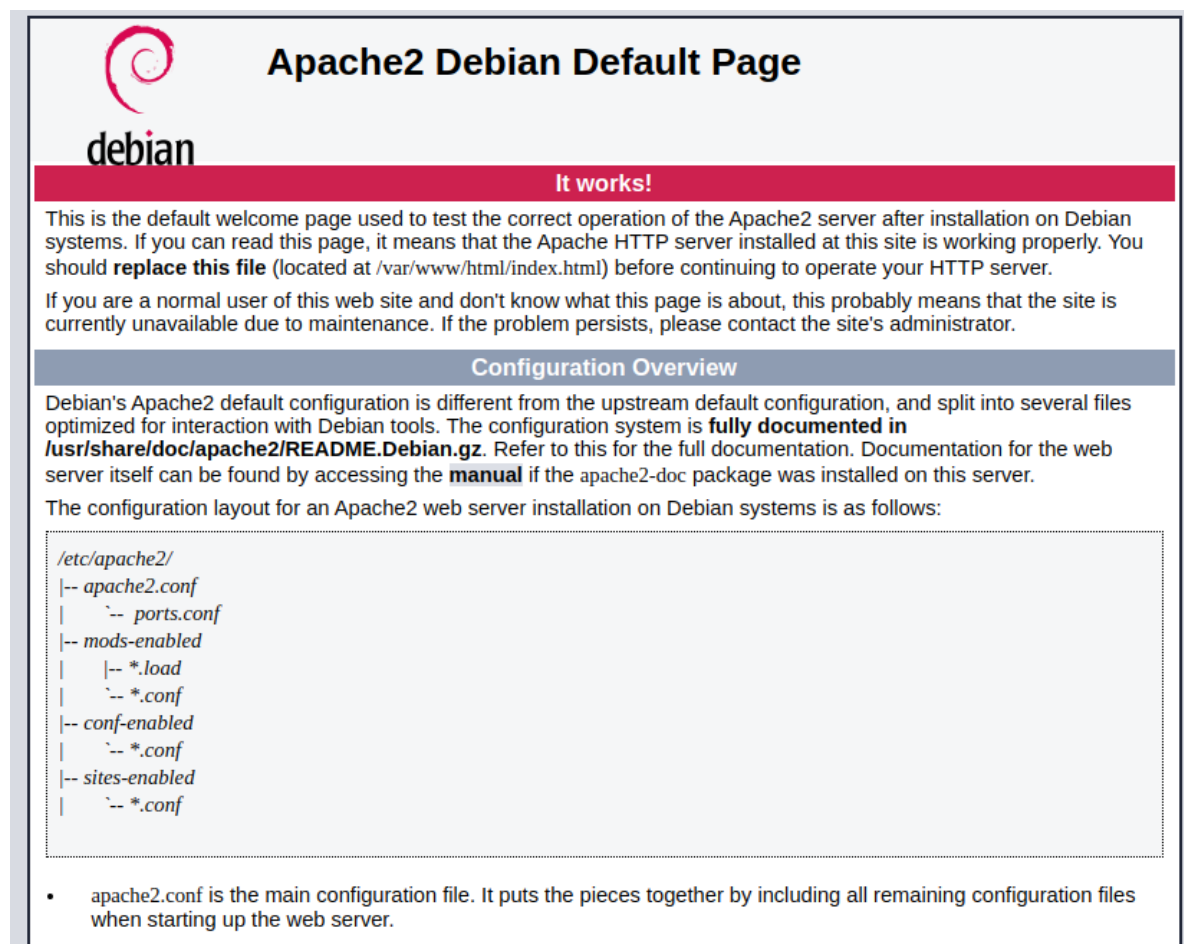
另外再安装MySQL和GD PHP扩展

```
sudo apt install php-mysql php-gd
```

要测试Web服务器是否已正确配置以进行PHP处理，使用以下代码在/var/www/html目录中创建一个名为info.php的新文件：

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

保存文件后，我们在浏览器输入“127.0.0.1”则可以看到Apache的欢迎页



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.


The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- **apache2.conf** is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

之后我们在“127.0.0.1”后加上“/info.php”，也就是“127.0.0.1/info.php”

我们即可看到PHP的详情页，当出现这个页面，即代表PHP正常可用

PHP Version 8.1.2	
	
System	Linux Recgov 5.16.0-kali7-amd64 #1 SMP PREEMPT Debian 5.16.18-1kali1 (2022-04-01) x86_64
Build Date	Apr 24 2022 08:36:32
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.1/apache2
Loaded Configuration File	/etc/php/8.1/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.1/apache2/conf.d
Additional .ini files parsed	/etc/php/8.1/apache2/conf.d/10-mysqld.ini, /etc/php/8.1/apache2/conf.d/10-opcache.ini, /etc/php/8.1/apache2/conf.d/10-pdo.ini, /etc/php/8.1/apache2/conf.d/20-calendar.ini, /etc/php/8.1/apache2/conf.d/20-ctype.ini, /etc/php/8.1/apache2/conf.d/20-exif.ini, /etc/php/8.1/apache2/conf.d/20-ffi.ini, /etc/php/8.1/apache2/conf.d/20-fileinfo.ini, /etc/php/8.1/apache2/conf.d/20-ftp.ini, /etc/php/8.1/apache2/conf.d/20-gettext.ini, /etc/php/8.1/apache2/conf.d/20-iconv.ini, /etc/php/8.1/apache2/conf.d/20-mysqli.ini, /etc/php/8.1/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.1/apache2/conf.d/20-phar.ini, /etc/php/8.1/apache2/conf.d/20-posix.ini, /etc/php/8.1/apache2/conf.d/20-readline.ini, /etc/php/8.1/apache2/conf.d/20-shmop.ini, /etc/php/8.1/apache2/conf.d/20-sockets.ini, /etc/php/8.1/apache2/conf.d/20-sysmsg.ini, /etc/php/8.1/apache2/conf.d/20-syssem.ini, /etc/php/8.1/apache2/conf.d/20-sysvshm.ini, /etc/php/8.1/apache2/conf.d/20-tokenizer.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902.NTS
PHP Extension Build	API20210902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

MySQL数据库的创建

之后我们需要创建一个MySQL数据库

首先我们输入下面的命令启动数据库

```
systemctl start mysql
```

此时，系统会再次向你索要root密码

启动MySQL后，由于是第一次启动，MySQL是没有密码的，我们需要使用下面的命令创建MySQL的密码

```
sudo mysql_secure_installation
```

输入后，我们根据提示输入两次密码，即可完成MySQL数据库root登录密码的创建

（注意，在设置过程中，会提示删除是否anonymous用户，是否拒绝root的远程访问，是否删除测试用的数据库等，这些都需要根据自己的实际情况进行选择。）

之后，我们需要使用下面的命令来重启MySQL

```
sudo /etc/init.d/mysqld restart
```

之后我们输入下面的命令来进入数据库

```
mysql -u root -p
```

之后，我们来创建一个普通数据库

```
create DATABASE Kali;
```

这样，我们就创建了一个名为“Kali”的数据库（这里的K为大写）

下面，我们需要为这个普通数据库（Kali）创建用户

```
grant all privileges on 数据库名称.*to 数据库用户名@'授权范围' identified by '数据库用户名的密码';
```

下面是一条实例

```
grant all privileges on Kali.*to Kali@'%' identified by 'Kali';
```

(%代表授权全网访问，如果是localhost即代表授权本机访问)

这里我们就为Kali这个名称的数据库，创建了一个数据库用户名为“Kali”，和密码为“Kali”的数据库用户

最终，我们要使权限生效

```
flush privileges;
```

部署一个钓鱼网站

我们先删除Apache2网站根目录所有文件

```
rm -rf /var/www/html/*
```

我们再执行如下命令来解压短信轰炸机源码到网站根目录

```
sudo unzip dy.zip -d /var/www/html/
```

我们需要修改网站文件来对接数据库，而这个网站源码，对接数据库的源码文件是这个"config.php"

```
sudo vim /var/www/html/config.php
```

由于这个源码内附带一个".sql"文件，需要我们手动导入数据库

所以，我们输入

```
sudo mysql -u root -p
```

登录root数据库后，我们需要切换用户到刚刚创建的数据库

```
use Kali
```

之后我们导入".sql"文件

```
source /var/www/html/install.sql
```

```
(max@Recgov)-[~]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 56
Server version: 10.6.7-MariaDB-3 Debian builddd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> use Kali
Database changed
MariaDB [Kali]> source /var/www/html/install.sql
Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.000 sec)

Query OK, 0 rows affected (0.034 sec)

Query OK, 1 row affected (0.001 sec)

Query OK, 0 rows affected (0.004 sec)

Query OK, 0 rows affected (0.004 sec)

MariaDB [Kali]>
```

完成!

之后我们在浏览器打开"127.0.0.1"即可

如果是局域网访问，那么我们需要用到如下命令

`ifconfig`

```
(max@Recgov)-[~]
$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 77082 bytes 27554479 (26.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77082 bytes 27554479 (26.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.115 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::e6aa:eaff:febf:b317 prefixlen 64 scopeid 0<link>
    ether e4:aa:ea:bf:b3:17 txqueuelen 1000 (Ethernet)
    RX packets 52400 bytes 30481791 (29.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36493 bytes 6903492 (6.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

我们可以看到下面的第二行"192.168.10.115"

只要在同一局域网内的设备，浏览器打开这个IP地址即可访问Kali本机的网站

而公网也同理，你需要一个公网IP，其实这里我更推荐使用VPS服务器，因为普通电脑不适合做网站，或者说，不适合当网站服务器来用

