****

实验报告

|  |  |
| --- | --- |
| 姓名： | 强珂阳 |
| 学号： | 57118106 |

东南大学网络空间安全学院

School of Cyber Science & Engineering

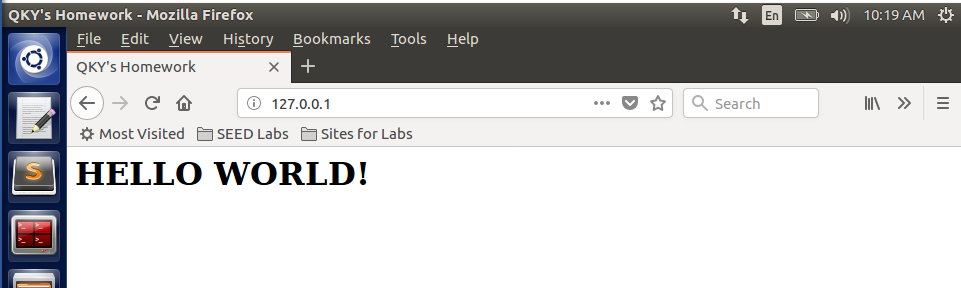
Southeast University

2020年9月

实验一

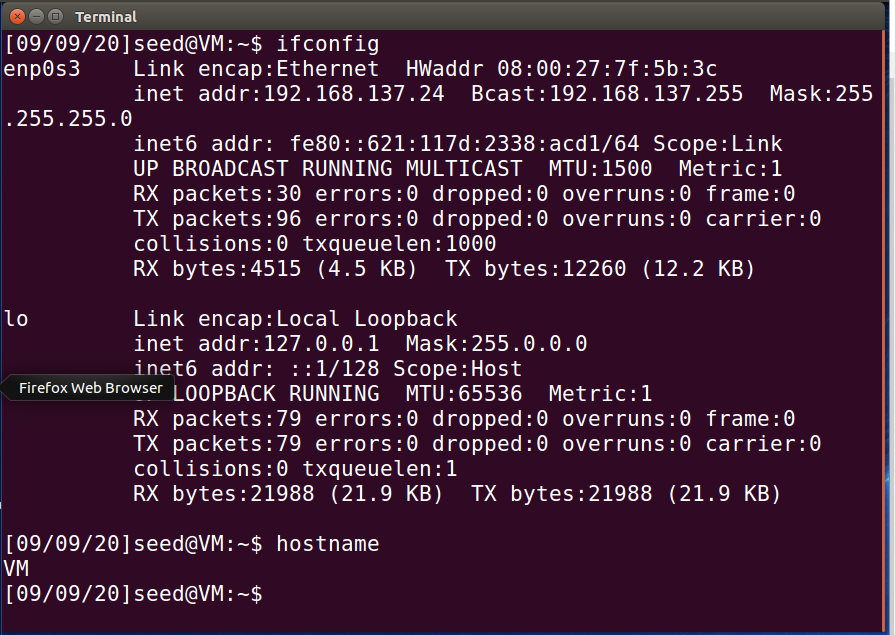
TASK1：**安装apache服务器 并用简单页面验证**

在安装完Apache后，更改index.html内容后，刷新网页显示，更改成功：

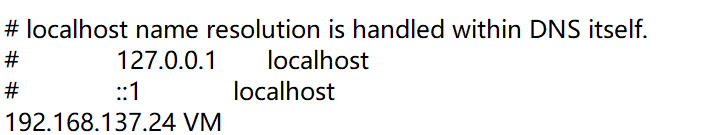


TASK2：**通过host文件解析文件名称**

通过ifconfig命令得到虚拟机ip地址，通过hostname命令获得虚拟机名称：

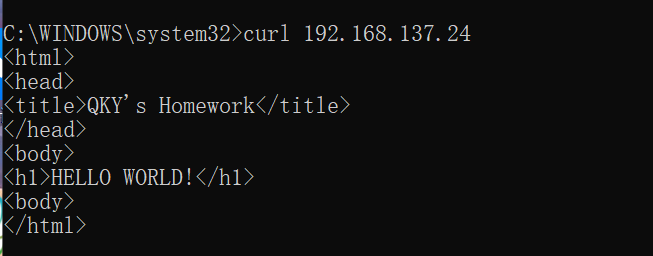


更改hosts文件的权限后，用记事本方式打开并添加虚拟机的ip地址以及主机名并保存：



TASK3：**编写HTTP客户端，使用http库检索站点的主页**

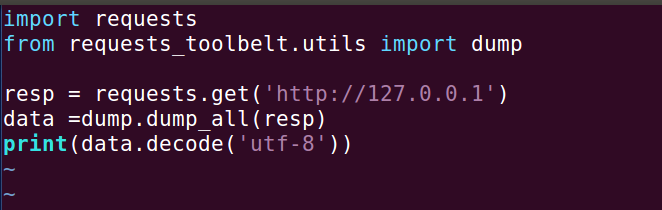
打开cmd，输入curl 192.168.137.24，得到编写的index文件内容：



查看虚拟机python版本：



下载requests\_toolbelt后编写test.py文件：



输出结果：

**root@VM:/home/seed# python3 test.py**

**< GET / HTTP/1.1**

**< Host: 127.0.0.1**

**< Connection: keep-alive**

**< Accept-Encoding: gzip, deflate**

**< User-Agent: python-requests/2.9.1**

**< Accept: \*/\***

**<**

**> HTTP/1.1 200 OK**

**> Last-Modified: Wed, 09 Sep 2020 05:25:17 GMT**

**> Connection: Keep-Alive**

**> Date: Wed, 09 Sep 2020 13:23:20 GMT**

**> Keep-Alive: timeout=5, max=100**

**> Server: Apache/2.4.18 (Ubuntu)**

**> Content-Type: text/html**

**> Vary: Accept-Encoding**

**> Content-Encoding: gzip**

**> Content-Length: 91**

**> ETag: "61-5aedaad538d58-gzip"**

**> Accept-Ranges: bytes**

**>**

**<html>**

**<head>**

**<title>QKY's Homework</title>**

**</head>**

**<body>**

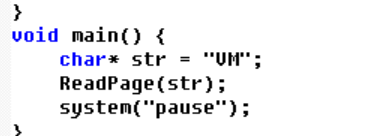
**<h1>HELLO WORLD!</h1>**

**<body>**

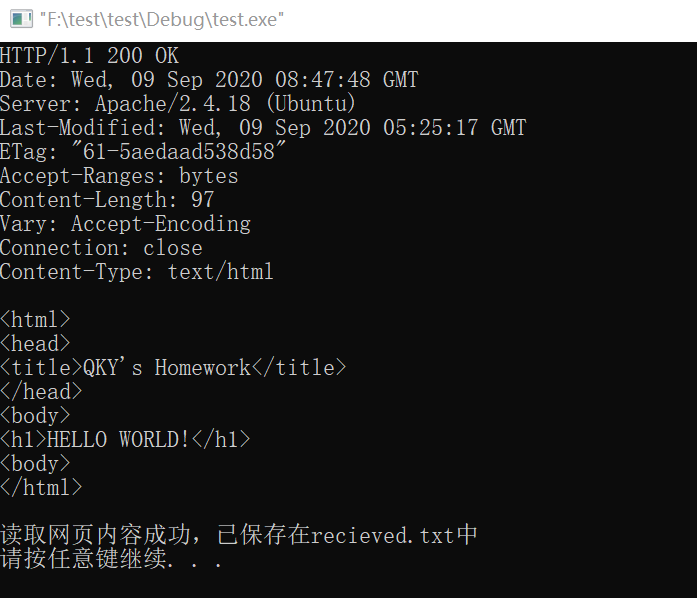
**</html>**

TASK4：**编写HTTP客户端以使用套接字检索站点的主页**

在物理机上创建test.cpp文件，并将main函数中的srt变量赋成自己的虚拟机名称：



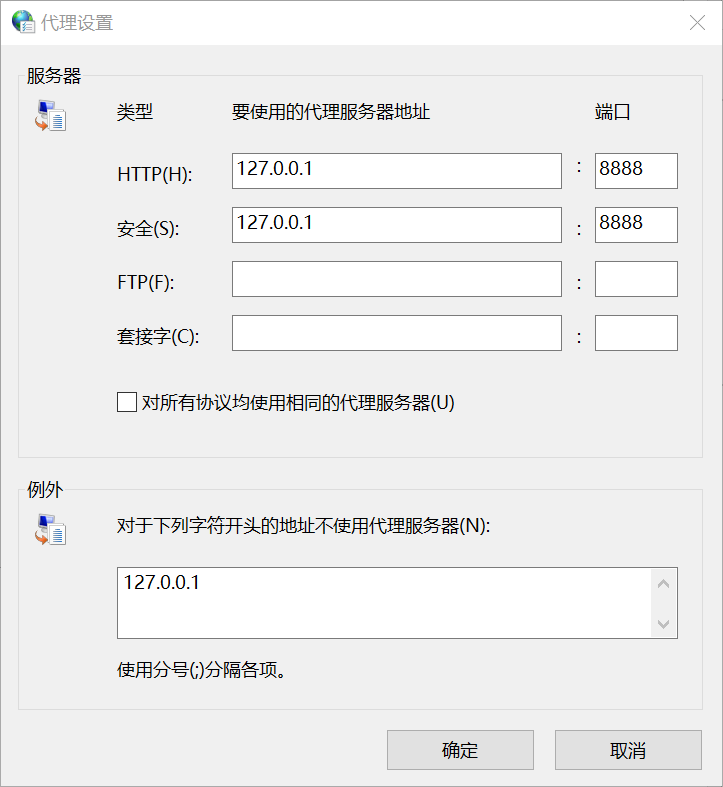
编译运行后得到：



说明网页定向准确。

TASK5：**下载软件Burp Suite并访问网站查看请求与响应的信息**

下载Burp Suit并配置好jdk环境。对测试浏览器进行代理设置：

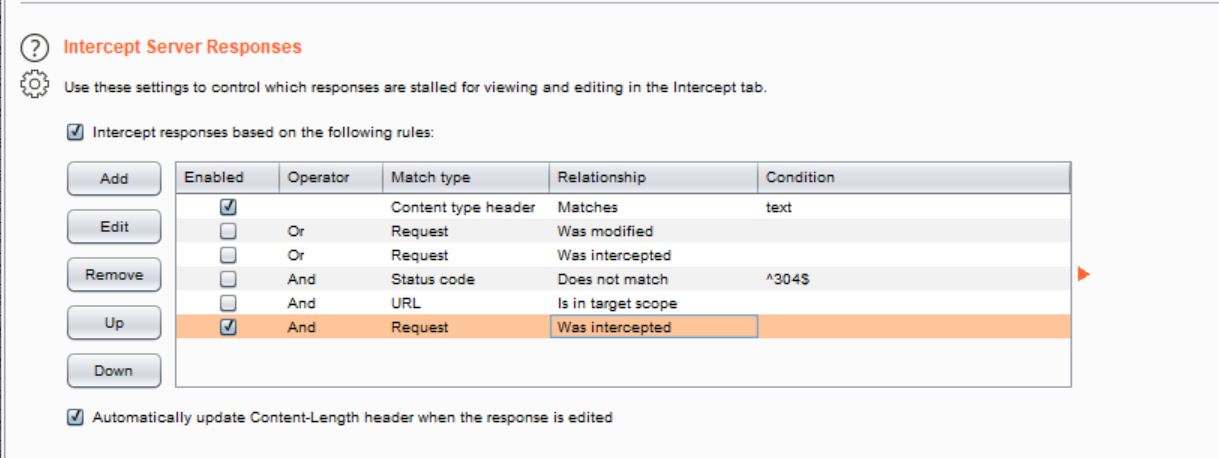


在Burp Suite中更改proxy代理，端口为8888.

使用浏览器打开my.seu.edu.cn查看拦截情况：



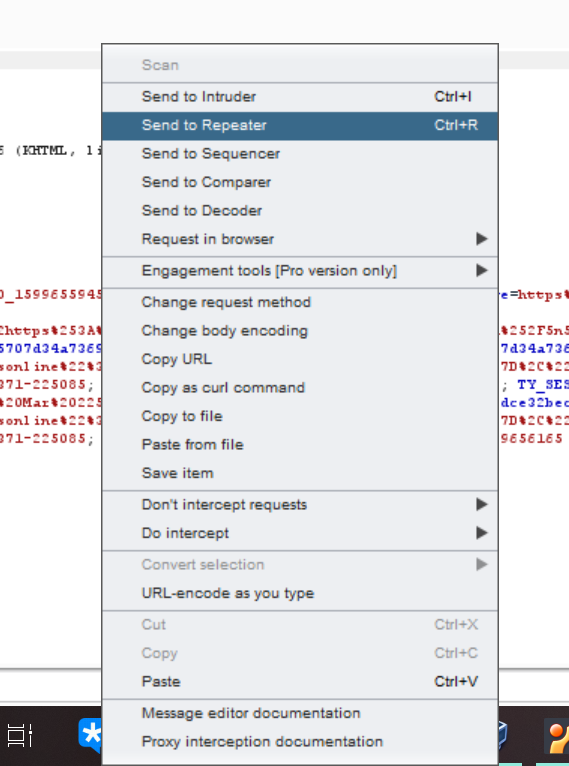
添加设置



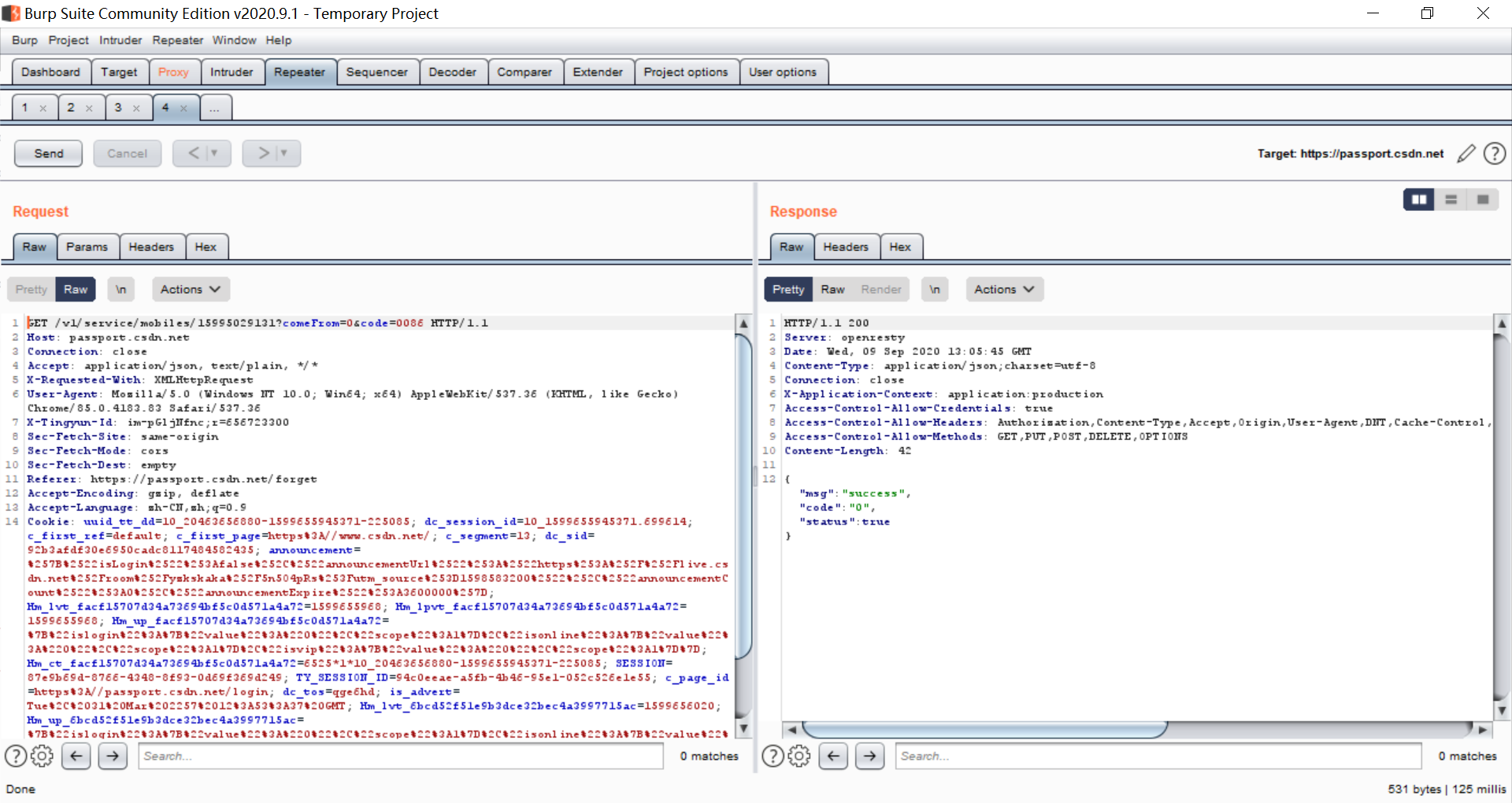
先关闭intertcept is on按钮关闭，并登录csdn网站进入通过手机找回密码的页面，打开intertcept is on按钮，输入手机号并点击获取验证码后，不断点击forward按钮。



在intercept页面右击选择send to repeater：



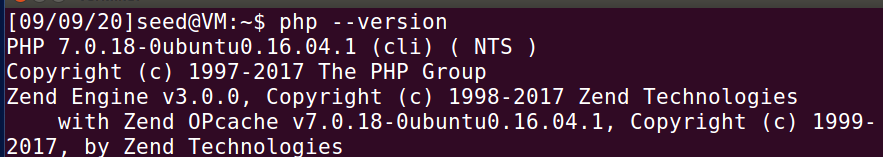
打开repeater，并点击send按钮发送request，可以看到界面右边出现response的内容，如下图：



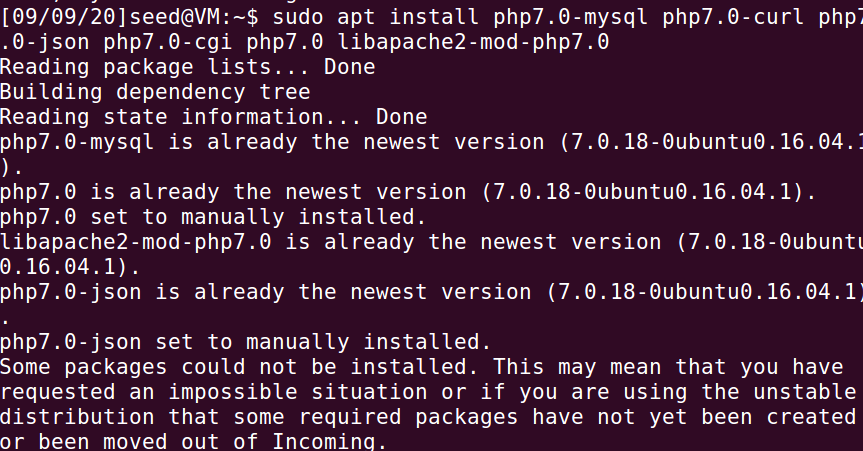
实验二（选做）

TASK1：**在虚拟机安装PHP，编写回显URL参数脚本**

查询本机php的版本，得到版本为7.0：



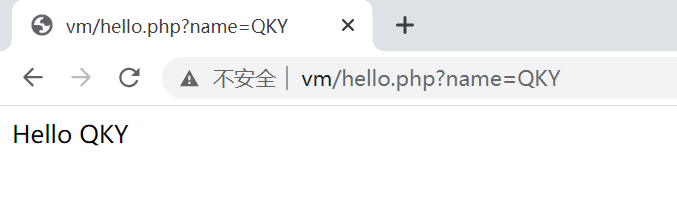
安装php 7.0对应的依赖库：



在/var/www/html中编写hello.php文件：

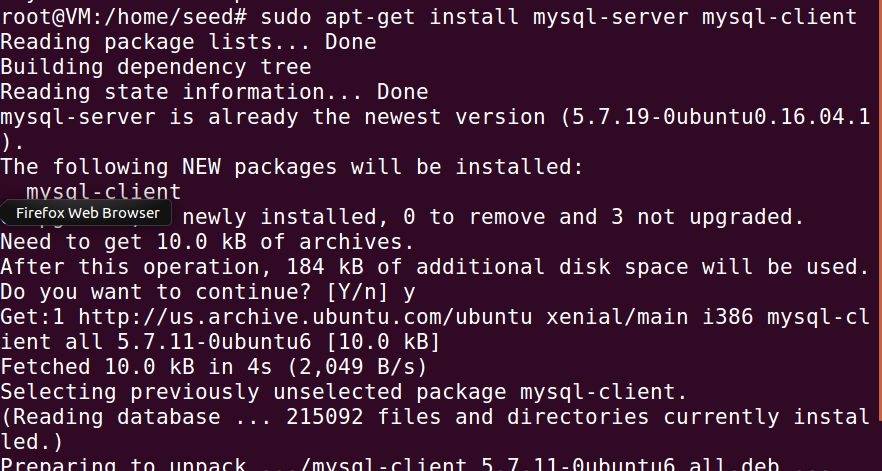


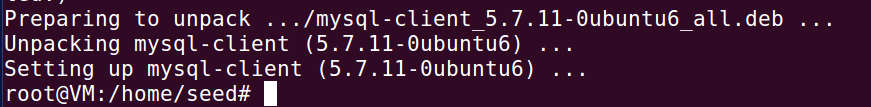
在物理机上打开<http://vm/hello.php?name=QKY>，显示：



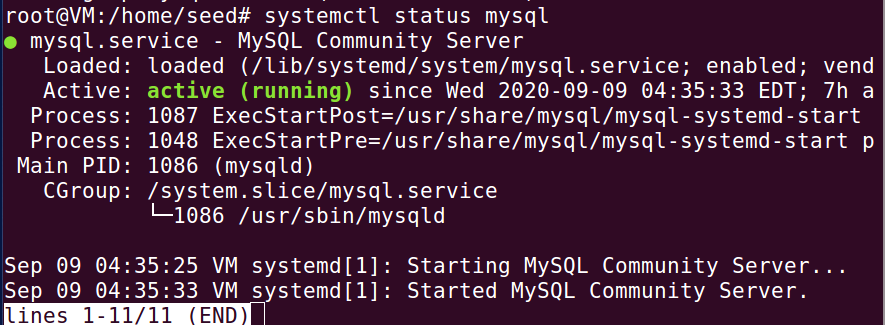
TASK2：**安装Mysql服务**

安装Mysql：

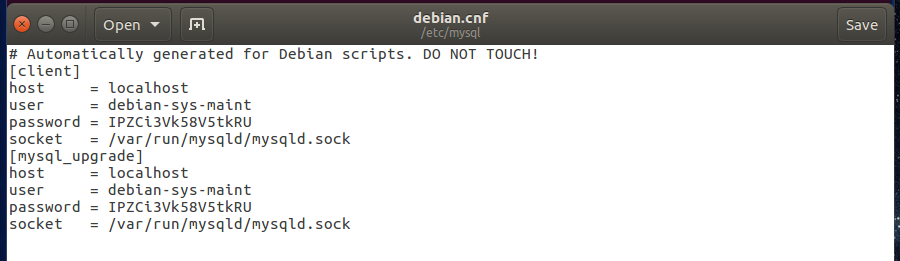




查看mysql状态，得知为启动状态：



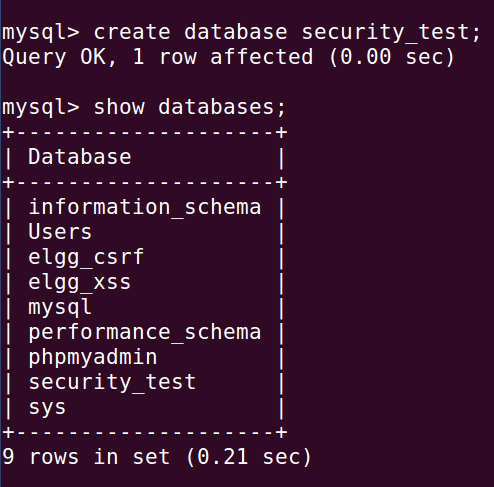
查看mysql自动创建的用户的用户名以及密码：



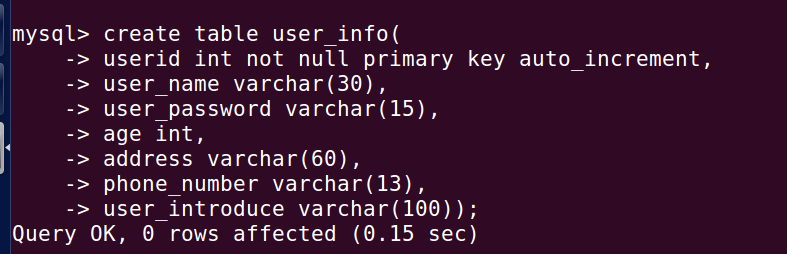
用户名：Debian-sys-maint

密码：IPZCi3Vk58V5tkRU

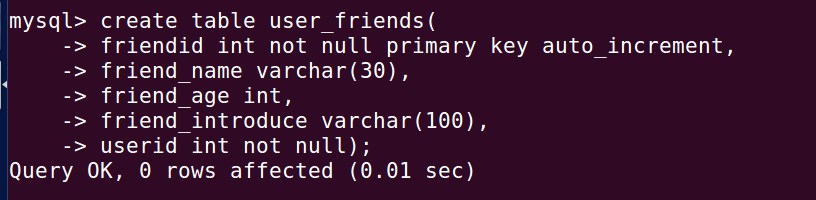
创建数据库security\_test:



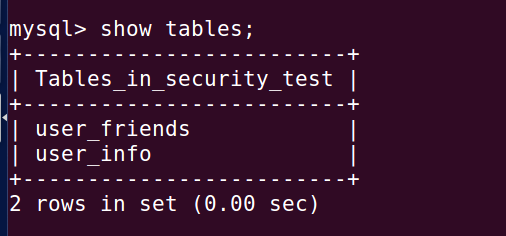
创建用户信息表：



创建用户好友列表：

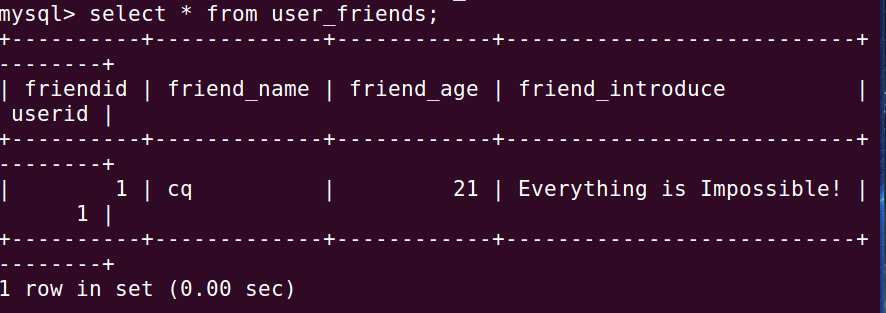


查看表格信息：



在user\_info表格中插入信息insert into user\_info values (1,'qky','123456',20,'china','14786432587','Nothing is Impossible!');

在user\_friends表格中插入信息insert into user\_friends(friendid,friend\_name,friend\_age,friend\_introduce,userid) values (1,'cq',21,'everything is impossible!',1);

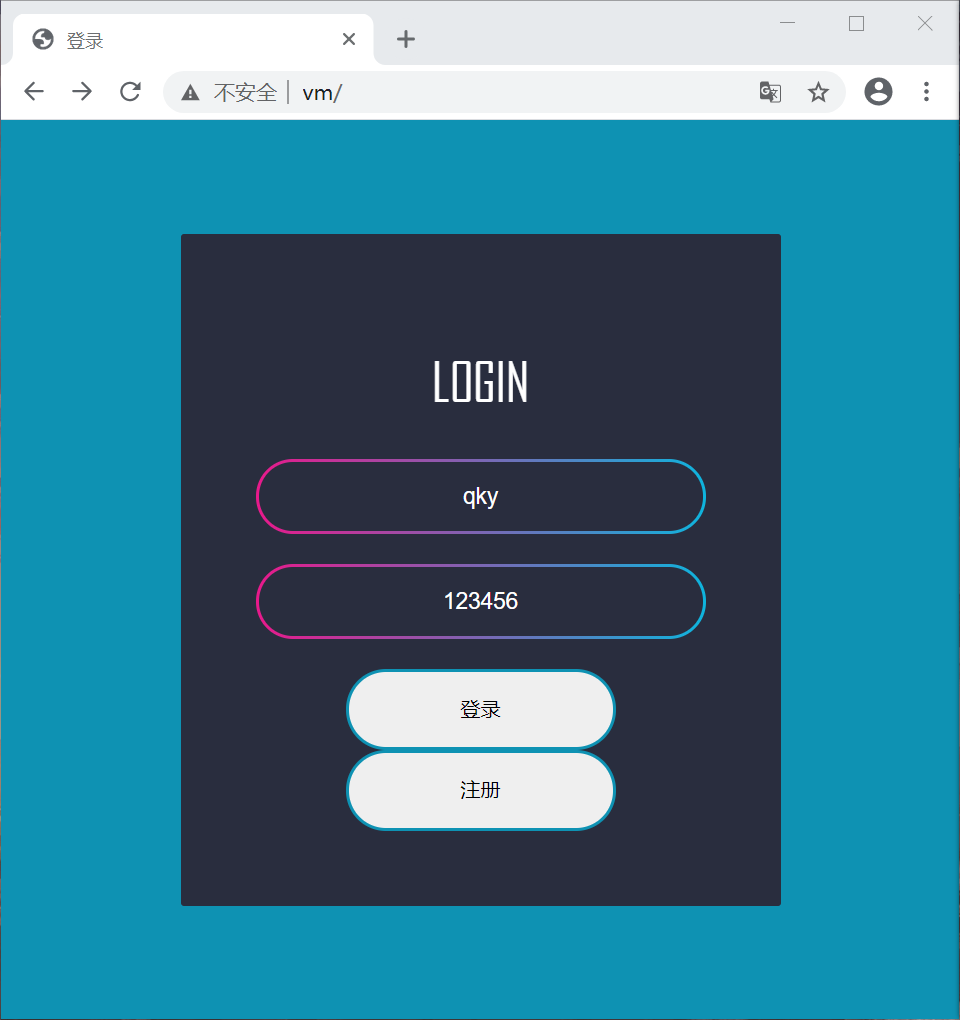


TASK2：**测试运行一个简易的项目模板**

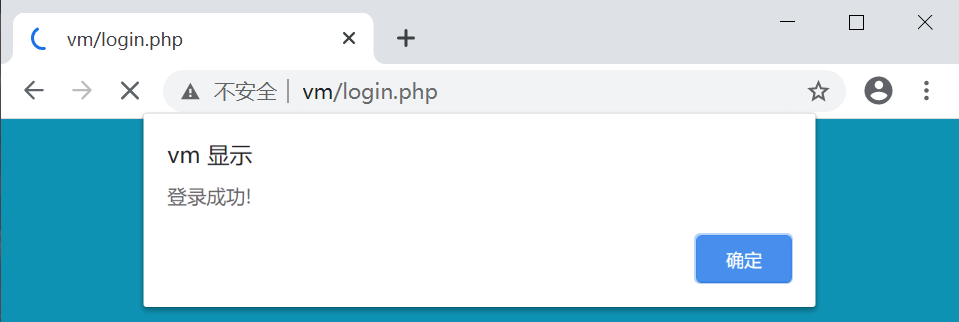
由于我的虚拟机联网经常出现问题，为了能够尽快完成实验，在这一个task里直接解压老师提供的文件到/var/www/html中并删掉原来的hello.php文件。打开utils文件夹下的mysqlBase.php文件，将对应数据改成自己虚拟机上的信息：



使用物理机访问<http://vm>，出现以下登陆界面，输入自己填入user\_info表中的用户名和密码：



登陆成功：



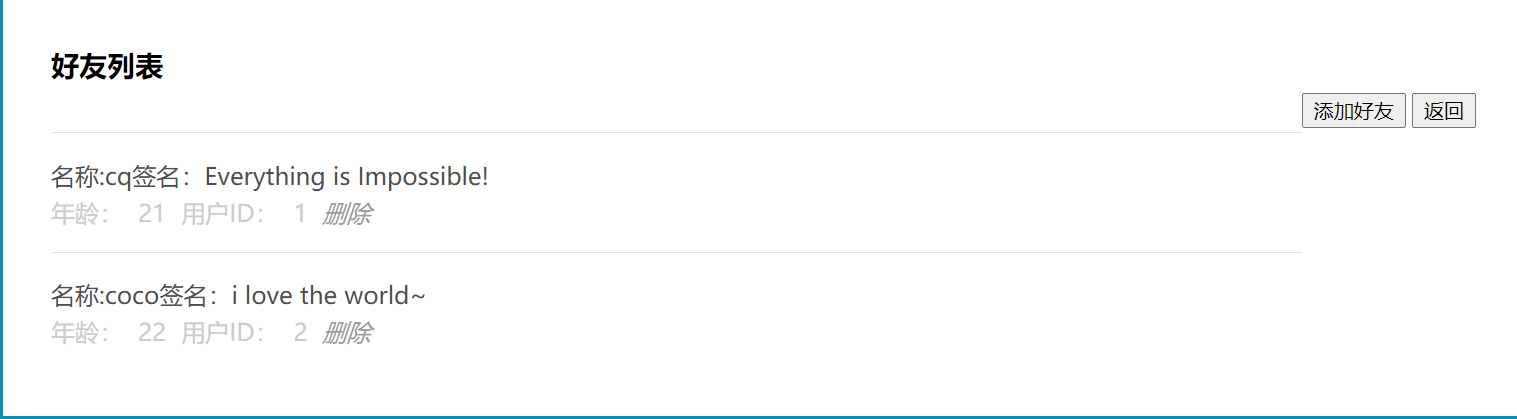
出现个人信息界面：



查看好友列表，可以看到填入user\_friends表格中的信息：



选择添加好友并编辑相关信息，好友列表出现新的一栏：



**总结：**

这个实验中，遇到最大的困难就是虚拟机连网的问题，将解决方法记录下，以供以后参考。在第一次将控制芯片选择准虚拟化网络后成功连网，但是重启虚拟机后又出现断网。在参考<https://www.cnblogs.com/heruiguo/p/11132887.html>后解决了问题，但依旧是重启后会断网。最后又尝试了更改控制芯片为Intel PRO/1000 MT 桌面（82540EM）后暂时解决了问题。

在实验在过程中，通过burp suit直观感受了浏览器访问网站过程中，发送请求与接收回复的过程。也初步体验了php等相关的语言，并对MySQL的数据结构有了一些认识。