1.这里和java中操作数据库是一样的，基本上

# 2.我们到了yanzheng的java文件中开始通过数据库来验证用户是不是正确的

public void doGet(ServletRequest req,ServletRespons res){

String u = req.getParameter("username");

String p = req.getPatameter("password");

//连接数据库 /下面这个是驱动包

class .forName("com.microsoft.jdbc.sqlserver.SQLServerDriver")

//得到连接 前面的是数据的Url 第二个是数据库名，后面的那个是密码

Connection cn = DriverManager.getConnection("","","")

//创建一个Statement

Statement sm = ct.creatStatement();

//我们知道用户名和密码是不可能重复的所以我们查询的时候选择 top 1

ResultSet rs = sm.executeQuery("select top 1 \* from where username ="'+u

+"' and password = '"+p+'");

//如果有的话就会执行下面的东西

if(re.next){

3.现在我们从数据库中验证就是基本就结束了，但是我们上面打开了很多的东西需要我们关闭，否则就是浪费了资源了，那么我们到了哪里去关闭呢，（不管将来会不会发生异常，我们都需要将它关闭，所以我们到了异常中的final中），但是我们发现我们生命的变量都写到了try里面了，需要将它放到外面去（方法下面就可以了）

Statement st = null;

public void doGet(ServletRequest req,ServletRespons res){

Connection cn =null;

Statement sm = mull;

ResultSet rs = null;

String u = req.getParameter("username");

String p = req.getPatameter("password");

//连接数据库 /下面这个是驱动包

class .forName("com.microsoft.jdbc.sqlserver.SQLServerDriver")

//得到连接 前面的是数据的Url 第二个是数据库名，后面的那个是密码

cn = DriverManager.getConnection("","","")

//创建一个Statement

sm = ，ct.creatStatement();

//我们知道用户名和密码是不可能重复的所以我们查询的时候选择 top 1

rs = sm.executeQuery("select top 1 \* from where username ="'+u

+'" and password =" '+p+'"”);

//如果有的话就会执行下面的东西

if(re.next){

## 4.上面应该有try但是我没写，关闭的时候也要注意顺序

1.先是resulet 然后是statement最后是连接Connection

finally{

try{if(rs!=null){

rs.close();}

if(sm!=null){

sm.close();}if(cn!=null){

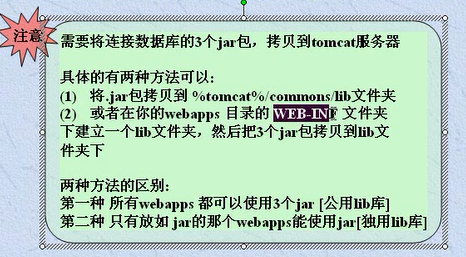
cn.close();}

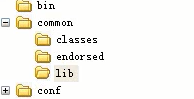
}catch(){

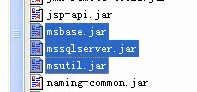
}

}

5.这样尽管代码正确了，但是我们在打开网页的时候还会出错，因为有三个数据库的jar包没有进入到我们的项目中







## 6.所以我们想尽办法找到这三个包，然后放到我们的conmmon文件夹下面

## 的lib中

# 7.即使这样可以显示了，我们的漏洞还是存在的，当我们的用户输入下面的东西时，阴影部分就是用户的上面有了or



8.所以我们回到yanzheng的java文件中修改下面的挑选语句

rs = sm.executeQuery("select top 1 pasaword from where username ="'+u+"'");

9.上面的只是先筛选了用户名，(通过用户名得到密码)现在我们就需要先对用户的名字进行分析，存在还是不存在

if(re.next){

//用户存在

String dbPassword = rs.getString(1);

if(dbPassword.equals(p)){

//用户真的合法

}else{

}

10.这样就是完成了