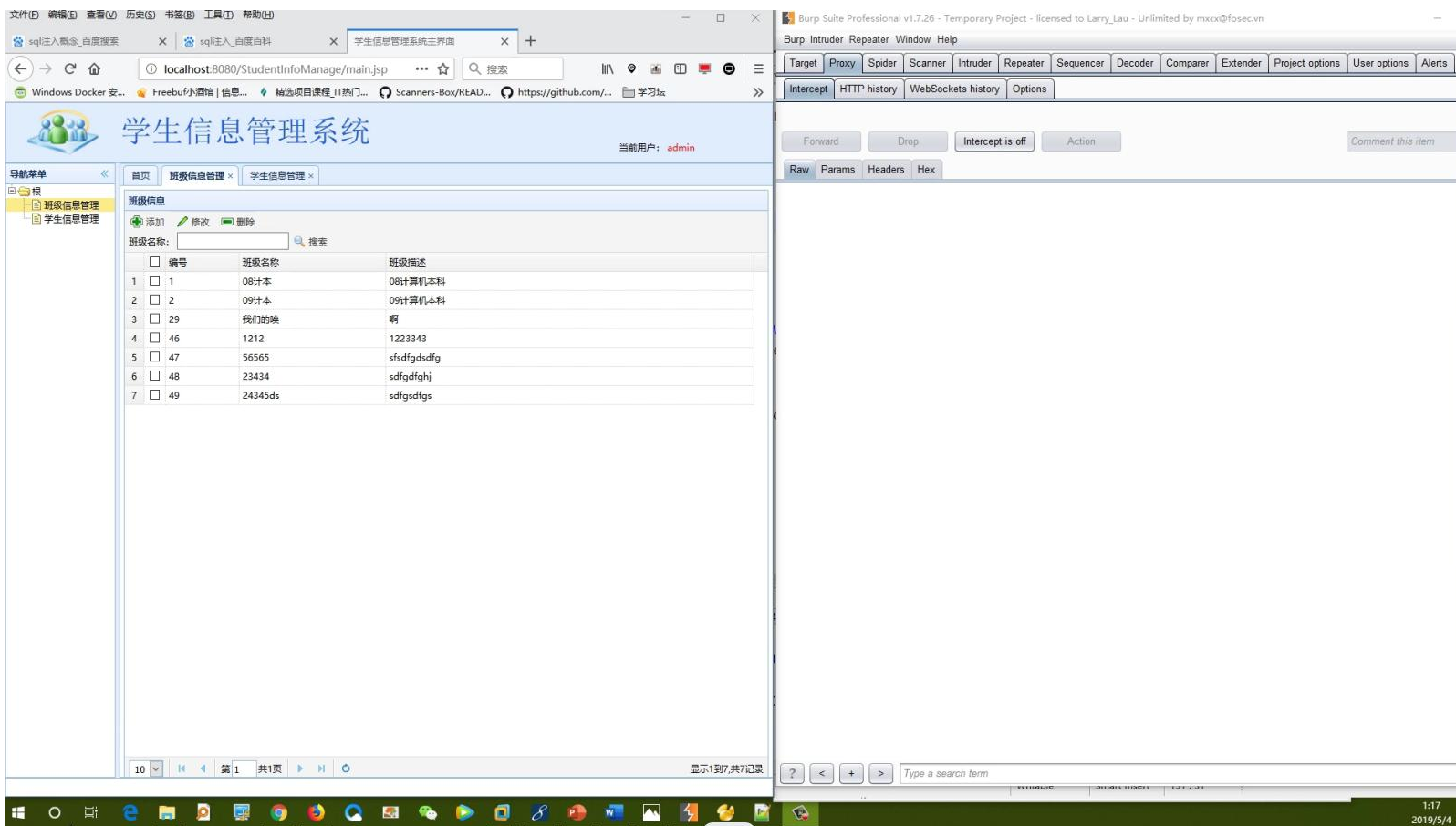
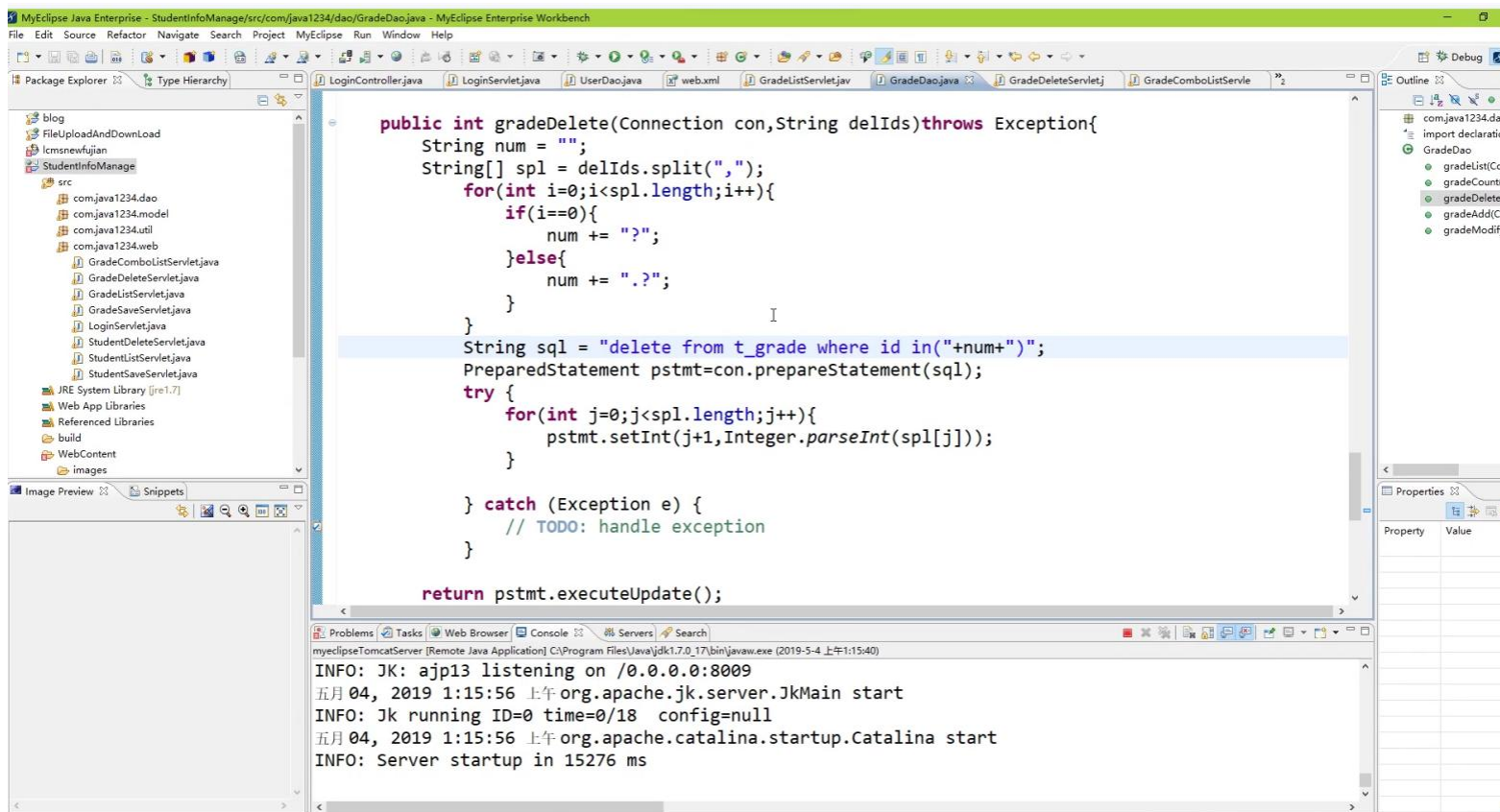


# java代码审计 深度解析

# 第八课 jdbc-in-修复后无法注入



赛博梦工厂  
Cyber Works



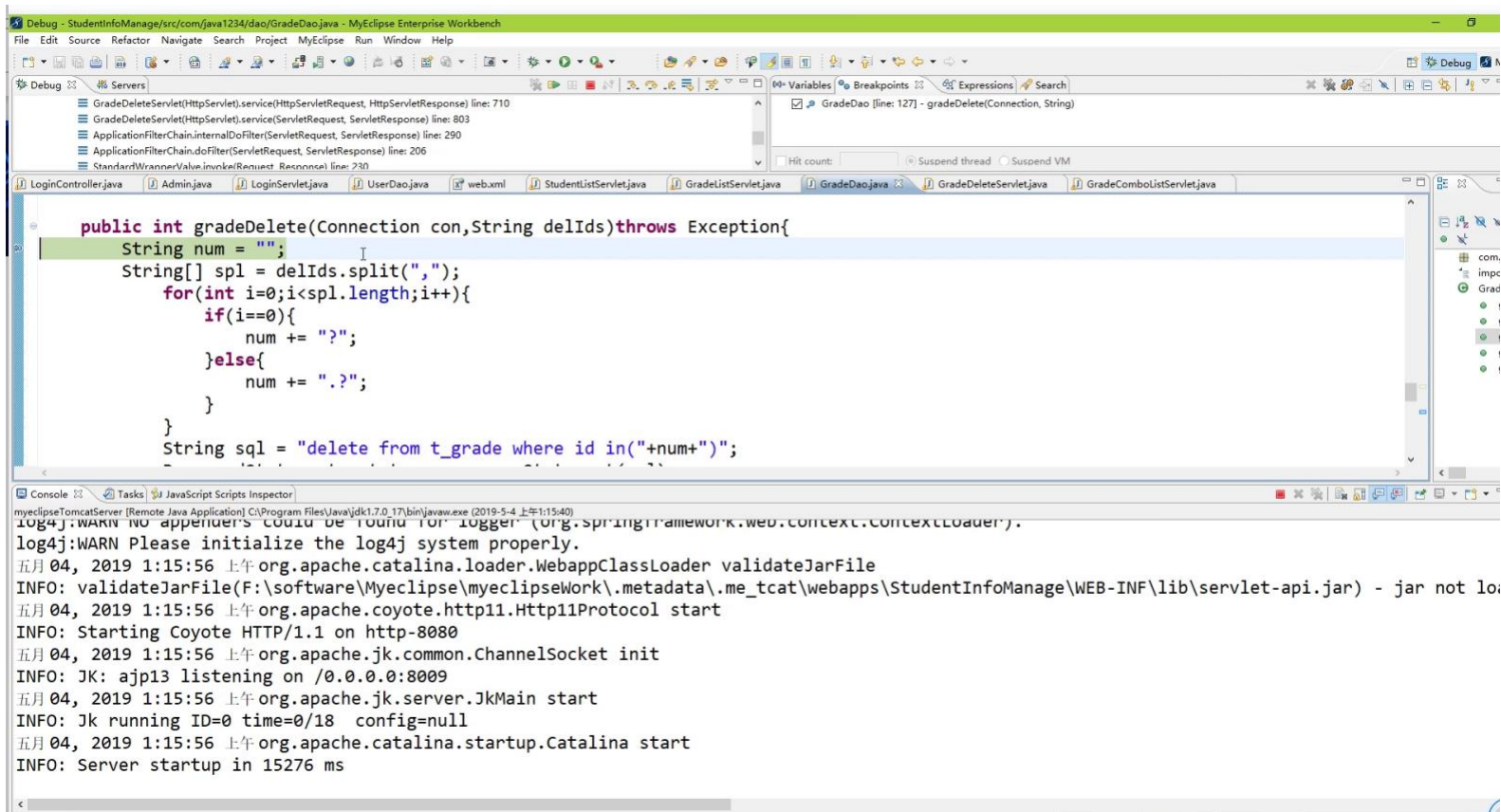
```
public int gradeDelete(Connection con,String delIds)throws Exception{
    String num = "";
    String[] spl = delIds.split(",");
    for(int i=0;i<spl.length;i++){
        if(i==0){
            num += "?";
        }else{
            num += ".?";
        }
    }
    String sql = "delete from t_grade where id in("+num+")";
    PreparedStatement pstmt=con.prepareStatement(sql);
    try {
        for(int j=0;j<spl.length;j++){
            pstmt.setInt(j+1,Integer.parseInt(spl[j]));
        }
    } catch (Exception e) {
        // TODO: handle exception
    }

    return pstmt.executeUpdate();
}
```

myeclipseTomcatServer [Remote Java Application] C:\Program Files\Java\jdk1.7.0\_17\bin\javaw.exe (2019-5-4 上午11:15:40)

INFO: JK: ajp13 listening on /0.0.0.0:8009  
五月 04, 2019 1:15:56 上午 org.apache.jk.server.JkMain start  
INFO: Jk running ID=0 time=0/18 config=null  
五月 04, 2019 1:15:56 上午 org.apache.catalina.startup.Catalina start  
INFO: Server startup in 15276 ms





Debug - StudentInfoManage/src/com/java1234/web/GradeDeleteServlet.java - MyEclipse Enterprise Workbench

File Edit Source Refactor Navigate Search Project MyEclipse Run Window Help

Debug Servers

- Daemon Thread [TP-Processor1] (Running)
- Daemon Thread [TP-Processor3] (Running)
- Daemon Thread [http-8080-1] (Running)

C:\Program Files\Java\jdk1.7.0\_17\bin\javaw.exe (2019-5-4 上午11:54:0)

LoginController.java Admin.java LoginServlet.java UserDao.java web.xml StudentListServlet.java GradeListServlet.java

```
for(int i=0;i<str.length;i++){
    boolean f=studentDao.getStudentByGradeId(con, str[i]);
    if(f){
        result.put("errorIndex", i);
        result.put("errorMsg", "班级下面有学生, 不能删除!");
        ResponseUtil.write(response, result);
        return;
    }
}
int delNums=gradeDao.gradeDelete(con, delIds);
if(delNums>0){
    result.put("success", "true");
    result.put("delNums", delNums);
}else{
    result.put("errorMsg", "删除失败");
}
ResponseUtil.write(response, result);
}catch(Exception e){
    e.printStackTrace();
}finally{
```

Console

Tasks JavaScript Scripts Inspector

myeclipseTomcatServer [Remote Java Application] C:\Program Files\Java\jdk1.7.0\_17\bin\javaw.exe (2019-5-4 上午11:54:0)

myeclipseTomcatServer [Remote Java Application] C:\Program Files\Java\jdk1.7.0\_17\bin\javaw.exe (2019-5-4 上午11:54:0)

java.sql.SQLException: No value specified for parameter 2

at com.mysql.jdbc.PreparedStatement.fillSendPacket(PreparedStatement.java:111)

at com.mysql.jdbc.PreparedStatement.executeUpdate(PreparedStatement.java:111)

at com.mysql.jdbc.PreparedStatement.executeUpdate(PreparedStatement.java:111)

t\_grade @db\_studentinfo (虚拟机) - 表

无标题 @db\_studentinfo... x t\_grade @db\_studentinfo...

文件 编辑 查看 窗口 帮助

导入向导 导出向导 筛选向导 网络查看 表单查看 备注 十六进制 图像 升序排序

| id | gradename | gradeDesc |
|----|-----------|-----------|
| 1  | 08计本      | 08计算机本科   |
| 2  | 09计本      | 09计算机本科   |
| 29 | 我们的       | 啊         |
| 46 | 1212      | 1223343   |
| 47 | 56565     | sfdgdsdfg |
| 48 | 23434     | sdfgdfghj |
| 49 | 24345ds   | sdfgsdfgs |

User options Ale

get: http://localho



```
Debug - StudentInfoManage/src/com/java1234/dao/GradeDao.java - MyEclipse Enterprise Workbench
File Edit Source Refactor Navigate Search Project MyEclipse Run Window Help
LoginController.java Admin.java LoginServlet.java UserDao.java web.xml StudentListServlet.java GradeListServlet.java GradeDao.java GradeDeleteServlet.java GradeComboListServlet.java

//安全的删除方法

public int gradeDelete(Connection con,String delIds)throws Exception{
    String num = "";
    String[] spl = delIds.split(",");
    for(int i=0;i<spl.length;i++){
        if(i==0){
            num += "?";
        }else{
            num += ".?";
        }
    }
    String sql = "delete from t_grade where id in("+num+")";
    PreparedStatement pstmt=con.prepareStatement(sql);
    try {
        for(int j=0;j<spl.length;j++){
            pstmt.setInt(j+1,Integer.parseInt(spl[j]));
        }
    } catch (Exception e) {
        // TODO: handle exception
    }

    return pstmt.executeUpdate();
}
```





谢谢观赏