java代码审计深度解析

第九课　jdbc-like原理及如何找注入

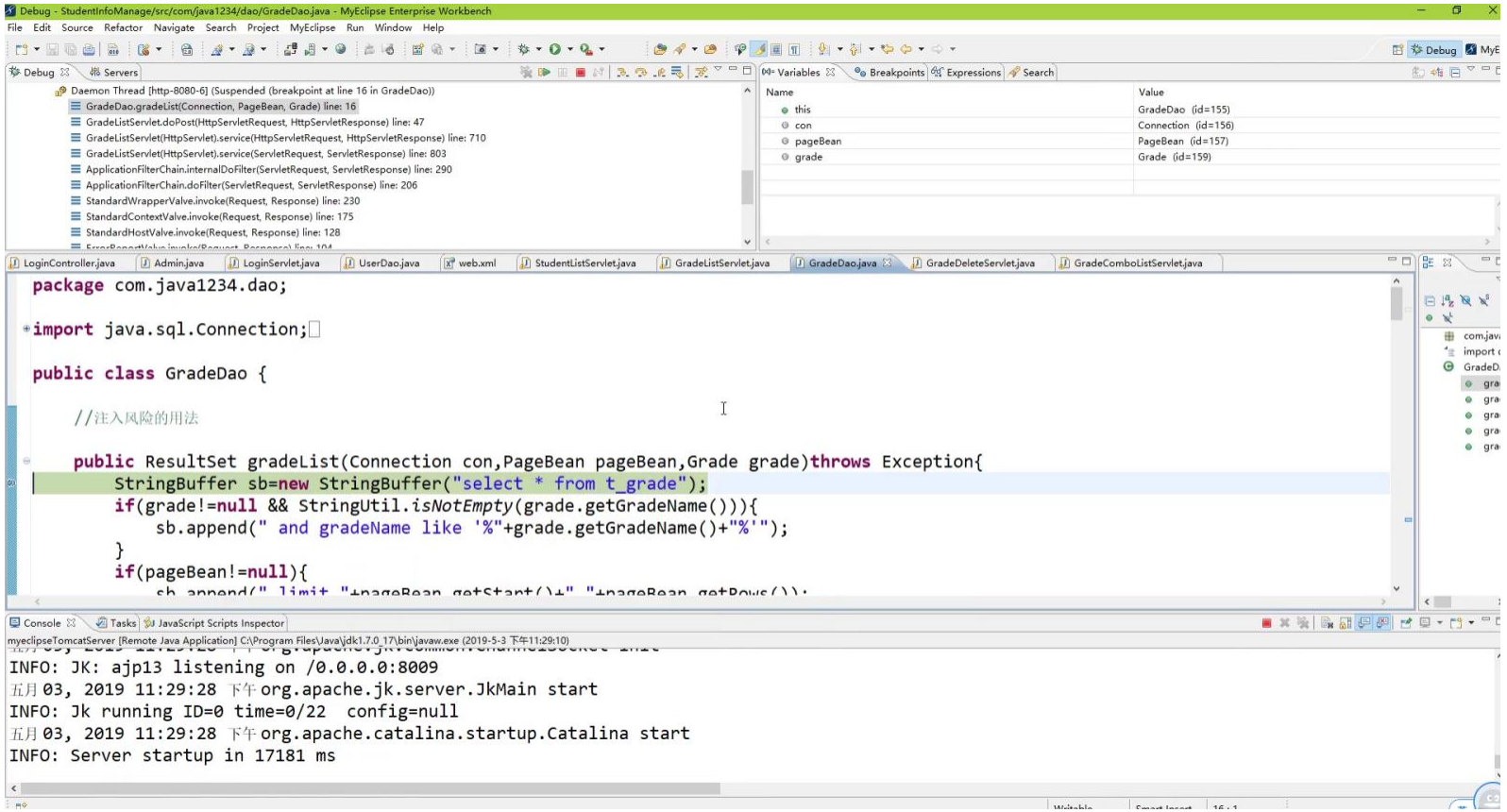
SQL注入-JDBC遇到like-不正确写法

当预处理遇到like

```
public ResultSet gradeList(Connection con,PageBean pageBean,Grade grade)throws Exception{
    StringBuffer sb=new StringBuffer("select * from t_grade");
    if(grade!=null && StringUtil.isNotEmpty(grade.getGradeName())){
        sb.append(" and gradeName like '%"+grade.getGradeName()+"%'");

    }
    if(pageBean!=null){
        sb.append(" limit "+pageBean.getStart()+","+pageBean.getRows());

    }
    PreparedStatement pstmt=con.prepareStatement(sb.toString().replaceFirst("and", "where"));
        return pstmt.executeQuery();
}
```


Debug - StudentInfoManage/src/com/java1234/dao/GradeDao.java - MyEclipse Enterprise Workbench
File Edit Source Refactor Navigate Search Project MyEclipse Run Window Help
Debug Servers
Daemon Thread [http-8080-6] (Suspended (breakpoint at line 16 in GradeDao))
GradeDao.gradeList(Connection, PageBean, Grade) line: 16
GradeListServlet.doPost(HttpServletRequest, HttpServletResponse) line: 47
GradeListServlet(HttpServlet).service(HttpServletRequest, HttpServletResponse) line: 710
GradeListServlet(HttpServlet).service(ServletRequest, ServletResponse) line: 803
ApplicationFilterChain.internalDoFilter(ServletRequest, ServletResponse) line: 290
ApplicationFilterChain.doFilter(ServletRequest, ServletResponse) line: 206
StandardWrapperValve.invoke(Request, Response) line: 230
StandardContextValve.invoke(Request, Response) line: 175
StandardHostValve.invoke(Request, Response) line: 128
Variables Breakpoints Expressions Search
Name Value
this GradeDao (id=155)
con Connection (id=156)
pageBean PageBean (id=157)
grade Grade (id=159)
LoginController.java Admin.java LoginServlet.java UserDao.java web.xml StudentListServlet.java GradeListServlet.java GradeDao.java GradeDeleteServlet.java GradeComboListServlet.java
package com.java1234.dao;
import java.sql.Connection;
public class GradeDao {
//注入风险的用法
public ResultSet gradeList(Connection con,PageBean pageBean,Grade grade)throws Exception{
StringBuffer sb=new StringBuffer("select * from t_grade");
if(grade!=null && StringUtil.isNotEmpty(grade.getGradeName())){
sb.append(" and gradeName like '%"+grade.getGradeName()+"%'");
}
if(pageBean!=null){
Console Tasks JavaScript Scripts Inspector
myeclipseTomcatServer [Remote Java Application] C:\Program Files\Java\jdk1.7.0_17\bin\javaw.exe (2019-5-3 下午11:29:10)
INFO: JK: ajp13 listening on /0.0.0.0:8009
五月 03, 2019 11:29:28 下午 org.apache.jk.server.JkMain start
INFO: Jk running ID=0 time=0/22 config=null
五月 03, 2019 11:29:28 下午 org.apache.catalina.startup.Catalina start
INFO: Server startup in 17181 ms

谢谢观赏