

java代码审计 深度解析



第二课 fortify全面介绍

免责声明 DISCLAIMER

本课程仅限于学习交流，请严格遵守国家法律法规！如利用技术从事违法活动，后果自负！



Fortify分析结果

The screenshot displays the Fortify Audit Workbench interface. The top menu bar includes File, Edit, Tools, Options, and Help. The main window is divided into several panes:

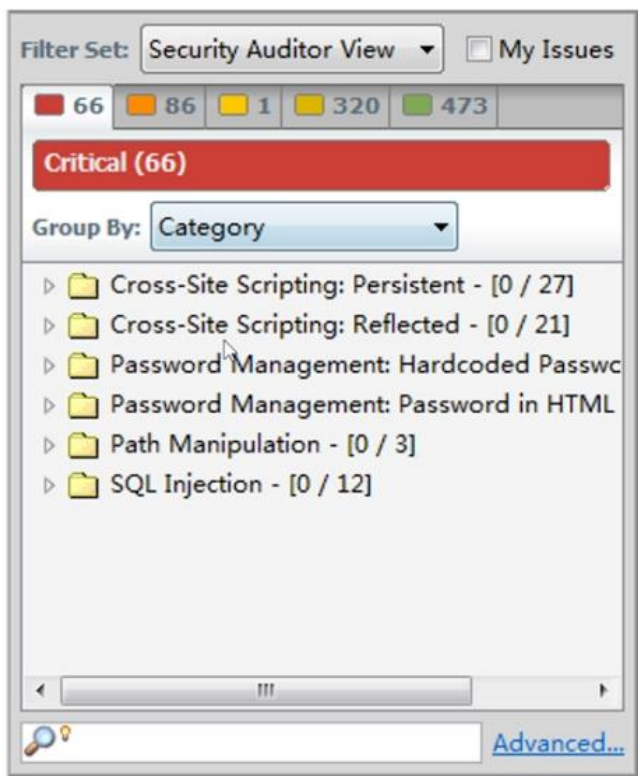
- Left Pane:** Filter Set: Security Auditor View. It shows a list of issues categorized by severity (Critical, High, Medium, Low) and a tree view of the project structure. The 'SQL Injection' category is expanded, showing a list of issues, including 'GoodsDao.java:86 (Shared Sink)'.
- Center Pane:** Project Summary. It displays the source code for 'GoodsDao.java'. The code is as follows:

```
77= public GoodsModel getGoods(String id)
78 {
79     GoodsModel model=null;
80     String sql_Str="select * from tb_goods where id="+id;
81     DBUtil db=new DBUtil(sql_Str);
82     try
83     {
84         Statement sm=db.getConnection().createStatement();
85
86         ResultSet rs=sm.executeQuery(sql_Str);
87         if(rs.next())
88         {
89             model=new GoodsModel();
90             model.setID(rs.getInt("id"));
91             model.setGoodsName(rs.getString("GoodsName"));
92             model.setGoodsTypeID(rs.getInt("GoodsTypeID"));
93             model.setDescription(rs.getString("GoodsDescription"));
94             model.setGoodsPrice(rs.getInt("GoodsPrice"));
95             model.setGoodsImage(rs.getString("GoodsImage"));
96             model.setRemainingCount(rs.getInt("RemainingCount"));
97         }
98     }
99     catch(SQLException ex)
100     {
101         ex.printStackTrace();
102     }
103 }
```
- Right Pane:** Functions. It shows a list of functions used in the code, including 'Top-level functions', 'com.eshop.dao', 'com.eshop.model', 'com.eshop.page', 'com.eshop.servlet', 'com.eshop.util', 'com.jspmartupload', 'java.awt', 'java.awt.image', 'java.io', 'java.lang', 'java.security', 'java.sql', 'java.util', 'java.util.regex', 'javax.imageio', 'javax.servlet', 'javax.servlet.http', and 'javax.servlet.jsp'.
- Bottom Pane:** Analysis Evidence. It shows a list of issues, including 'GoodsDetail.jsp:6 - getParameter(return)', 'GoodsDetail.jsp:6 - Assignment to goodsid', 'GoodsDetail.jsp:8 - getGoods(0)', 'GoodsDao.java:80 - Assignment to sql_Str', and 'GoodsDao.java:86 - executeQuery(0)'. The 'GoodsDao.java:86 - executeQuery(0)' issue is highlighted.

The bottom pane also displays a call graph for the 'GoodsDao.getGoods' method, showing the flow of data and the execution of the 'executeQuery(0)' method.



问题面板



过滤器组

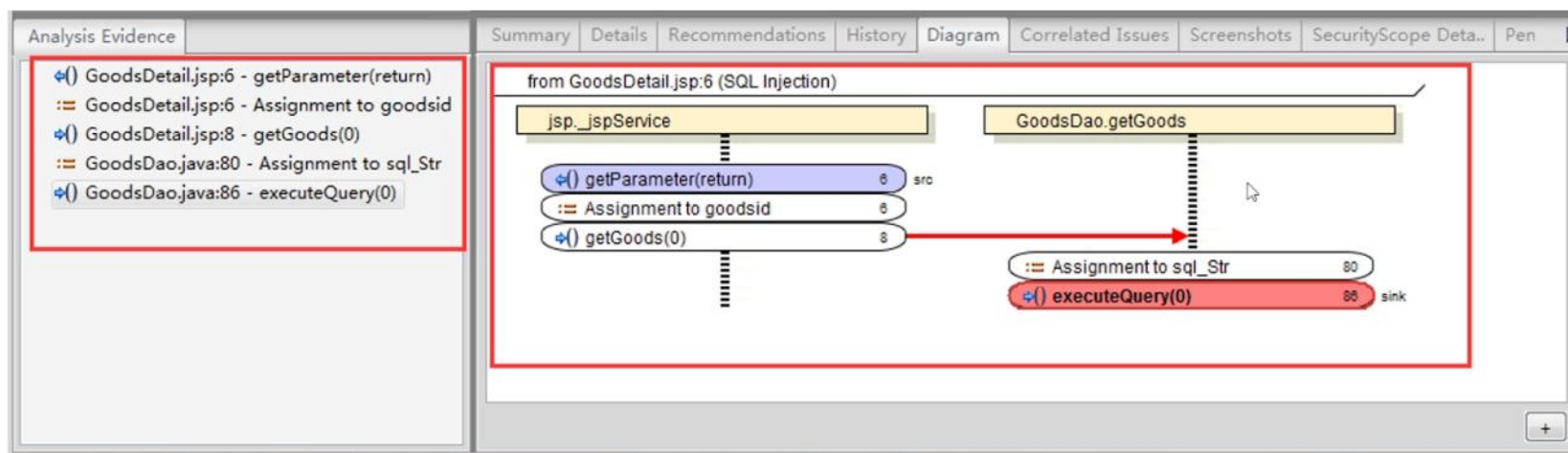
分类选项卡

问题列表



赛博梦工厂
Cyber Works

问题面板-数据流图



HPE Security Fortify Audit Workbench

Start New Project

[Scan Java Project...](#)[Advanced Scan...](#)

Open Project



Recent Projects:

shenjisaomiaojieguo	0 % Audi...	Jan 22, 2...
daimashenjiyuanma	0 % Audi...	Jan 10, 2...
11	0 % Audi...	Nov 15, ...
EShop	0 % Audi...	Aug 8, 2...

[Open Project...](#)

Open Collaborative Audit



Collaborative Applications:

Sign in to list collabo...

[Sign In...](#)

赛博梦工厂
Cyber Works

C:\Users\gy\AppData\Local\Fortify\AWB-16.20\daimashenjiyuanma\daimashenjiyuanma.fpr

File Edit Tools Options Help

Summary | Audit Guide | Scan | Reports

AUDIT WORKBENCH **FORTIFY**

Filter Set: Quick View ☐ My Issues

131 103 0 0 ... 234

Critical (131)

Group By: Category

- > Cross-Site Scripting: DOM - [0 / 6]
- > Cross-Site Scripting: Persistent - [0 / 3]
- > Cross-Site Scripting: Reflected - [0 / 11]
- > Dynamic Code Evaluation: Code Injection - [0 / 6]
- > Open Redirect - [0 / 8]
- > SQL Injection - [0 / 11]
- > SQL Injection: Hibernate - [0 / 86]

Advanced...

Analysis Evidence

Project Summary

Summary Certification Runtime Analysis Build Information Analysis Information

Build ID: daimashenjiyuanma Scanned: 779 files, 55,202 LOC (Executable)

Scan Date: Jan 9, 2016 Total Issues: 234

Warnings: 2 occurred during scan Certification: Results Certification Valid

All Issues by Folder

High (103)

Critical (131)

Summary Details Recommendations History Diagram Screenshots Filters Warnings

Issue:

User:

Analy...

Edit...

Click to append comment (Ctrl+Enter to save)

More Information... Recommendations...

Functions

Show: All

Group by: package Legend...

Include API: ☒ External ☒ Internal ☐ Superclasses

- > Top-level functions
- > /
- > /jsp/authority
- > /jsp/code
- > /jsp/common
- > /jsp/login
- > /jsp/property
- > /jsp/repair
- > /jsp/transfer
- > /jsp/warehouse
- > /struts-dojo-tags
- > /struts-tags
- > com.google.gson
- > com.logs.actions.authority
- > com.logs.actions.code
- > com.logs.actions.common
- > com.logs.actions.log
- > com.logs.actions.property
- > com.logs.actions.repair
- > com.logs.actions.transfer
- > com.logs.actions.warehouse
- > com.logs.dao.authority
- > com.logs.dao.code
- > com.logs.dao.common
- > com.logs.dao.impl.repair
- > com.logs.dao.impl.authority
- > com.logs.dao.impl.code

Search:

Scanning



赛博梦工厂
Cyber Works



谢谢观赏