Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

解题思路：

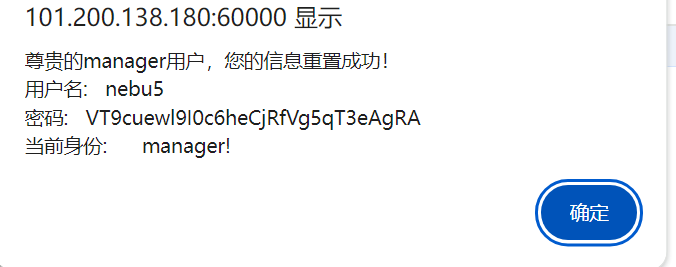
首先尝试admin弱密码，然后发现根本没有弱密码，那就随便注册一个账号进去看看。

在注册的时候发现job被锁住了，这里可以猜测job就是区分admin和普通用户的标识，那我们就可以抓包试着传个job：



然后尝试登陆：

发现还是不行，那就试着重置一下



接着登录：

Nebu5

VT9cuewl9I0c6heCjRfVg5qT3eAgRA

进入后台页面

接着一个一个试，发现<http://101.200.138.180:60000/gongzi_iscc.php>有漏洞，输入ls与00，发现输出/C，而/C正好就是ls和00的异或，那么试着输入/C和00试试，发现：



接着读根目录发现没有flag



那只能看看dockerfile



现在没啥提示，只能盲猜flag在sercert.host/flag下，那就试试：

Payload:curl <http://secret.host/flag>即可得到flag