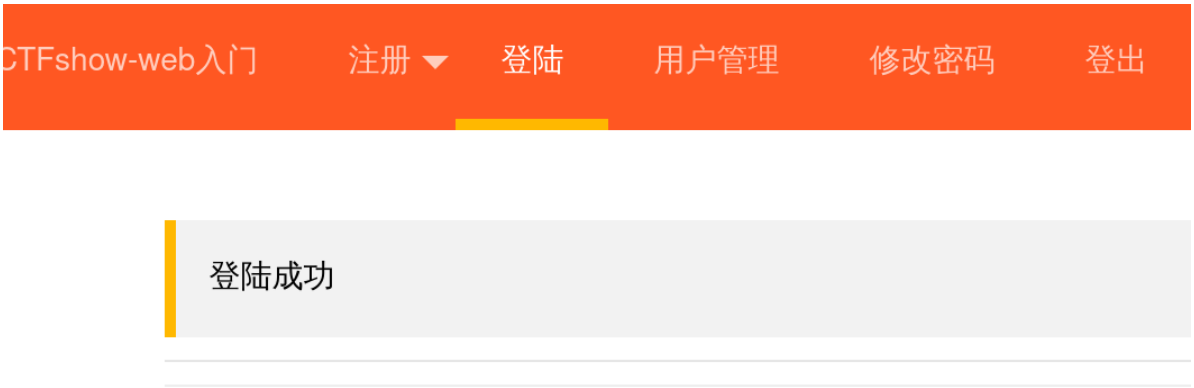
1.这次多了个改密码的功能，注册登录后试了一下改密码，发现是直接改的没有要求输入旧密码，这题用到的方法像是csrf，有点像钓鱼，在修改密码确定后抓包，可以看到是在/api/change.php文件改的，get传参p

2.构造payload

```
<script>window.location.href='http://127.0.0.1/api/change.php?p=1717';</script>
```

3.将用户名和密码都设置为payload，当管理员看到我们注册的这个账户时，浏览器会将我们的payload渲染在页面上，没有过滤会被当作指令执行，带上当前浏览器的cookie（也就是管理员的cookie）访问本地改密码的文件加上传参直接改成了我们想要的密码

改成我们想要的密码后，直接登录，用户名：admin，密码：1717



4.然后查看用户管理，根据payload，管理员查看用户管理时会跳转到那个页面改密码，那我们也是一样的，这会导致我们还没有复制flag，就跳转过去了，可以用bp抓包解决这个问题，得到flag

> 欢迎你，admin ctfshow{7ac1138a-8fcc-4f3b-84ef-9d7aacf6fde3}