

一. 页面:

1. 传统用户名密码页面
2. 扫码登录页面
3. 手机邮箱验证码登录页面
4. 与其他登录页面 UI 或交互相关的操作的验证 统一身份认证

二. 测试:

1. 输入正确用户名密码
2. 错误密码
3. 不存在用户名
3. 输入 SQL 注入等攻击语句
4. 输入为空及长度恶意输入
5. 验证码超时持续输入
6. 输入错误验证码
7. 输入正确验证码
8. 验证码恶意攻击输入
9. 错误邮箱格式 错误手机号格式
10. 安全性: 不同的 ip 地址登录同一个账号; 密码连续错误之后锁定账号
11. 防止直接改网址跳转, 进行 url 保护
12. 手机的话密码设置不可能是汉字自己主动切换到英文输入法
13. 登录的响应时间小于一定数值
14. 登录的响应时间小于一定数值

15. 退出登录是否跳转到登录页面，退出登录后访问是否仍然有访问数据的权限
16. 在已有用户极多的情况下进行各项测试，各种操作时间是否能很快完成
17. 按钮是否可以正常使用；
18. 系统提示信息友好；
19. 登录成功进入页面后功能是否完整；
20. 验证码可辨识度是否高