20200720信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/7/20 20:39	**更新时间:**	2020/7/20 20:45
作者:	820410740@qq.com		
URL:	https://blog.csdn.net/qq_37077262/article/details/103013368		

爆破靶场
无防护机制
爆破方式：直接burpsuite抓包，放入爆破模块设置字典进行爆破。
验证码（on server）
爆破方式：
burp抓包，更换账号发送几次，看返回信息，如果没有“验证码错误”，说明验证码长期有效，可直接爆破
验证码（on client）
爆破方式：验证码有前端生成验证，可利用burp抓包直接绕过。进行爆破。
判断验证码在服务端还是客户端：
可利用burp抓包，删除验证码传参，发送数据包。看返回信息，如果没有“验证码错误”，则在客户端。
token爆破
爆破步骤如下：
https://blog.csdn.net/qq_37077262/article/details/103013368
Token 是在服务端产生的。如果前端使用用户名/密码向服务端请求认证，服务端认证成功，那么在服务端会返回 Token 给前端。前端可以在每次请求的时候带上 Token 证明自己的合法地位。如果这个 Token 在服务端持久化（比如存入数据库），那它就是一个永久的身份令牌。