密码暴力破解与防御

裤子 – 网络上已经泄露的数据，如rockyou.txt

网络存在漏洞导致客户表数据库被黑客倒出

暴力密码破解工具：Python, Burp Suite, Kali: wfuzz, Hydra, medusa, msfconsole

密码作用：

1. 加密
2. 完整性 – HASH checking for integrity
3. 身份认证

权限管理：

1. 认证：你是谁
2. 授权：你能做什么

漏洞利用：

1. 从数据库获得密码，解密 – 利用SQL injection, etc
2. 窃听通信数据，解密 – 抓包，窃听数据
3. 从登入框猜测密码

密码破解

1. 连续试
2. 字典
3. 自动

如何暴力破解：

1. 字典 Wordlists/Dictionary (通用的)

* Kali自带的 /usr/share/wordlists
* 网络下载 (如：GitHub, Google)

1. 专用字典

* crunch -h （指定格式字典, kali自带）
* cupp , ccupp (社工字典)
* cewl <https://sqlmap.org> -w dict.txt (文章内容字典)

1. Python爆破

* 从字典取读

1. Burp Suite 密码爆破

* Intruder

1. Sniper
2. Battery Ram (Username value = Password Value)
3. Pitchfork – 1 to 1
4. Cluster Bomb – one to many

暴力破解防御

1. Sleep
2. Token
3. 限制尝试次数，锁定账户
4. 二次验证 Two-factor Authentication
5. 行为识别 – not recognise device, different country login
6. WAF
7. reCAPTCHA (IP 验证)
8. 强制修改密码
9. 取消密码登入 – 如：利用微信，手机号码登入

个人用户安全建议：

1. 使用复杂密码 – 大小写，特别符号，字数长度8以上
2. 不同网站不同密码
3. 定期修改密码
4. 防止被钓鱼