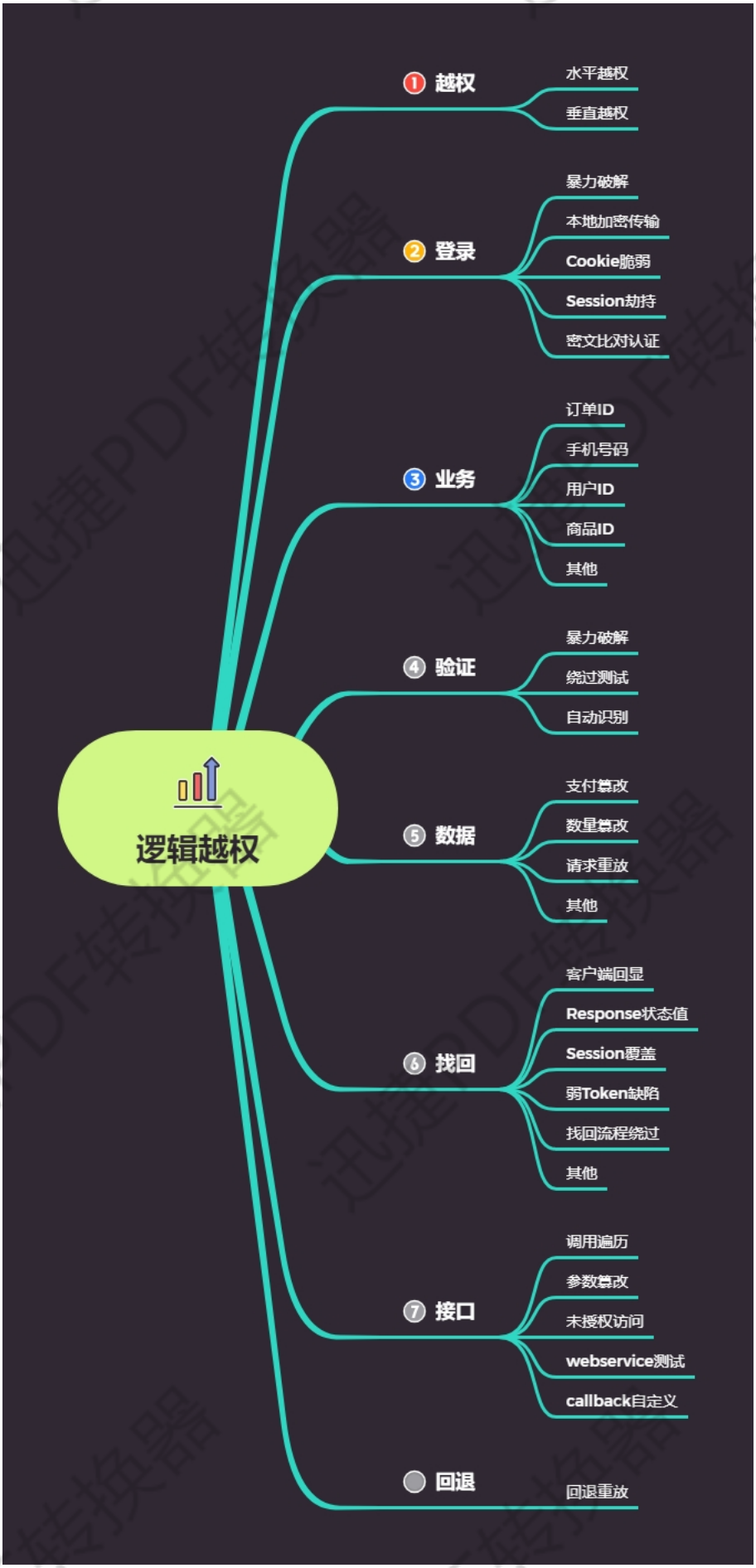
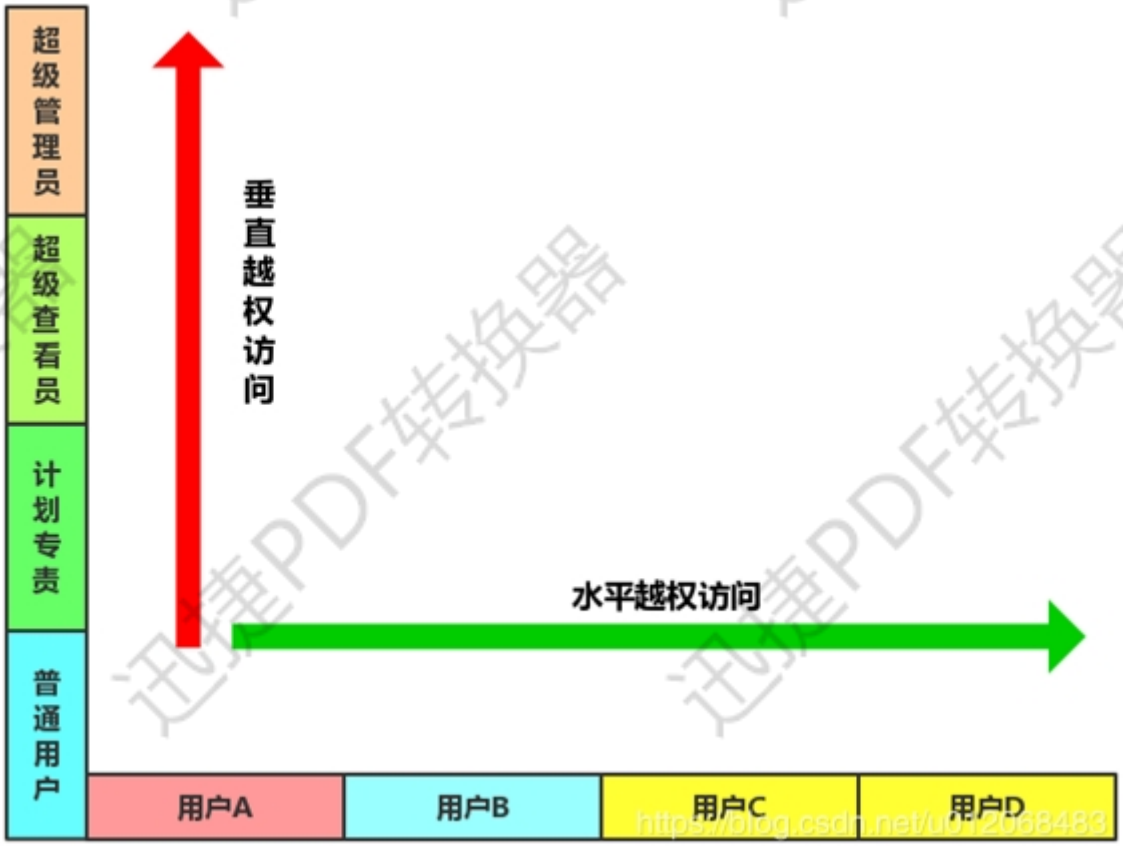
# WEB 漏洞-逻辑越权之水平垂直越权全解


逻辑越权
1 越权
水平越权
垂直越权
2 登录
暴力破解
本地加密传输
Cookie脆弱
Session劫持
密文比对认证
3 业务
订单ID
手机号码
用户ID
商品ID
其他
4 验证
暴力破解
绕过测试
自动识别
5 数据
支付篡改
数量篡改
请求重放
其他
6 找回
客户端回显
Response状态值
Session覆盖
弱Token缺陷
找回流程绕过
其他
7 接口
调用遍历
参数篡改
未授权访问
webservice测试
callback自定义
回退
回退重放

#水平，垂直越权，未授权访问
解释，原理，检测，利用，防御等
通过更换的某个 ID 之类的身份标识，从而使 A 账号获取（修改、删除等）B 账号数据。
使用低权限身份的账号，发送高权限账号才能有的请求，获得其高权限的操作。
通过删除请求中的认证信息后重放该请求，依旧可以访问或者完成操作。

原理：
前端安全造成：界面
判断用户等级后，代码界面部分进行可选显示
后盾安全造成：数据库
user 表(管理员和普通用户同表)
id,username,password,usertype
1,admin,123456,1
2,xiaodi,11111,2
登录用户 admin 或 xiaodi 时，代码是如何验证这个级别？（usertype 判断）
如果在访问数据包中有传输用户的编号、用户组编号或类型编号的时候，那么尝试对这个值进行修改，就是测试越权漏洞的基本。

#修复防御方案
1.前后端同时对用户输入信息进行校验，双重验证机制
2.调用功能前验证用户是否有权限调用相关功能
3.执行关键操作前必须验证用户身份，验证用户是否具备操作数据的权限
4.直接对象引用的加密资源 ID，防止攻击者枚举 ID，敏感数据特殊化处理
5.永远不要相信来自用户的输入，对于可控参数进行严格的检查与过滤




---

演示案例：

- Pikachu-本地水平垂直越权演示（漏洞成因）
- 墨者水平-身份认证失效漏洞实战（漏洞成因）
- 越权检测-小米范越权漏洞检测工具（工具使用）
- 越权检测-Burpsuite 插件 Authz 安装测试（插件使用）

---

涉及资源：

https://github.com/ztosec/secscan-authcheck

http://pan.baidu.com/s/1pLjaQKF (privilegechecker)

https://www.mozhe.cn/bug/detail/eUM3SktudHdrUVh6eFloU0VERzB4Zz09bW96aGUmozhe