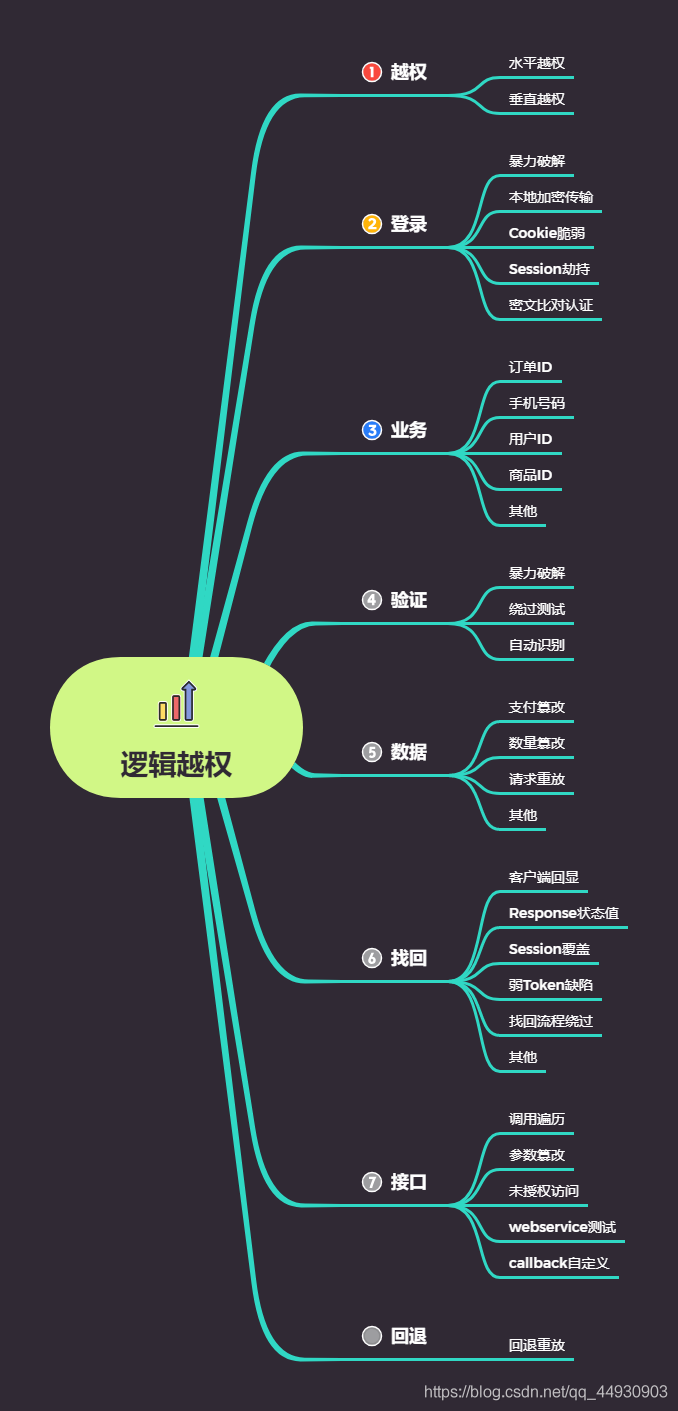
# 33 WEB漏洞-逻辑越权之水平垂直越权全解



#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。

垂直越权：添加用户

前提条件：获取的添加用户的数据包 怎么来的数据包

1.普通用户前端有操作界面可以抓取数据包

2.通过网站源码本地搭建自己去模拟抓取

3.盲猜

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,liuyifei,11111,2

登录用户admin或liuyifei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

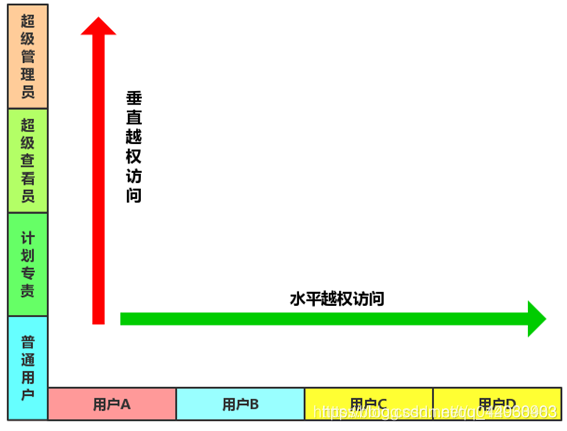
1.前后端同时对用户输入信息进行校验，双重验证机制

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