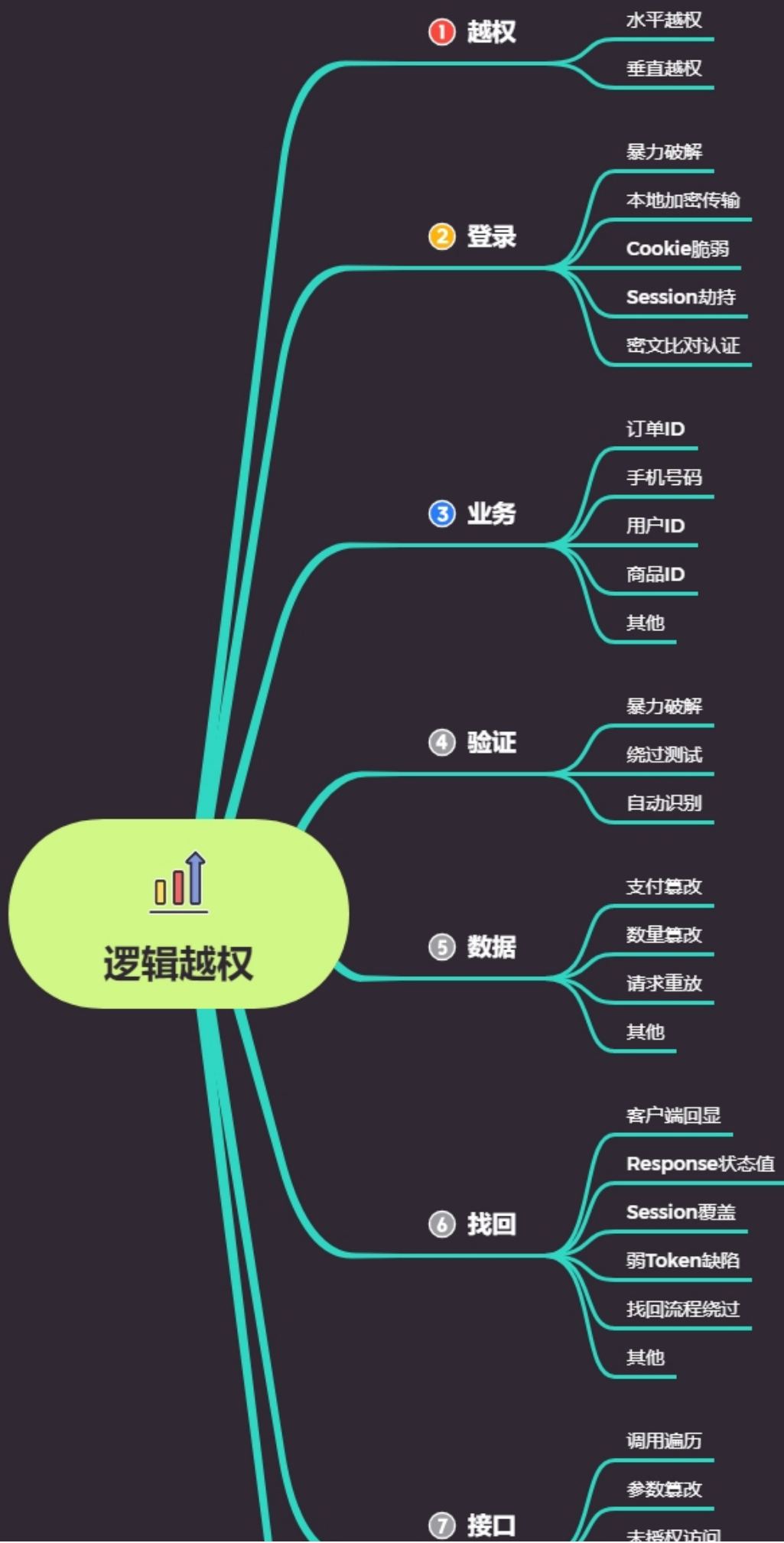
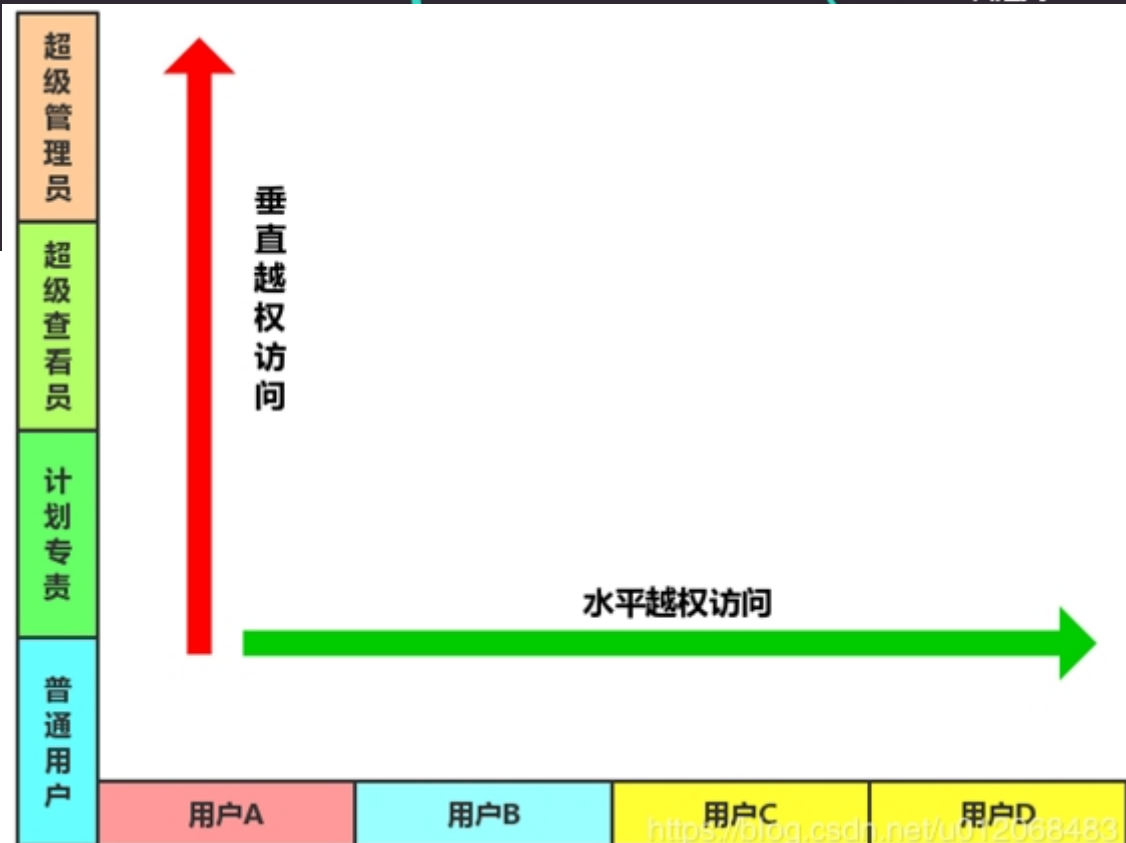


Day33 WEB漏洞-逻辑越权 之水平垂直越权全解



越权分为：水平越权和垂直越权（作用更大），未授权访问



- 1 水平越权：通过更换某个ID之类的身份标识，从而使A账号获取修改B账号数据；
- 2 垂直越权：使用低权限身份的账号，发送高权限账号才能有的请求，获取其更高权限的操作；
- 3 未授权访问：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

33.1 越权原理

1.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

2.后端安全造成：数据库

user 表(管理员和普通用户同表)：

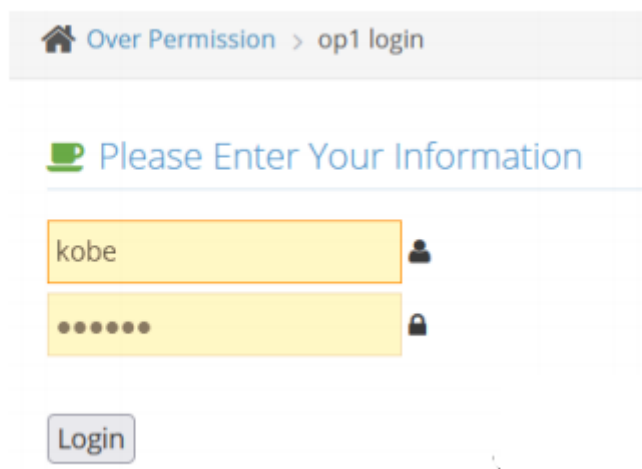
id	username	password	usertype
1	admin	123456	1
2	xiaodi	11111	2

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。

33.2 水平越权

pikachu靶场中逻辑水平越权登录kobe相关信息，登录，查看个人信息时对其进行抓包：



查看个人信息时对其进行抓包，可以得到：

```
GET /pikachu-master/vul/overpermission/op1/op1_mem.php?username=kobe&submit=%E7%82%B9%E5%87%BB%E6%9F%A5%E7%9C%68%E4%B6%AA%E4%BA%BA%E4%BF%A1%E6%81 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/pikachu-master/vul/overpermission/op1/op1_mem.php
Cookie: PHPSESSID=2ba250640bd8d32b06892231e073ae8
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

将username更改为lucy，便可得到lucy的相关信息：

hello,lucy,你的具体信息如下:

姓名:lucy

性别:girl

手机:12345678922

住址:usa

邮箱:lucy@pikachu.com

33.3 垂直越权

pikachu:

在登录admin(较高一级的管理员)的情况下, 对其操作进行抓包, 在登录pikachu (低一级用户) 时, 就可以将较高一级的包调出来, 更改cookie:PHPSESSID=的值, 可以条件: 需要有admin的数据包更改相关的user值, 便可以对其进行添加.

墨者:

抓两个数据包, 看到有个包的card_id的值, 我们考虑用burp suite的thunder功能对其进行爆破, 排序相关的length对较大的值进行查看, 或者查看图片源地址, 可以看到马春生的相关caid_id账号, 在该数据包中查看账号和密码 (可能需要解密), 登录, 得到其flag;



- 1 条件: 可以抓到admin的数据包
- 2
- 3 获取admin数据包方法:
- 4 1、普通用户前端有操作界面可以抓取数据包
- 5 2、盲猜
- 6 3、通过网站源码本地搭建自己去获取

33.4 修复方案



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

33.5 越权检测

小米范越权漏洞检测工具、burpsuite的anthz插件

资源：



- 1 <https://github.com/ztosec/secscan-authcheck>
- 2 <http://pan.baidu.com/s/1pLjaQKF>
(privilegechecker)
- 3 <https://www.mozhe.cn/bug/detail/eUM3SktudHdrUVh6eF1oU0VERzB4Zz09bw96aGUmozhe>