如何做好认证与会话管理

01 定义&原理

02 做好认证与会话管理

扫码试看/订阅

《Web 安全攻防实战》视频课程

01 定义&原理

定义&原理

认证

一个验证凭证的过程，载体如账号密码，cookie（session）、token，数字证书，手机验证码。一般分为登录过程的认证与保持登录的认证。

定义&原理

会话管理

HTTP 协议是无状态无连接的协议，服务端对于客户端每次发送的请求都认为它是一个新的请求，上一次会话和下一次会话没有联系。

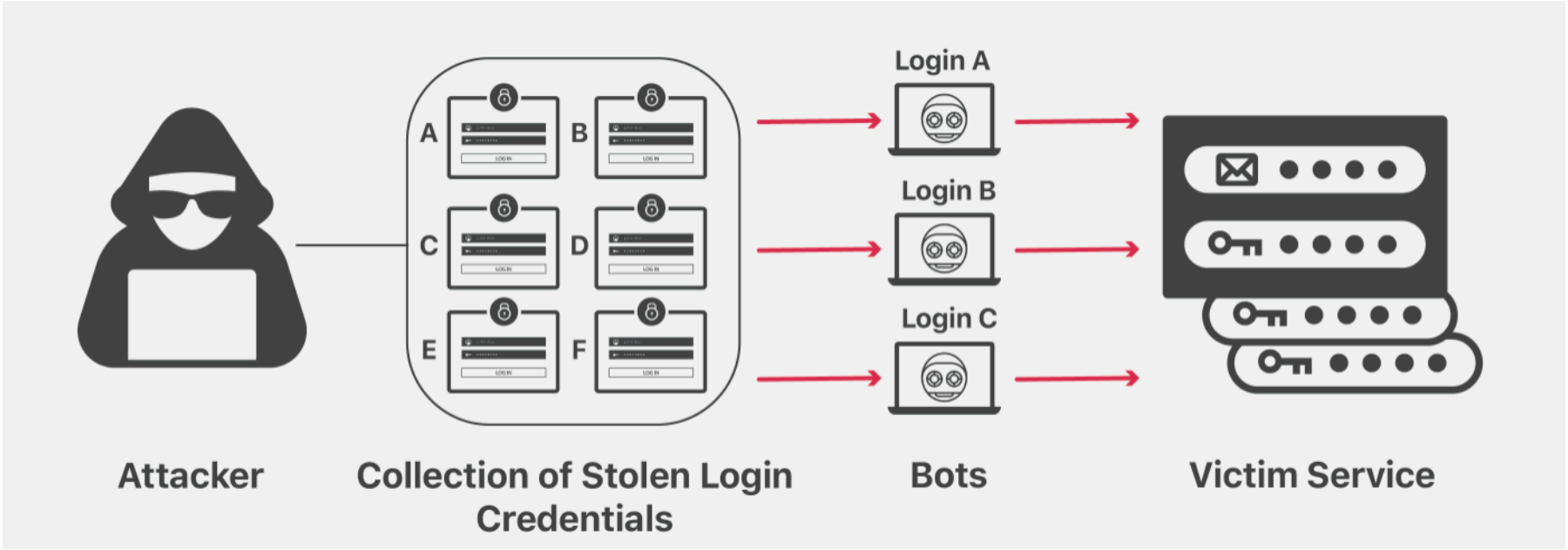
即在切换页面保持登录状态的认证过程即是会话管理，对用户透明。

02 做好认证与会话管理

单因素认证与&密码强度

- 长期以来，网站的建设者认为持有正确密码的用户是可信的，需要防御的仅是弱口令的问题

凭据填充攻击



凭证填充是自动注入用户/密码对以欺骗性地获取用户权限、这是暴力攻击的一个子集，大量溢出的凭据会自动输入网站，直到它们与现有帐户相匹配。

一家公司受到凭证填充攻击，不一定表示它自身的安全已受损（或密码强度不足），通常关联为另一个网站沦陷。

多因素认证&便捷性考量

登录密码	安全性高的密码可以使帐号更安全。建议您定期更换密码，设置一个包含字母，符号或数字中至少两项且长度超过6位的密码。	已设置 | 修改
手机绑定	您已绑定了手机181****7323 [您的手机为安全手机，可以找回密码，但不能用于登录]	已设置 | 修改
备用邮箱	备用邮箱绑定后可用来接收阿里云发送的各类系统、营销、服务通知。	未设置 | 设置
密保问题	建议您设置三个容易记住，且最不容易被他人获取的问题及答案，更有效保障您的密码安全。	未设置 | 设置
虚拟MFA	绑定虚拟MFA后，您可以在登录时通过它来进行二次校验。	未设置 | 设置
操作保护	在控制台关键操作（如：释放、修改密码等）时，通过设置保护强度和验证方式再次确认您的身份，进一步提高账号安全性，有效保护您安全使用云产品。	未设置 | 设置
登录掩码	网络掩码决定哪些IP地址会受到登录控制台的影响，包括密码登录和SSO登录。如果指定掩码，账号必须只能从指定的IP地址进行登录。如果不指定任何掩码，登录控制台功能将适用于整个网络。当需要配置多个掩码时，请使用分号来分隔掩码，例如：42.120.66.0/24;42.120.74.98	未设置 | 设置

多因素认证的安全性当然有提高，但便捷性下降，需综合考虑安全性与便捷性。

如：支付转账与订单查询

非登录过程的认证

基于 session 的认证

基于 token 的认证

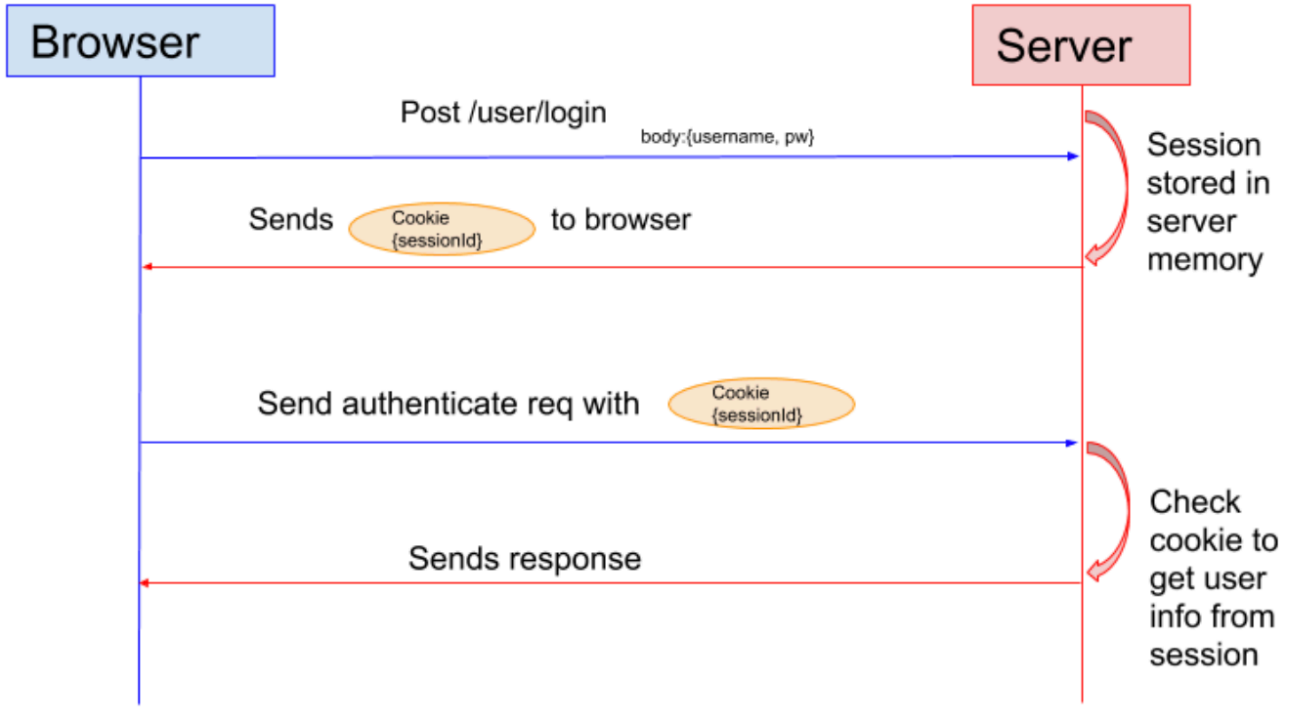
基于 session 的认证

sesionid 过期时间：

设置强制过期时间（会话保持攻击）

sesionid 位置：

- URL
- 隐藏域
- cookie（相对安全）



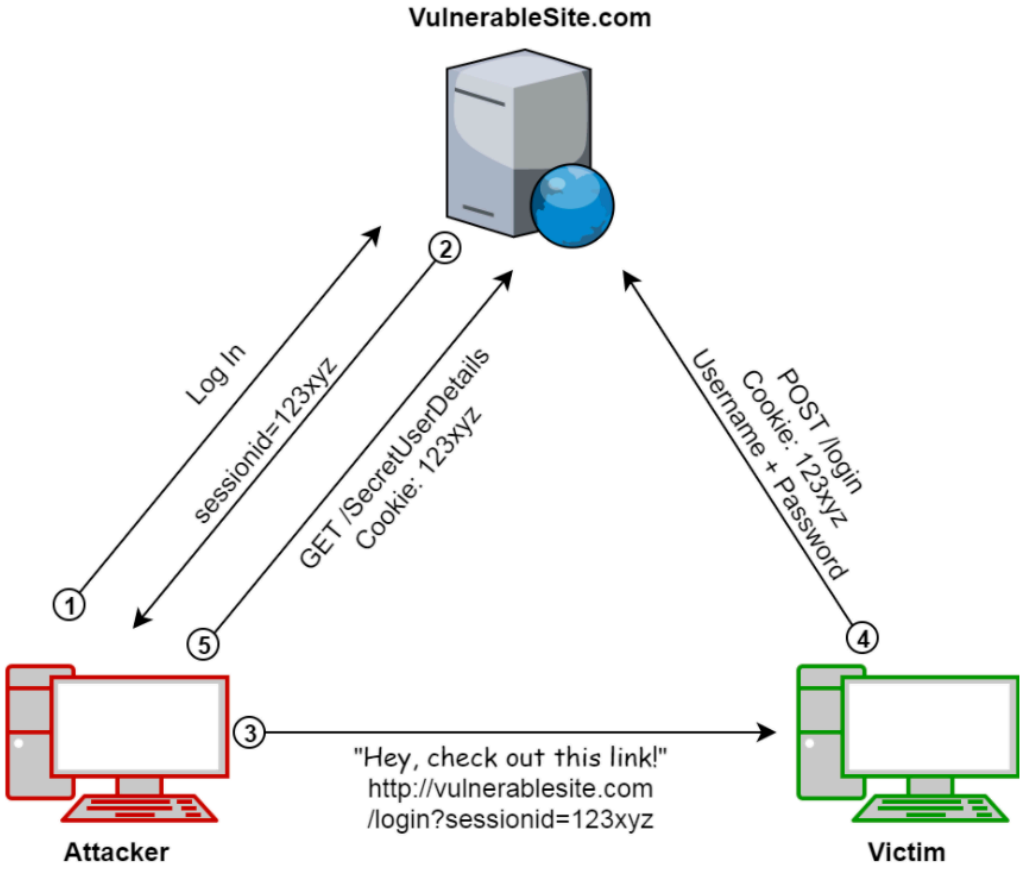
Session Based Authentication flow

session fixation（会话固定攻击）

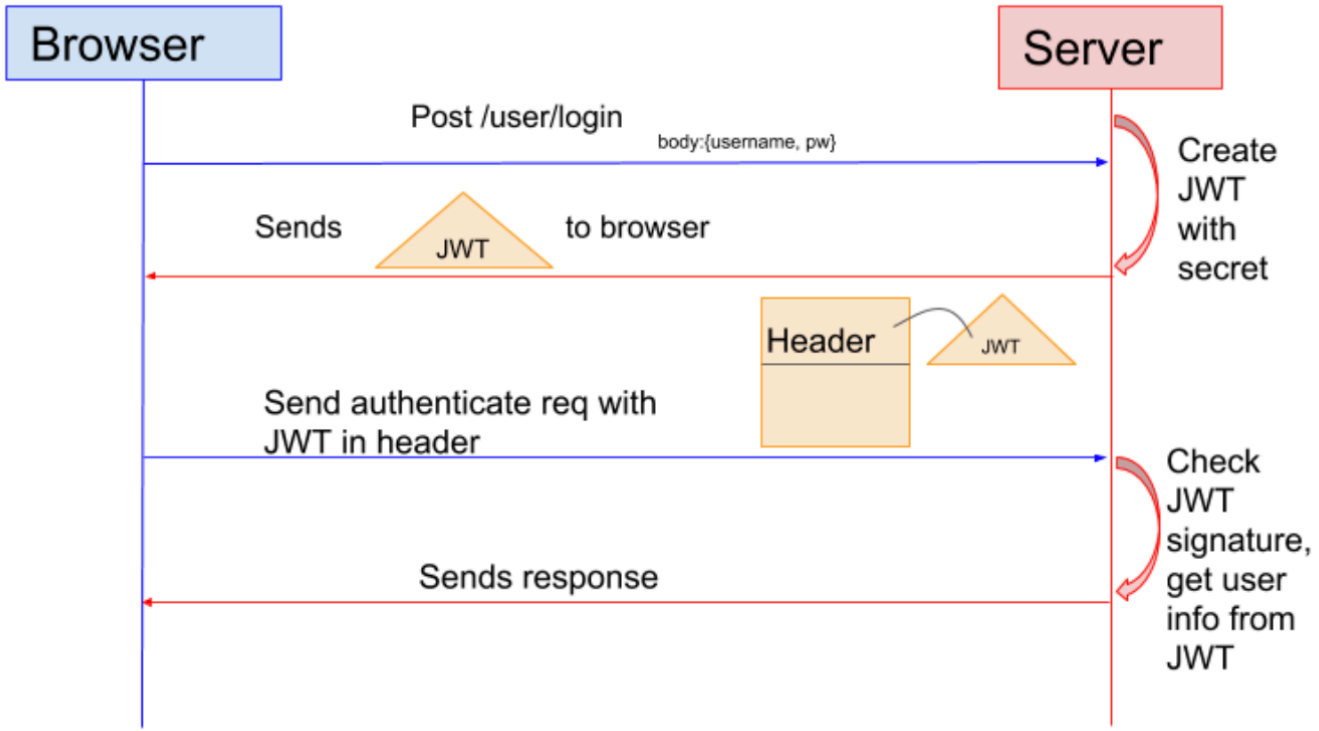
- 使用 URL 传递 sessionID
- 登录前后 sessionID 不变化

```
15    http://www.target.com/login.html?sid=3cdf7d
```

登录完毕，更改 sessionID



基于 token 的认证



Token Based Authentication flow

JWT(json web token)

1 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.2 eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.3 XbPfbIHMI6arZ3Y922BhjWgQzWXcXNrz0ogtVhfEd2o

1 Header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

2 Payload

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

3 Signature

```
HMACSHA256(
BASE64URL(header)
.
BASE64URL(payload),
secret)
```

未校验签名

"alg":"none" + name:"admin"

密钥爆破（pyjwt库）

单点登录

用户只需要登录一次就可以访问所有相互信任的应用系统。把认证的流程统一起来，风险集中化。

访问控制：水平权限&垂直权限

01

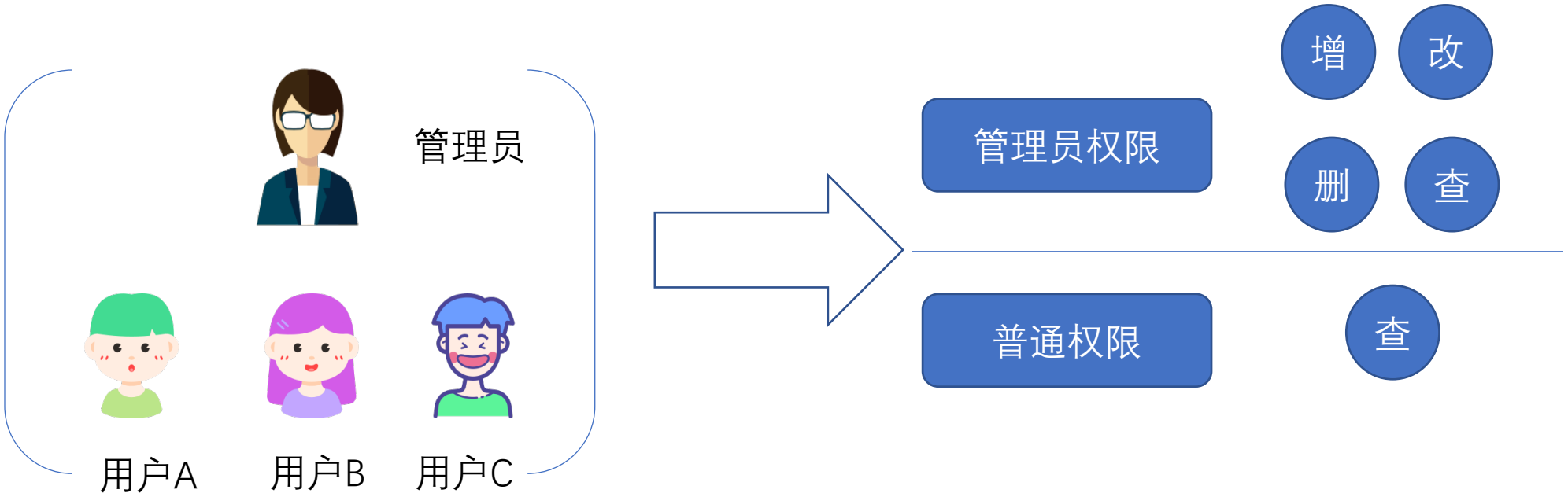
定义&原理

01 定义&原理

定义&原理

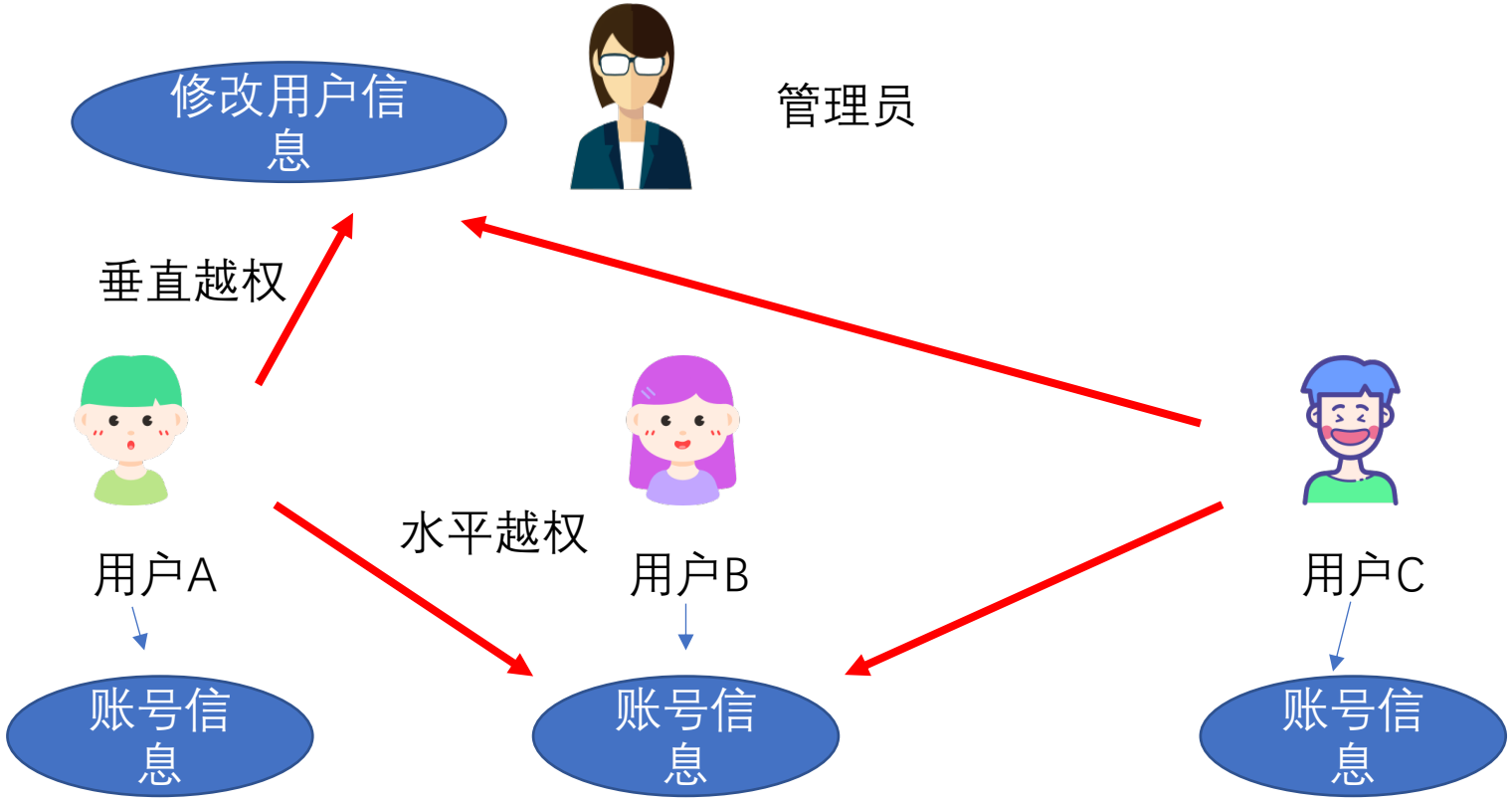
访问控制

系统对于用户执行某种操作的限制称为访问控制。



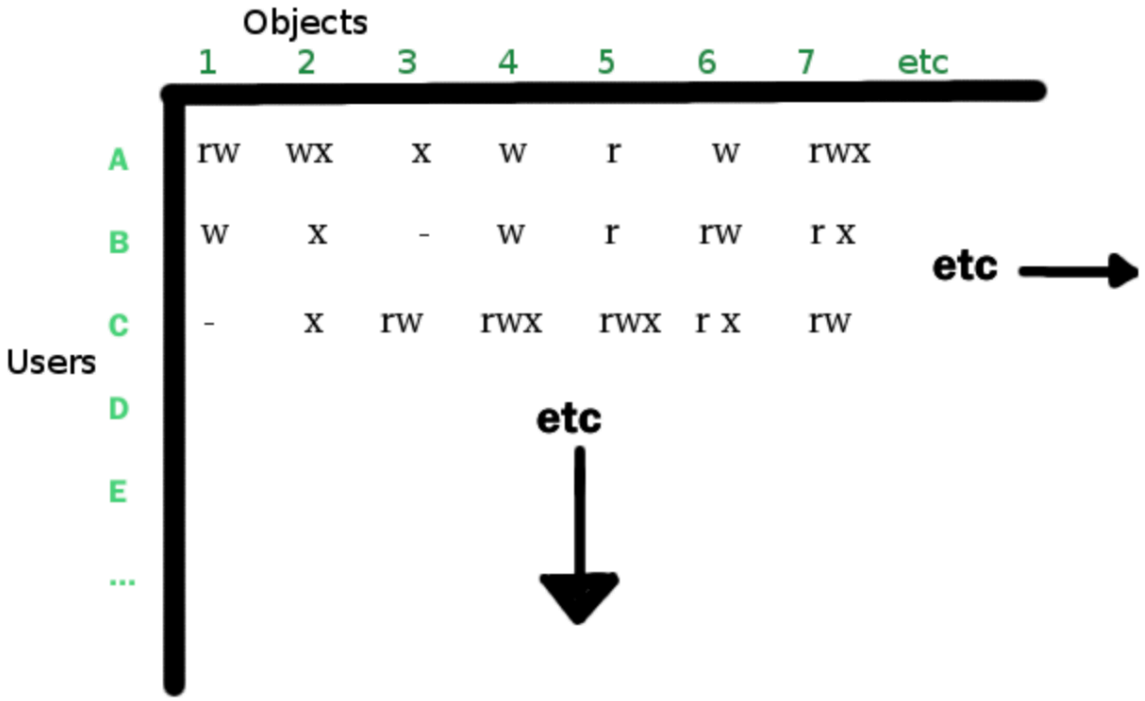
定义&原理

水平越权&垂直越权



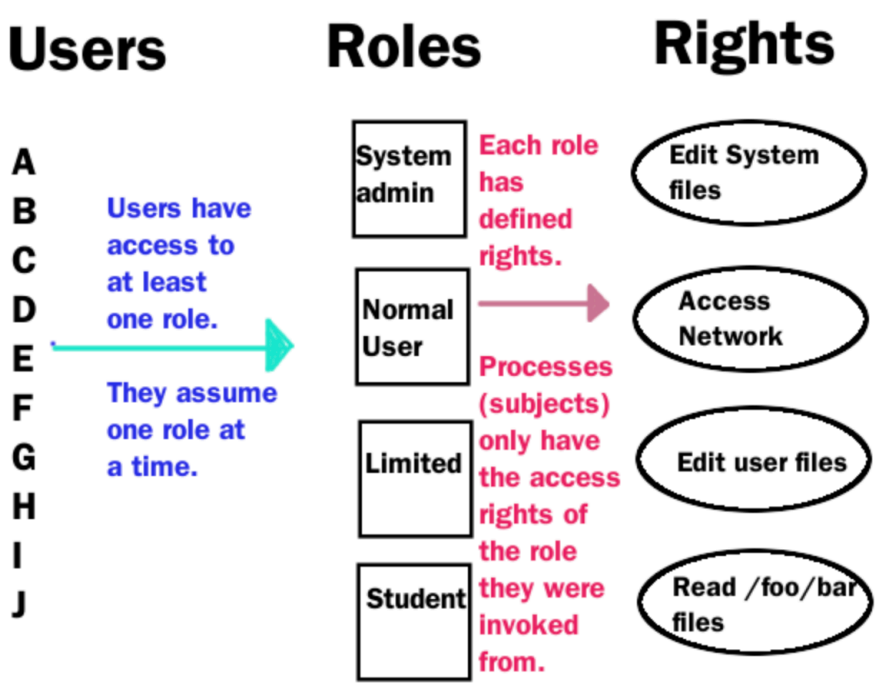
定义&原理

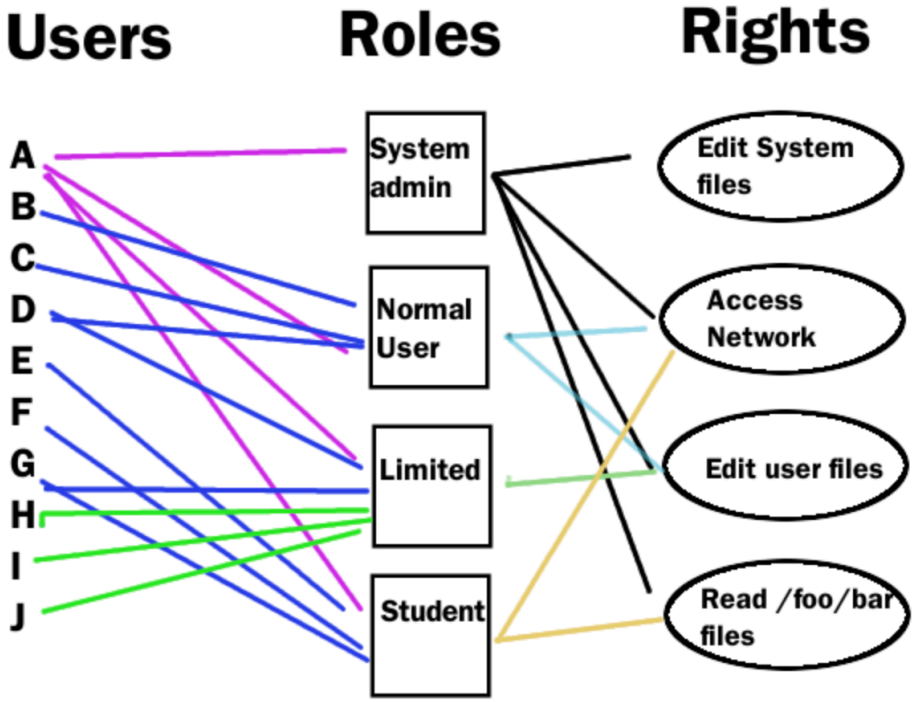
垂直权限&基于控制矩阵（有限制）



定义&原理

垂直权限&基于角色的权限控制

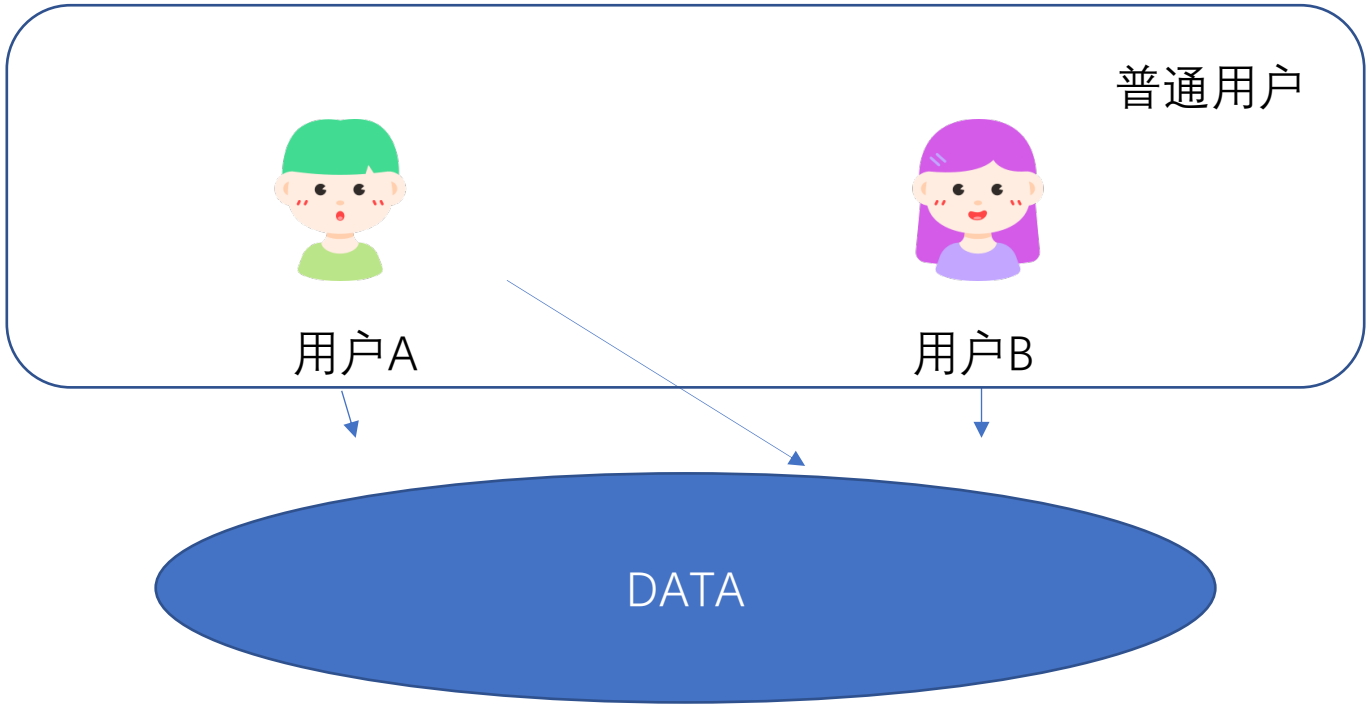




最小权限原则

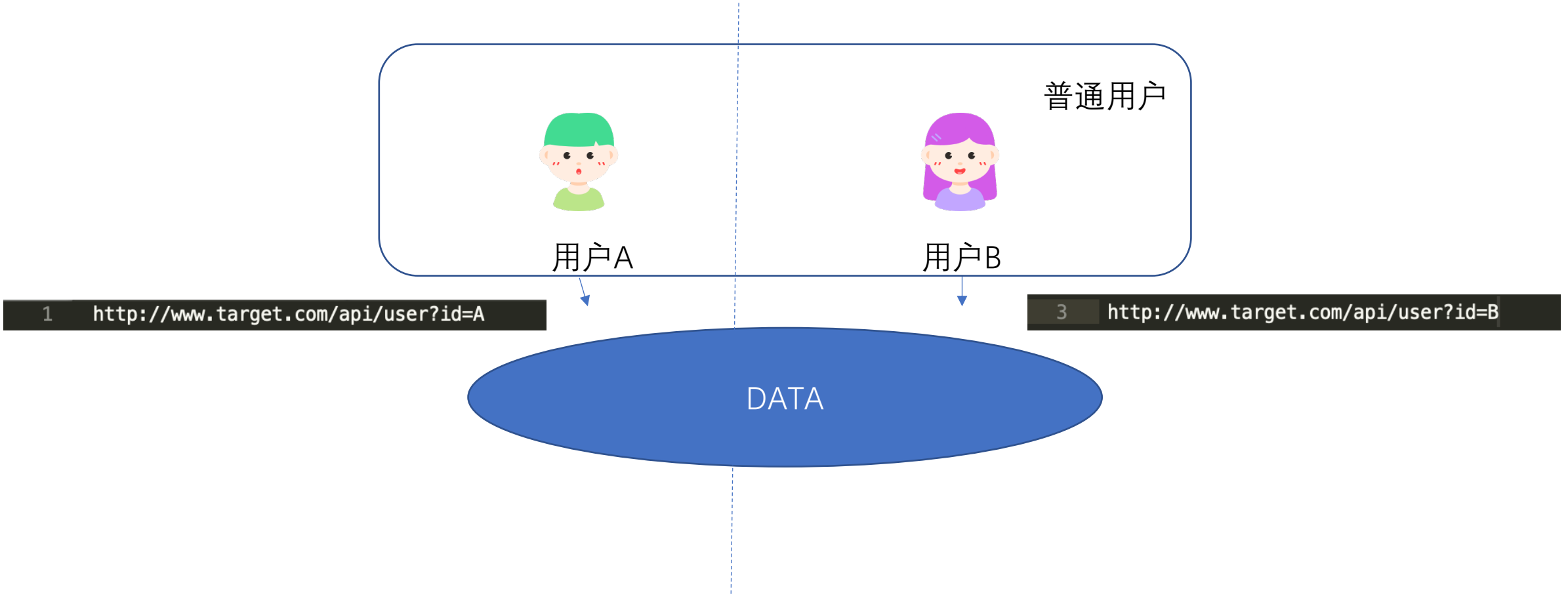
定义&原理

水平权限&同角色互访问题



定义&原理

水平权限&权限控制



定义&原理

水平权限&越权点

下面两张分别可能存在什么问题？

```
POST /password_change.php HTTP/1.1
Host: www.target.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 66
Origin: http://www.target.com
Connection: close
Referer: http://www.target.com/password_change.php
Cookie: wp-settings-time-1=1600832530; PHPSESSID=v1k0k29n8e30a8lb006prs65l4;
Upgrade-Insecure-Requests: 1

uname=Lihua&password_new=stsd@1&password_conf=stsd@1&action=change
```

```
3  http://www.target.com/api/user?id=19731&action=del
```

扫码试看/订阅

《Web 安全攻防实战》视频课程