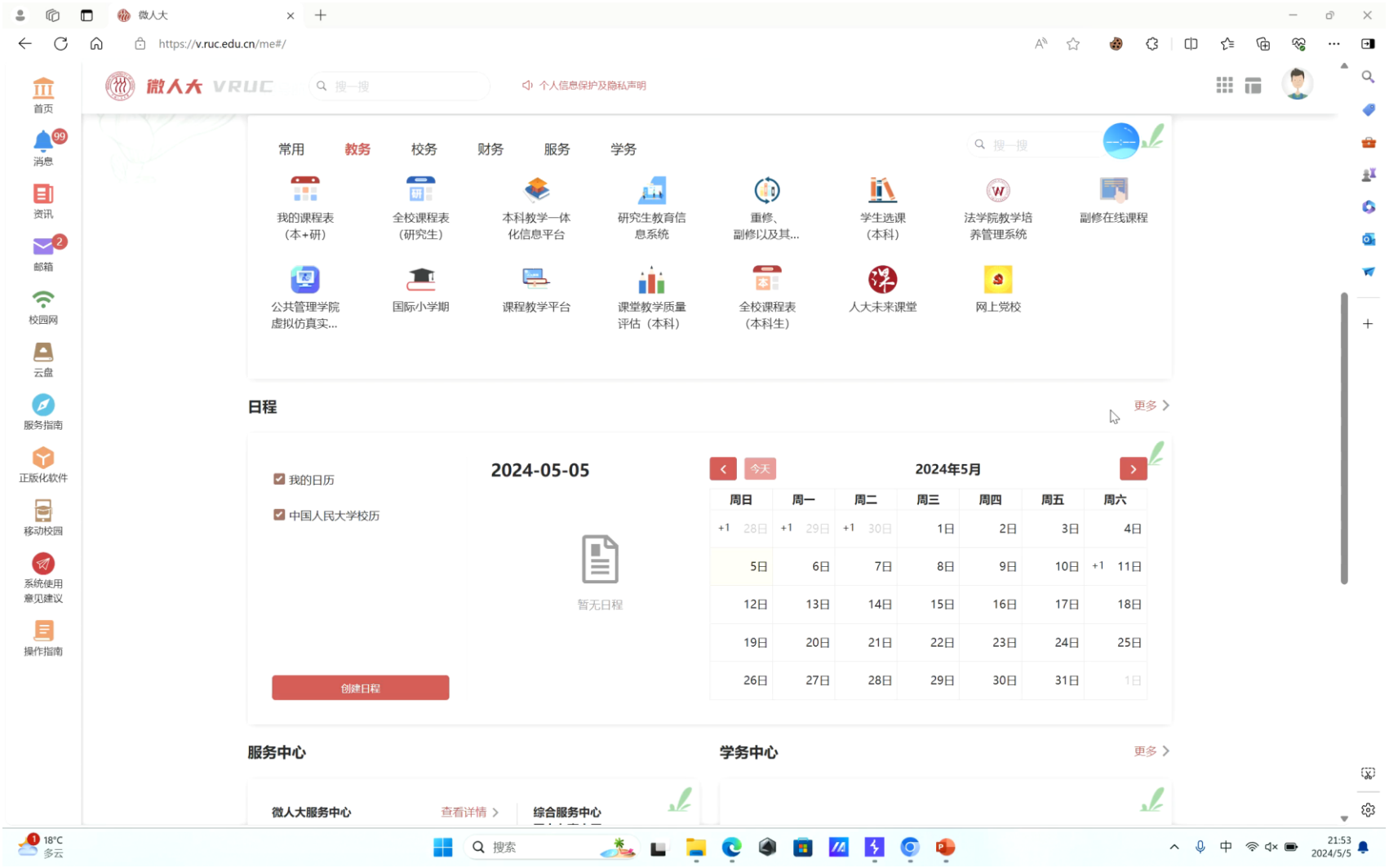
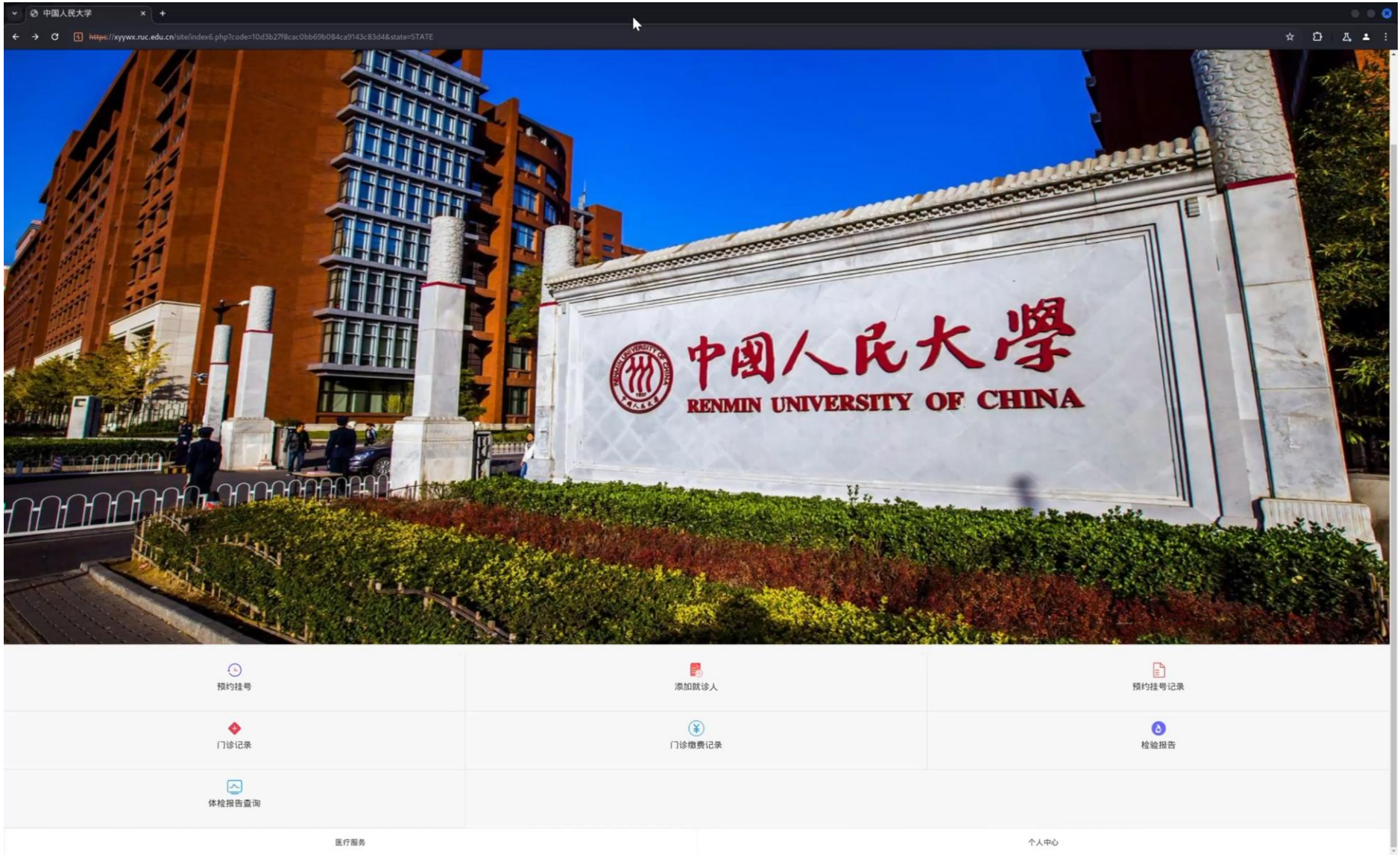
9. 服务端安全——业务逻辑漏洞

授课教师：游伟 副教授
授课时间：周五16:00 – 17:30（教二2406）
课程主页：https://www.youwei.site/course/websecurity

引子1


微人大
https://v.ruc.edu.cn/me#/
微人大 VRUC
搜一搜
个人信息保护及隐私声明
首页
消息
资讯
邮箱
校园网
云盘
服务指南
正版化软件
移动校园
系统使用意见建议
操作指南
常用
教务
校务
财务
服务
学务
我的课程表（本+研）
全校课程表（研究生）
本科教学一体化信息平台
研究生教育信息系统
重修、副修以及其...
学生选课（本科）
法学院教学培养管理系统
副修在线课程
公共管理学院虚拟仿真实...
国际小学期
课程教学平台
课堂教学质量评估（本科）
全校课程表（本科生）
人大未来课堂
网上党校
日程
更多
我的日历
中国人民大学校历
2024-05-05
暂无日程
创建日程
今天
2024年5月
周日 周一 周二 周三 周四 周五 周六
服务中心
微人大服务中心
查看详情
综合服务中心
学务中心
更多
18°C 多云
搜索
21:53 2024/5/5

引子2

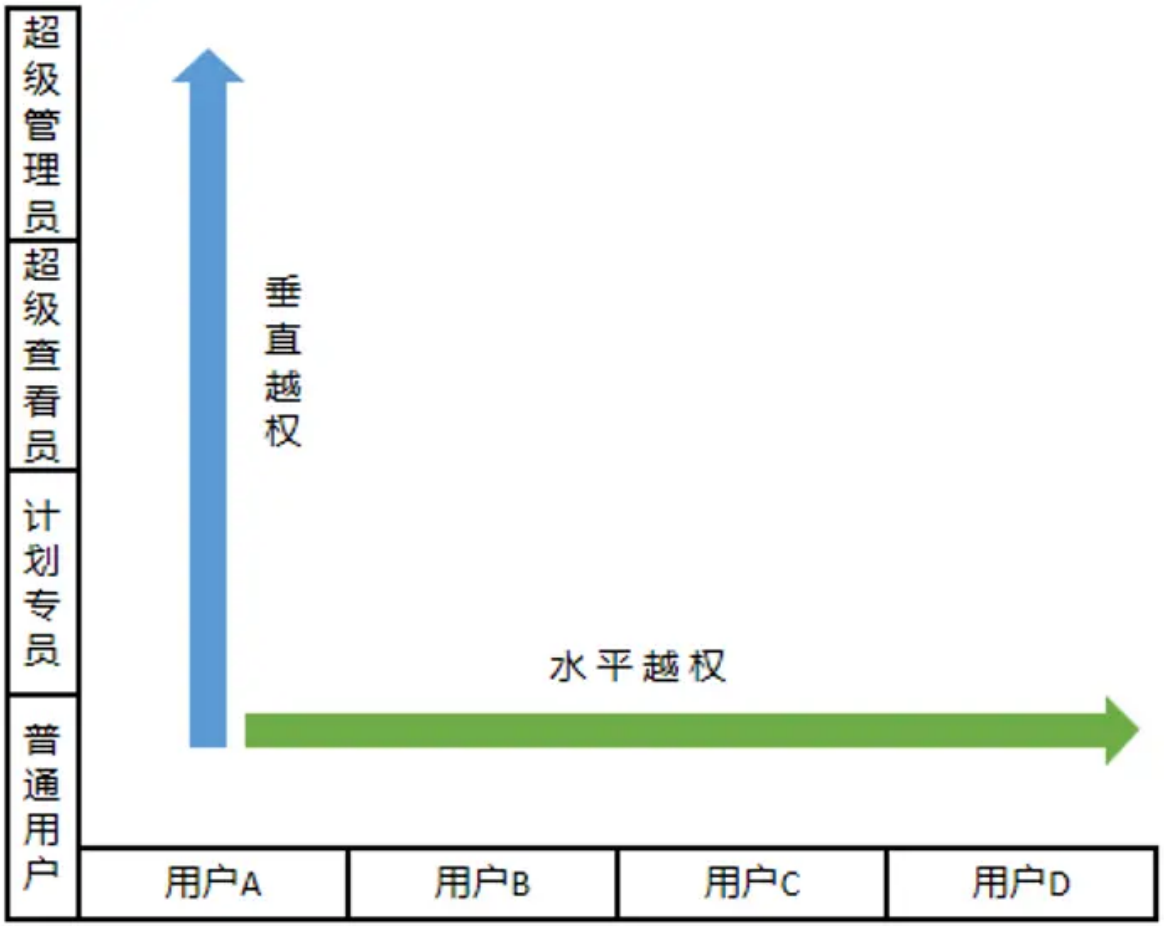

中国人民大学
https://xyywx.ruc.edu.cn/site/index6.php?code=10d3b27f8cac0bb69b084ca9143c83d4&state=STATE
中國人民大學
RENMIN UNIVERSITY OF CHINA
预约挂号
添加就诊人
预约挂号记录
门诊记录
门诊缴费记录
检验报告
体检报告查询
医疗服务
个人中心

越权漏洞

- 越权访问（Broken Access Control，简称BAC）是Web应用程序中一种常见的漏洞，由于其存在范围广、危害大，被OWASP列为Web应用十大安全隐患的第二名。
- 该漏洞是指应用在检查授权时存在纰漏，使得攻击者在获得低权限用户账户后，利用一些方式绕过权限检查，访问或者操作其他用户或者更高权限。越权漏洞的成因主要是因为开发人员在对数据进行增、删、改、查询时对客户端请求的数据过分相信而遗漏了权限的判定，一旦权限验证不充分，就易致越权漏洞。

越权漏洞

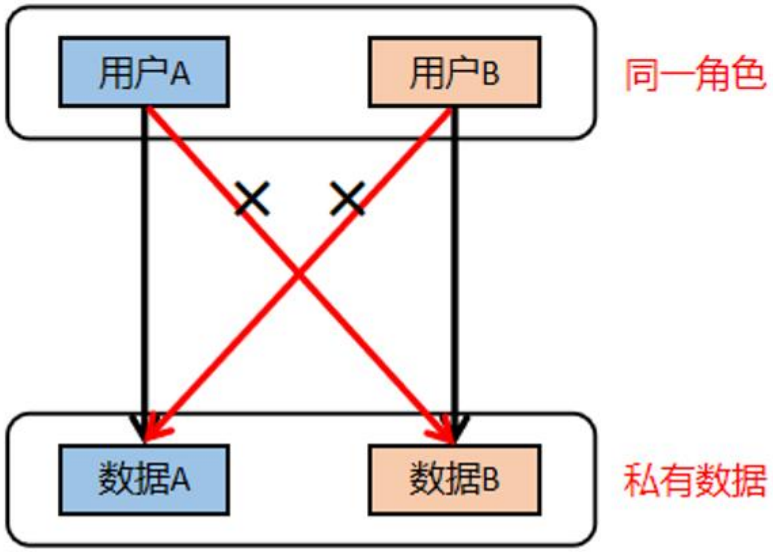
- 越权访问漏洞主要分为水平越权、垂直越权。



水平越权

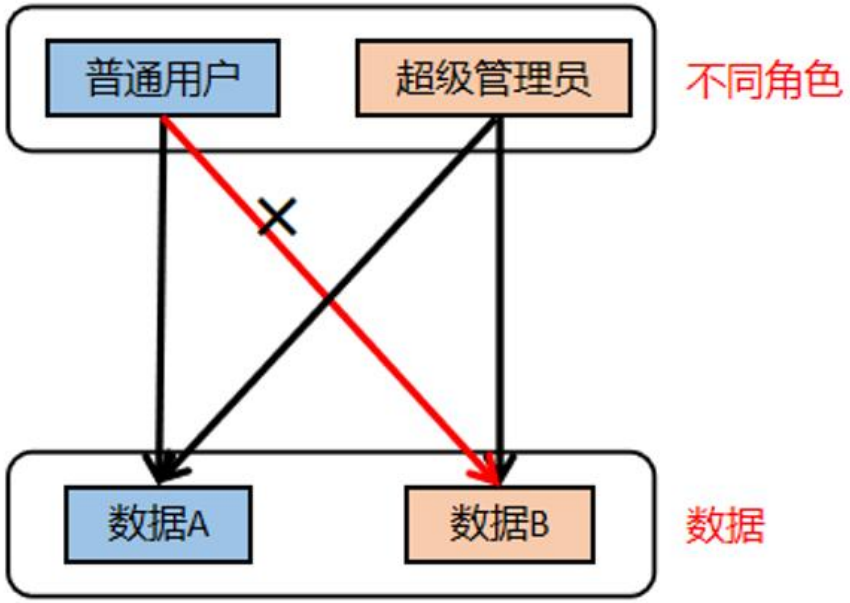
- 水平越权：指攻击者尝试访问与他拥有相同权限的用户资源。

例如，用户A和用户B属于同一角色，拥有相同的权限等级，他们能获取自己的私有数据（数据A和数据B），但如果系统只验证了能访问数据的角色，而没有对数据做细分或者校验，导致用户A能访问到用户B的数据（数据B），那么用户A访问数据B的这种行为就叫做水平越权访问。



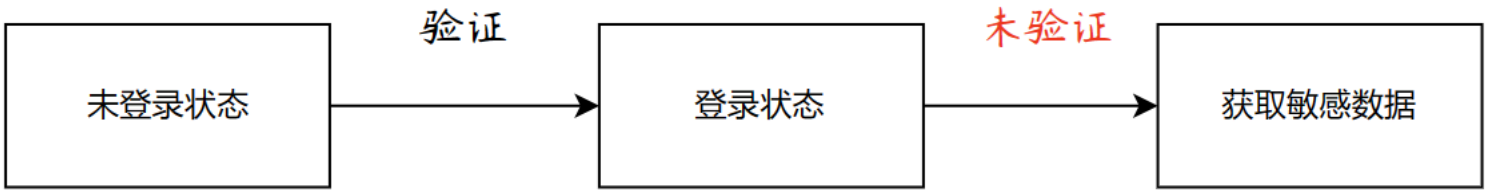
垂直越权

- 垂直越权：由于后台应用没有做权限控制，或仅仅在菜单、按钮上做了权限控制，导致恶意用户只要猜测其他管理页面的URL或者敏感的参数信息，就可以访问或控制其他角色拥有的数据或页面，达到权限提升的目的。



越权漏洞产生的原因

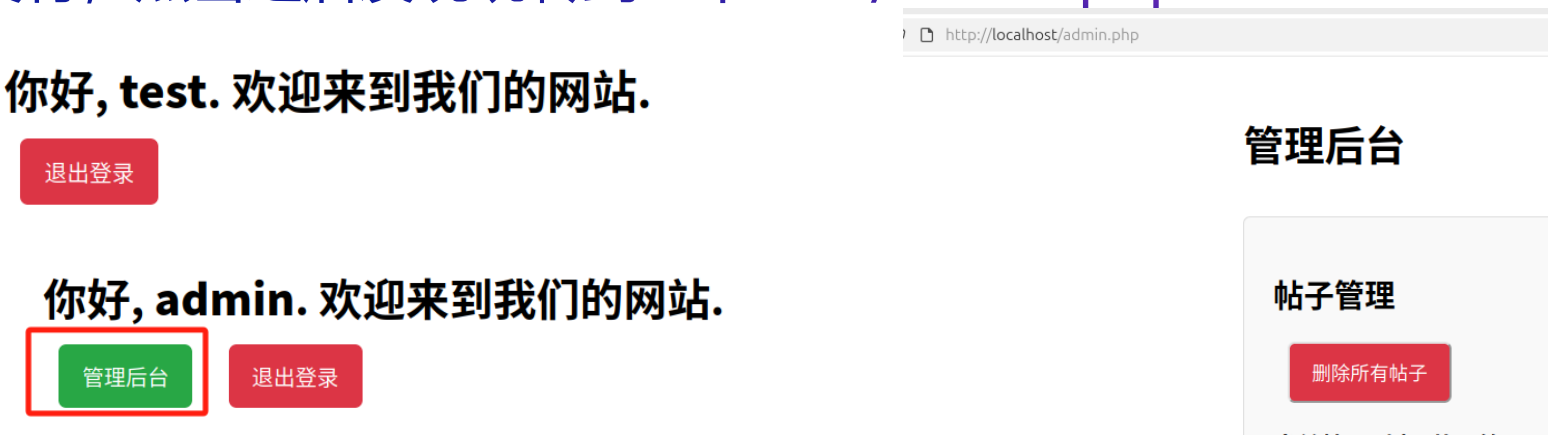
- 通常情况下，一个 Web 程序功能流程是登录 - 提交请求 - 验证权限 - 数据库查询 - 返回结果。如果验证权限不足，便会导致越权。常见的程序都会认为通过登录后即可验证用户的身份，从而不会做下一步验证，最后导致越权。



越权漏洞

- 1. 隐藏 URL
  - 实现控制访问有些程序的管理员的管理页面只有管理员才显示，普通用户看不到，利用 URL 实现访问控制，但 URL 泄露或被恶意攻击者猜到后，这会导致越权攻击。

- 访问靶机，登录admin/1234，可以看到后台管理页面按钮，而其他账号没有，点击之后发现跳转到一个url /admin.php



- 使用test/test123账号也能访问，并删除其他用户的帖子

越权漏洞

- 2. 直接对象引用
  - 这种通过修改一下参数就可以产生越权，例如查看用户信息页面 URL 后加上自己的 id 便可查看，当修改为他人的 ID 号时会返回他人的信息，便产生了越权 。

- 访问靶机，登录test/test123，看到有“个人信息”按钮，点击之后跳转到一个带id的url，并在页面上显示用户的敏感信息，将id改为1，可以看到admin的敏感信息

越权漏洞

- 3. 多阶段功能
  - 多阶段功能是一个功能有多个阶段的实现。例如修改密码，可能第一步是验证用户身份信息，号码验证码类的。当验证成功后，跳到第二步，输入新密码，很多程序会在这一步不再验证用户身份，导致恶意攻击者抓包直接修改参数值，导致可修改任意用户密码。

- 访问靶机，登录test/test123，点击跳转修改邮箱页面，需要验证原密码，验证成功后，进入修改邮箱界面

越权漏洞

- 查看发送的报文，可以看到携带参数中有一个用户id，将这个id修改为admin的id：1，就能绕过前面验证密码的步骤，直接修改admin的邮箱了

```
1  POST /changeMail.php HTTP/1.1
2  Host: 10.10.17.36:32945
3  Content-Length: 80
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://10.10.17.36:32945
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.10.17.36:32945/changeMail.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: user_progress=6; PHPSESSID=4da086fe9996c3c77fe308a829ff34f1
14 Connection: close
15
16 email=user1%40example.com&id=2&change_email=
   %E6%9B%B4%E6%96%B0%E9%82%AE%E7%AE%B1
```

Pretty Raw Hex

```
1  POST /changeMail.php HTTP/1.1
2  Host: 10.10.17.36:32945
3  Content-Length: 80
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://10.10.17.36:32945
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.10.17.36:32945/changeMail.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: user_progress=6; PHPSESSID=4da086fe9996c3c77fe308a829ff34f1
14 Connection: close
15
16 email=user1%40example.com&id=1&change_email=
   %E6%9B%B4%E6%96%B0%E9%82%AE%E7%AE%B1
```

越权漏洞

- 4. 静态文件
  - 很多网站的下载功能，一些被下载的静态文件，例如 pdf、word、xls 等，可能只有付费用户或会员可下载，但当这些文件的 URL 地址泄露后，导致任何人可下载或读取，如果知道 URL 命名规则，则会便利服务器的收费文档进行批量下载。
- 访问靶机，登录admin/1234，有一个查看数据库选项，点击下载了一个.sql文件，查看页面源代码发现vruc.sql的存储位置；
- 退出登录，登录test/test123，访问对应url也能下载文件

越权漏洞的防御

- 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
- 特别敏感操作可以让用户再次输入密码或其他的验证信息
- 可以从用户的加密认证 cookie 中获取当前用户id，防止攻击者对其修改，或在 session、cookie 中加入不可预测、不可猜解的 user 信息
- 加密直接对象引用的资源ID，防止攻击者枚举ID，敏感数据特殊化处理
- 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
- 前后端同时对用户输入信息进行校验，双重验证机制