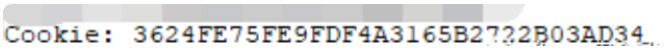
cookie越权--宝马

搜索资产搜索到了一个用户登录后台，但是我没号，注册一个去。

这边有个个人资料，这种点最多的基本是水平越权了吧，但是盒子的这种车企我又感觉不会出现，所以决定抓包看看。



为了方便我就直接写在记事本分析一下，cookie用了md5加密，但是soMD5解不了，用一下一位大佬的VIP账户去md5解一下解出来是：

```
SKRTU248IP043S57Y79
```

然后再抓一次包看看有没有规律

解密出来是

```
KYUIPORE43S5SM79
```

多抓几次直接放解密出来的给大家看

```
LOITUHN45D43S59U79
```

```
KYOUI6794YT43S5L879
```

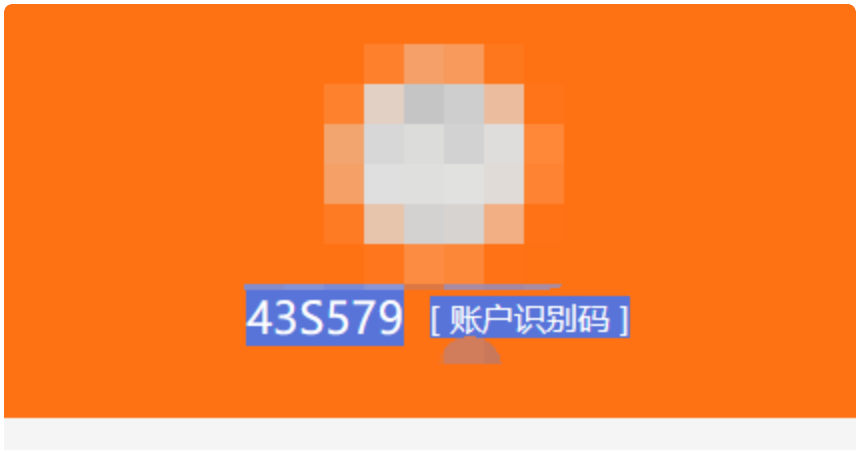
不知道大家发现了规律没有，看似cokie是随机值但是注意看中间的

```
43S5
```

和最后的两位数

```
79
```

然后再回到我们的后台界面



个人资料

我们的账户码就是43S579，所以这边的cookie再43S5前面的值就是随机值然后再隔2位也就是79前的两位也是随机值，这边不一定是2位因为有几次测试的就是3位数的一个随机值。

那这边就尝试更换一下别的账户的识别码看看能不能实现水平越权，先再注册一个

一个账户。

这边记住这个识别码，先用识别码为43S579的这个点击查看个人资料抓包

```
Cookie: F93BD9A7069F21A887F393030D20FC78
```

解密值为

```
1  IOPYTU76843S57SP79
```

按之前的规律来看最后两位就是账户识别码的最后两位所以先把识别码为59KI893的93用来替换cookie中原来的识别码73，再把59KI8用来替换43S57，最后得到的就是。

```
1  IOPYTU76859KI8SP94
```

因为原cookie采用的md5加密这边加密一下再替换

```
1  469F50BE850778E1C652FD18F77F1420
```

替换后放包

账户43S579的成功越到了59KI893上，逻辑洞存在。

，这边的cookie发送到服务器应该是会核对前面和中间那两位随机值的，因为此前我试着更改随机值时就会错误，而识别码的作用应该就是绝对回显信息，两半识别码分散发送最后服务器又重新拼接，然后识别核对识别码，最后发送该账户识别码对应的信息。