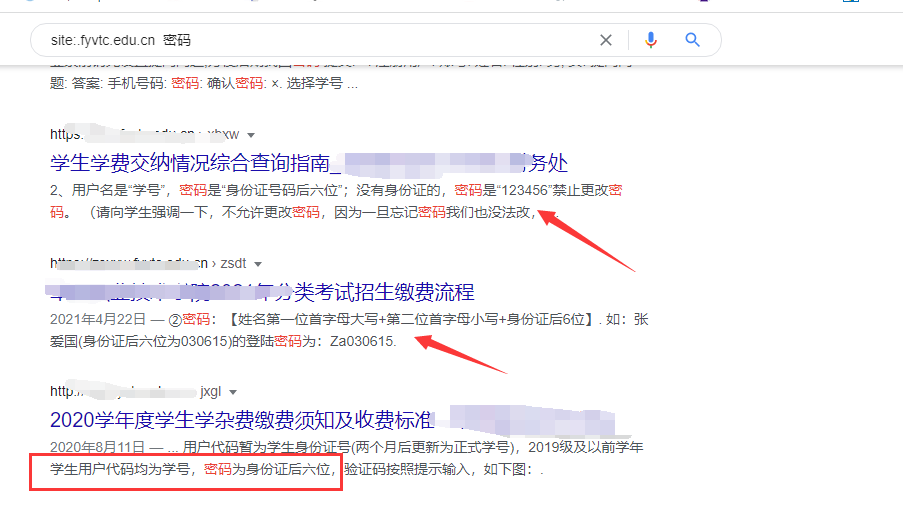
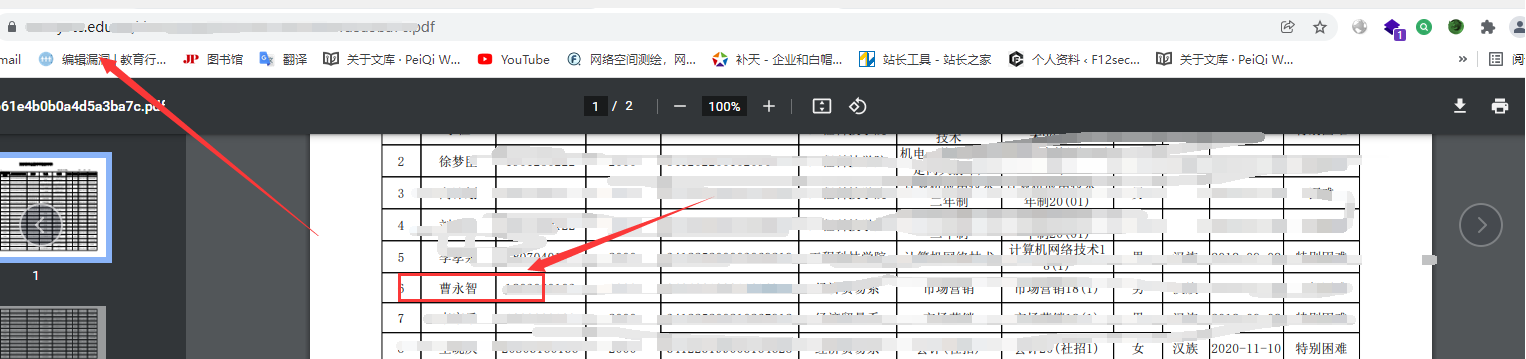
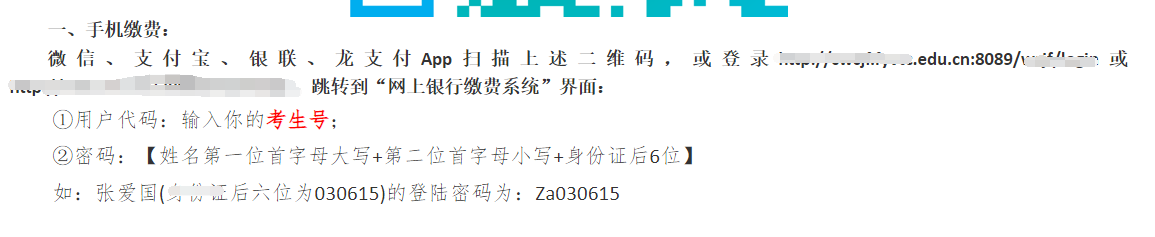
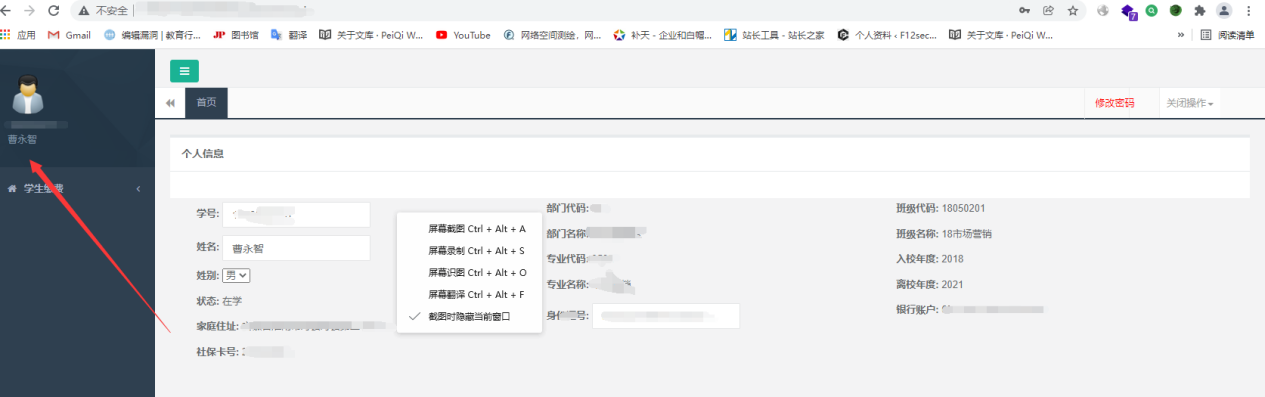
### 信息收集

对于我们在挖edusrc的时候遇见最大的问题就是如何突破一站式服务大厅的网站，要突破这一点，我们就需要拥有教师的gh 、sfz和 学生的sfz、 xh这些个人隐私信息，所以我们就需要做好信息收集：

1. 利用好谷歌语法查找敏感信息：  
    site:xxx.edu.cn  
    这个语句是寻找这个学校的相关域名的站点，但是在这个后面加一些敏感信息就可以指定查找了，比如：site:xxx.edu.cn sfz site:xxx.edu.cn xh 这样的等条件  
     
   如上图一样，直接可以从这个pdf中获取很多信息，一般隐私信息都会以doc pdf xls 这些文件发布到网上，所以造成信息泄露（如果你不追求什么漏洞，上上rank 这一个都够你上几百rank 就谷歌收：site:.edu.cn sfz filetype: pdf|xls|doc 即可。  
    如果以上没有找到自己想要的信息，你就可以去找所在学校相关的教育局站点，因为助学金等奖励都会通过当地教育局进行展开，这样在相关教育局站点我们也可以收集到我们需要的信息。
2. 利用谷歌语法查找脆弱的系统获取信息：  
    site:xxx.edu.cn 初始密码  
    利用上面的语法可以查找许多相关弱口令系统，然后利用上面收集的信息，进行登录，从这些能登录进去的系统，我们也可以获取很多有用的信息，在进一步说，至少我们有学生权限的账号了，可以测试水平或者垂直漏洞，毕竟后台漏洞是要比前台多：  
      
   然后利用我们收集的信息大量尝试登录即可  
   （这是写文章随手挖的）：  
     
   然后再利用我们的初始密码解说去大量爆破弱口令用户：  
     
     
   此次是很顺利的获取的sfz 和xh 这些信息所以这个系统轻松登录，如果二者缺一可以思考如何获取，这一点自己思考：  
     
   后面继续正常漏洞即可，不管出货不出货都可以获取自己想要的信息，上面即可看出大量的信息泄露。
3. 案例：  
   去年是某天的专属src 获取奖励1k：  
     
   AIGK@R4K]9[EKR7MGO%BXQI  
     
   