兰州大学存在未授权访问漏洞

时间	单位	作者	等级	Rank
2022-10-09 18:11:19	兰州大学 (/list/firm/5541)	这咋办嘛 (/profile/14123/)	中危	3

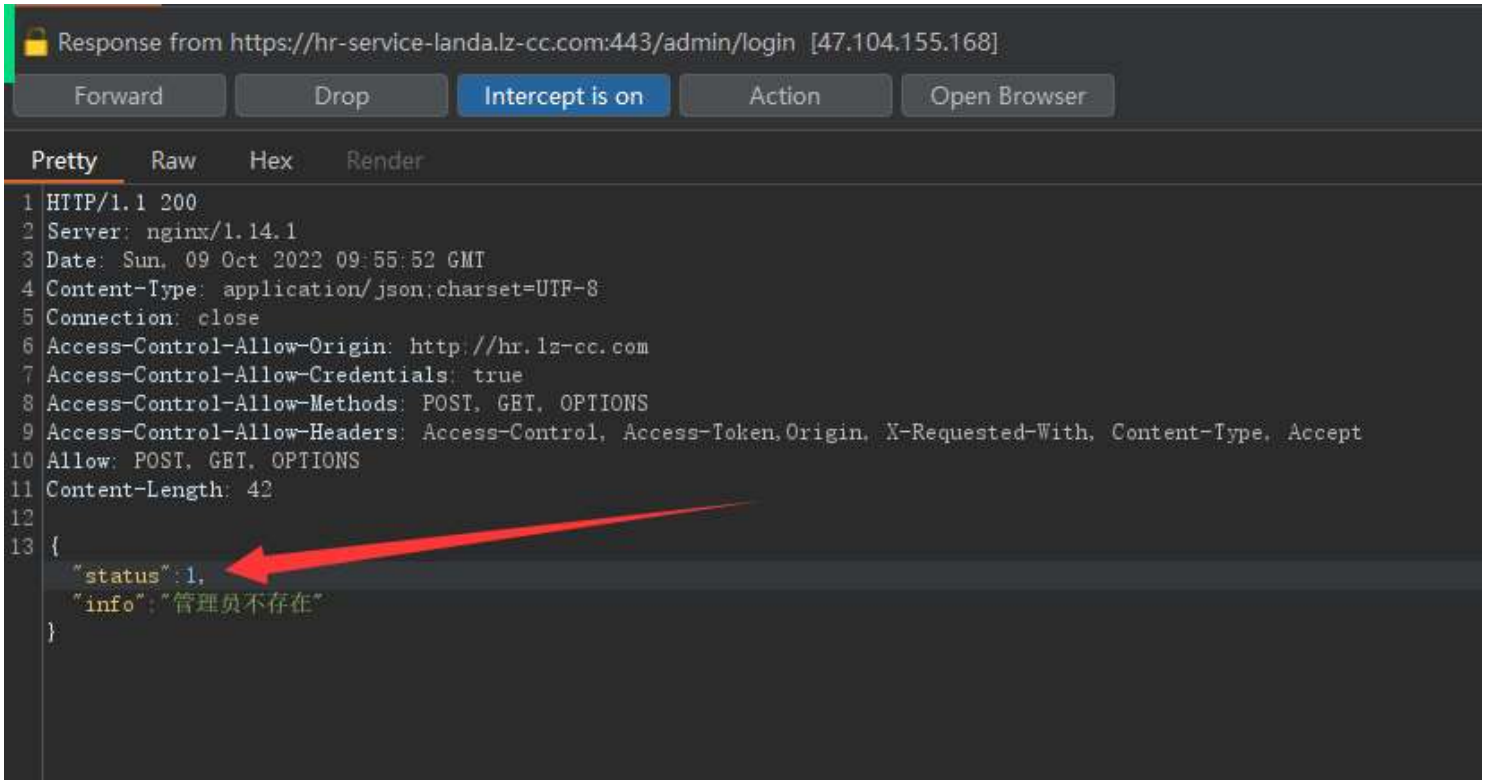
第一次挖证书站，审核哥哥给个高危吧，谢谢了。

漏洞存在地址：http://hr.lz-cc.com/#/login

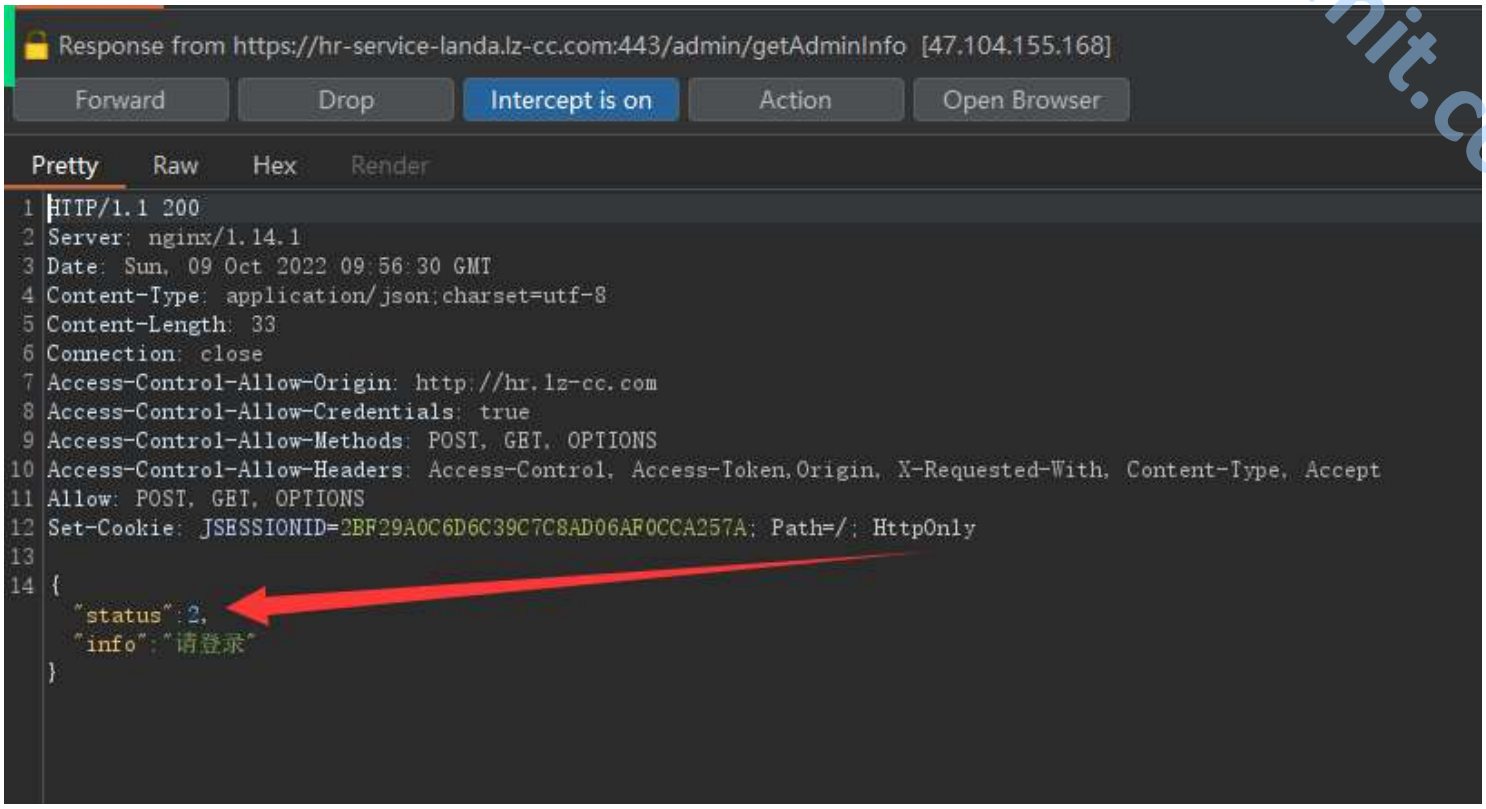
1、输入任意账号密码

以admin/admin为例

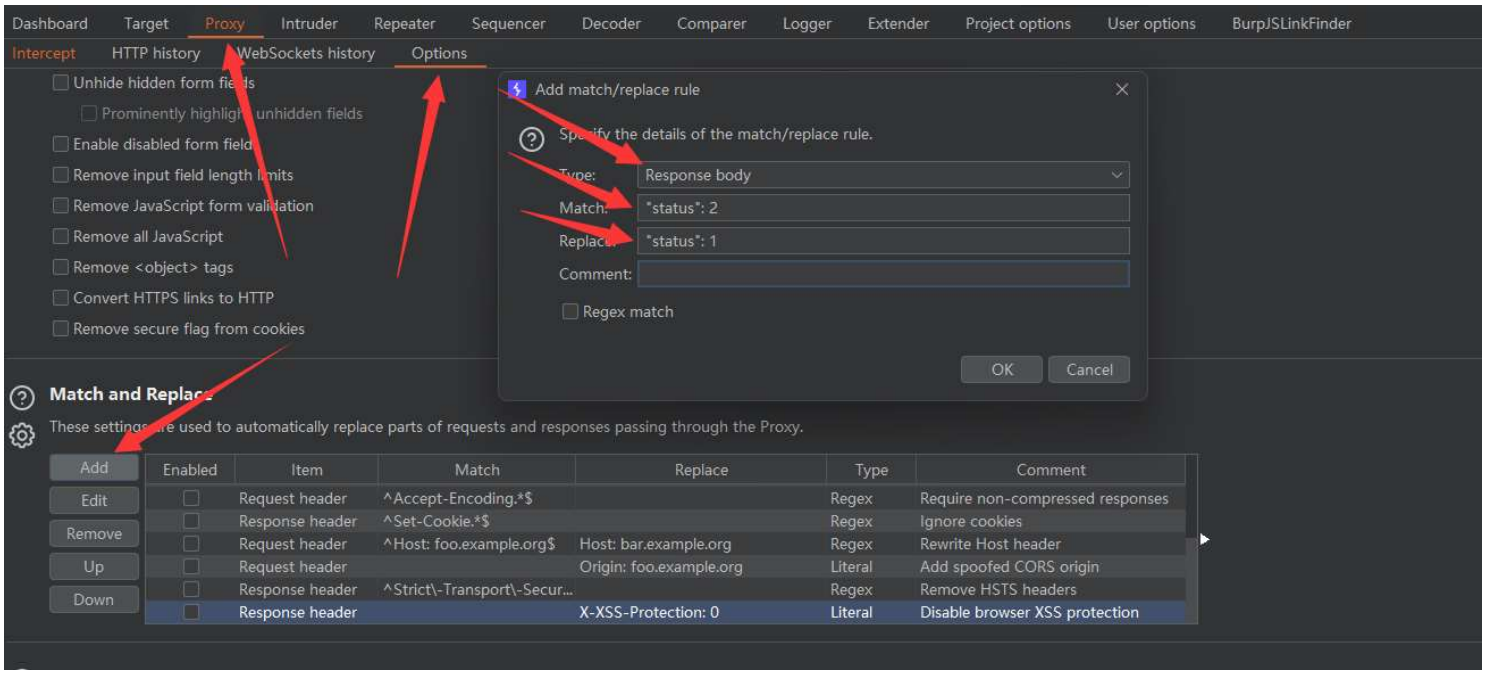
修改返回包将status字段500改成1

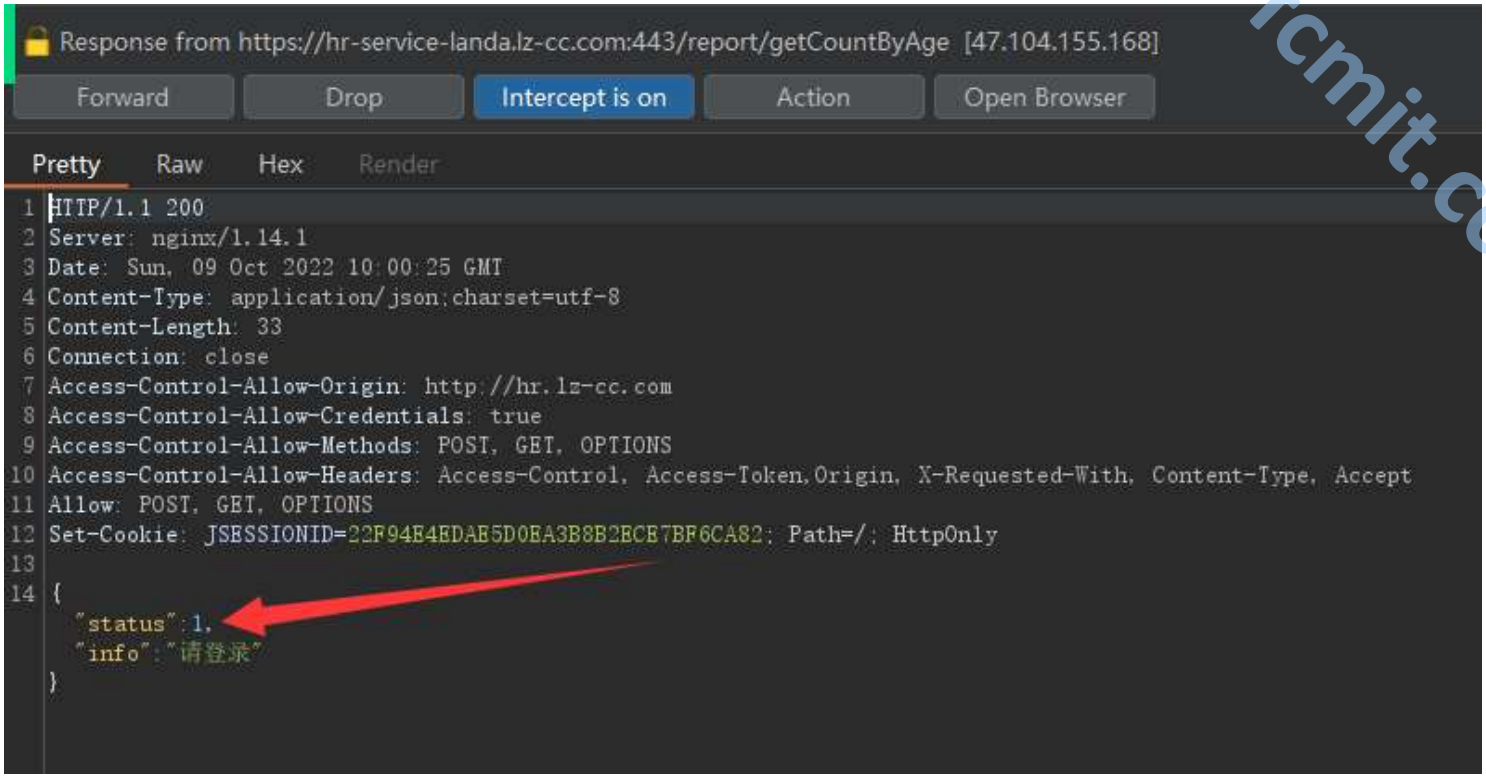


之后遇到这种返回包将2改为1

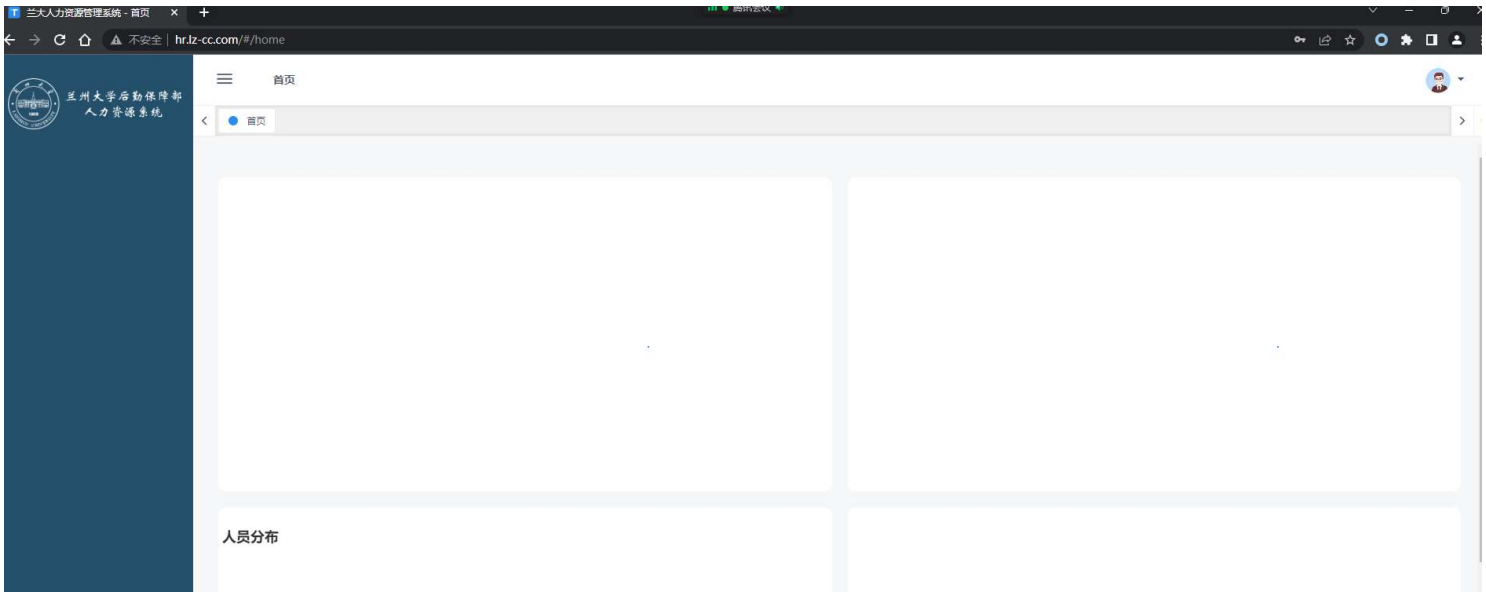


由于有很多这样需要修改的返回包，将BurpSuite如下图一样配置 自动替换，之后的返回包就自动替换为1了



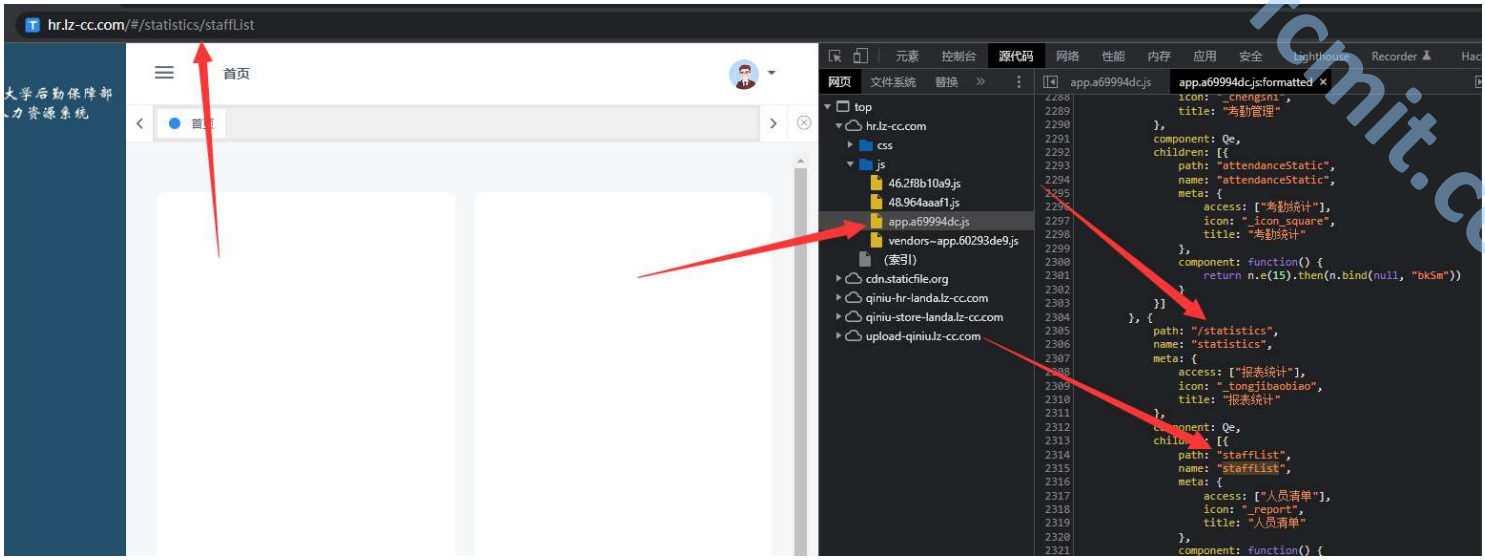


2、可以看到能够成功越过登录进入后台界面，但无任何功能，通过分析js代码

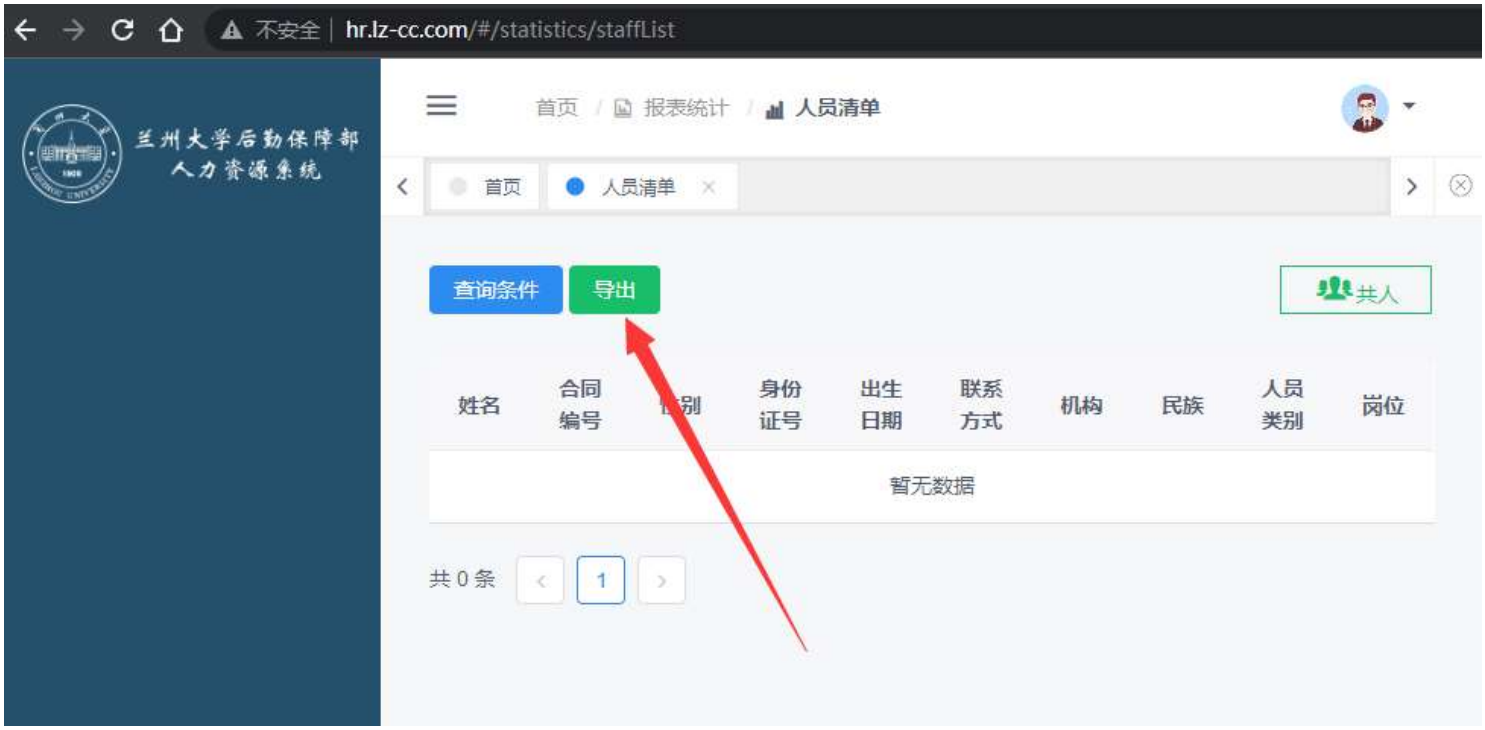


经过分析测试，发现以下接口存在未授权下载用户敏感信息，将url #后面的链接替换为/statistics/staffList

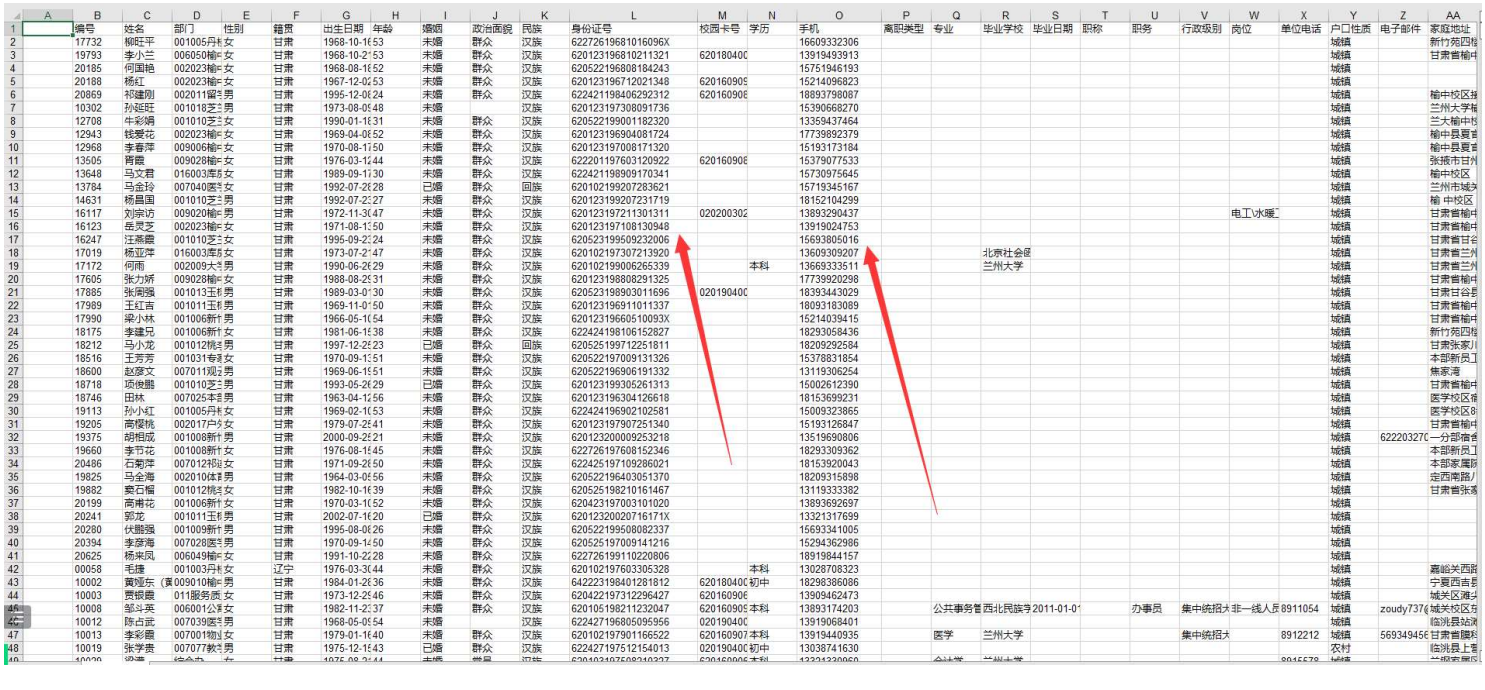
注：绕过登录进入后台后替换 不要直接访问



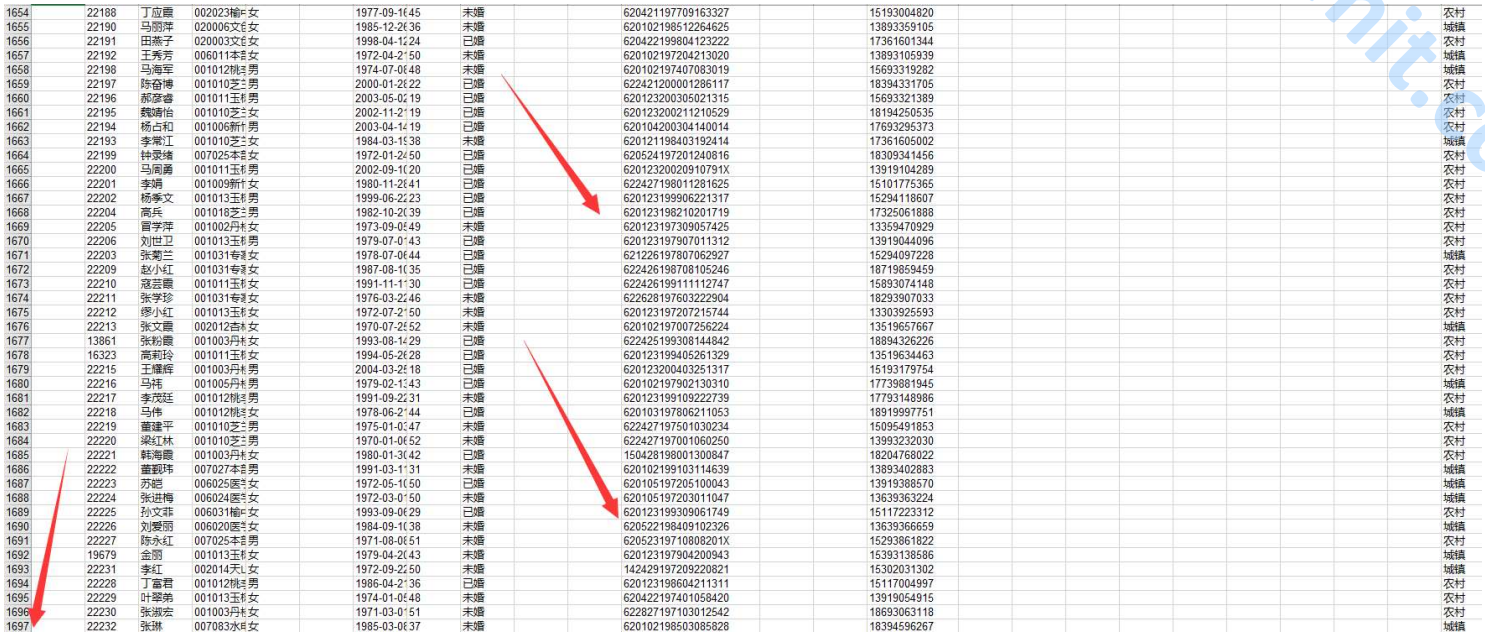
可以发现该处有一个导出按钮，点击导出，由于数据过多 需等待过长时间，请耐心等待



3、可以看到有着大量的敏感信息 身份证 手机号 姓名



往下拖拽，可以看到至少泄露了1700多人的敏感信息。



| | | |