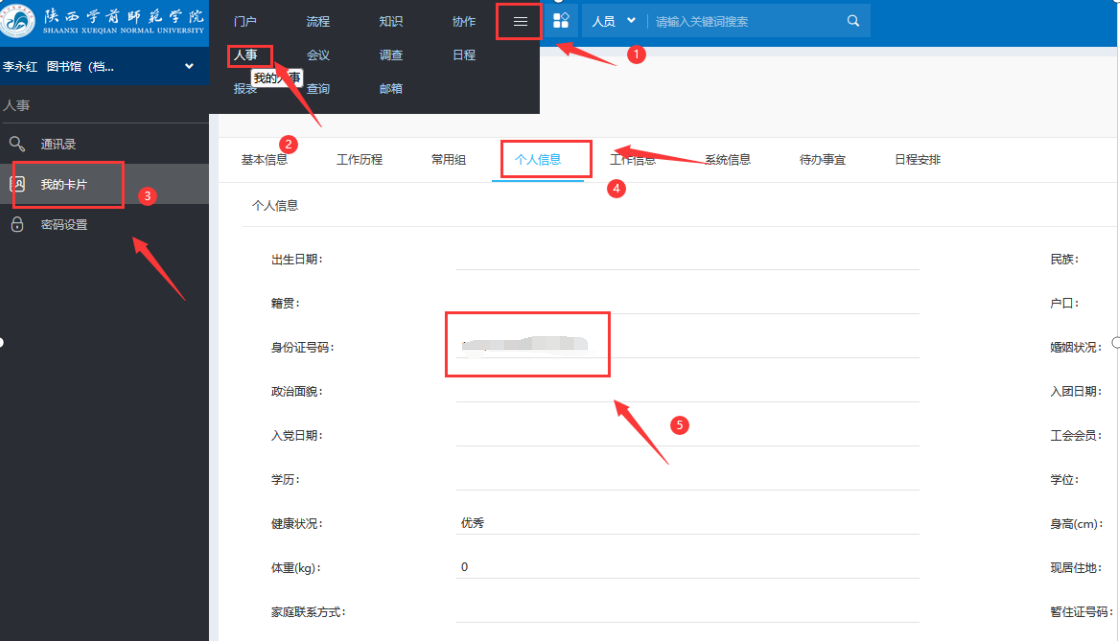
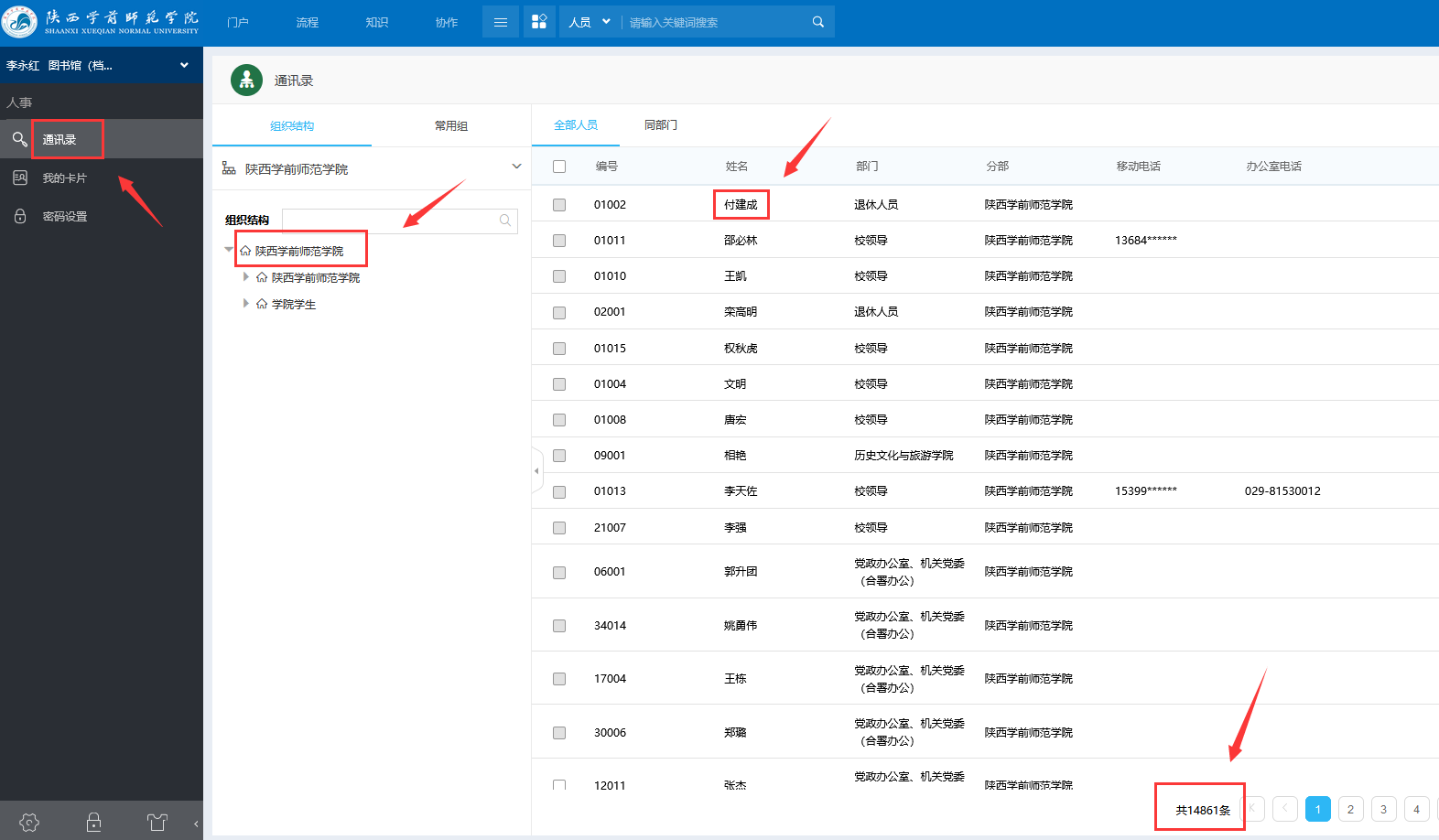
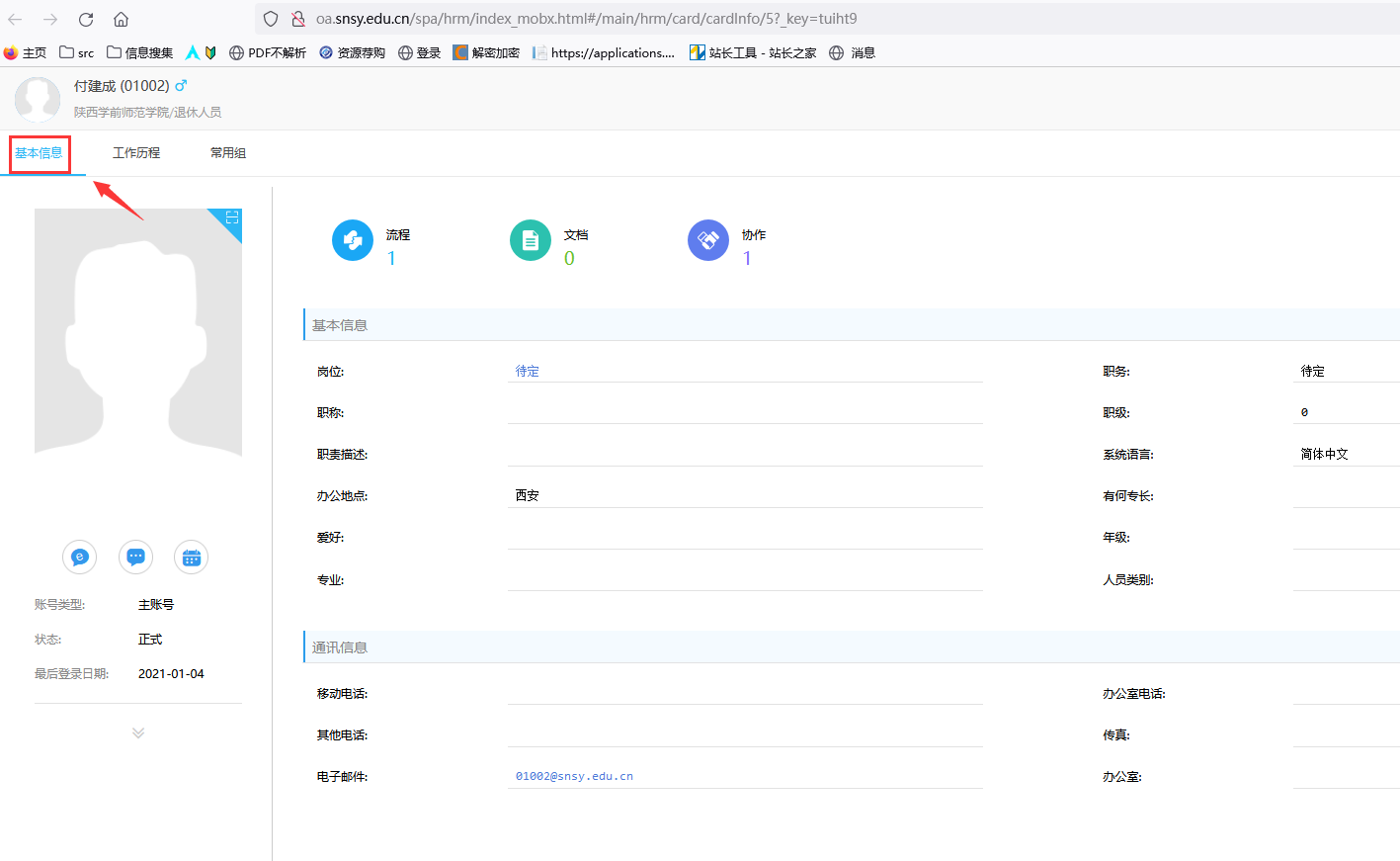
人事 -> 我的卡片 -> 个人信息，可以查看到自己的身份证号



通讯录可以看到约1.5w条师生个人信息，直接点击姓名进行访问（这里以付建成为例）



可以正常访问其基本信息，但并不包含身份证等敏感信息，当然，这很合理



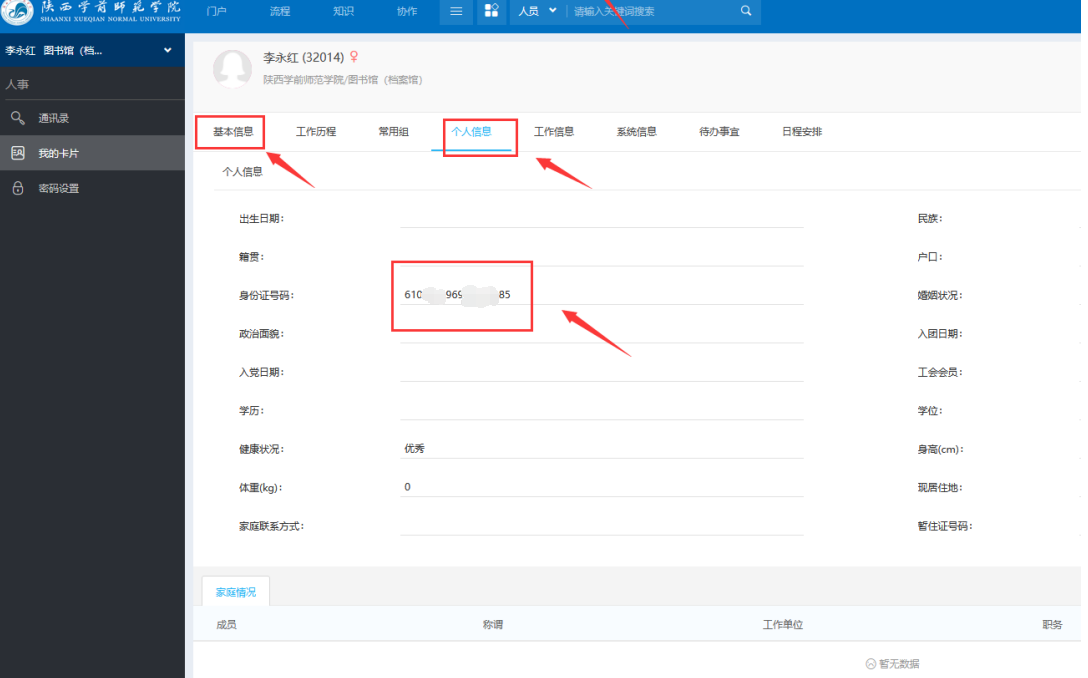
不过仔细对比发现，个人卡片的身份证信息在“个人信息”模块，而不是”基本信息“模块；

而他人卡片并不存在“个人信息”模块；

对比两个模块的URL路径，发现个人信息模块路径含“/cardPersonal/”，

而基本信息模块与之对应的路径是“/cardinfo/”；

直接将他人卡片URL路径中的“/cardinfo/”替换成“/cardPersonal/”新建标签页（这点很重要）访问；



越权成功，身份证这不就出来了吗，利用此法可获取全校师生约1.5w个人敏感信息

