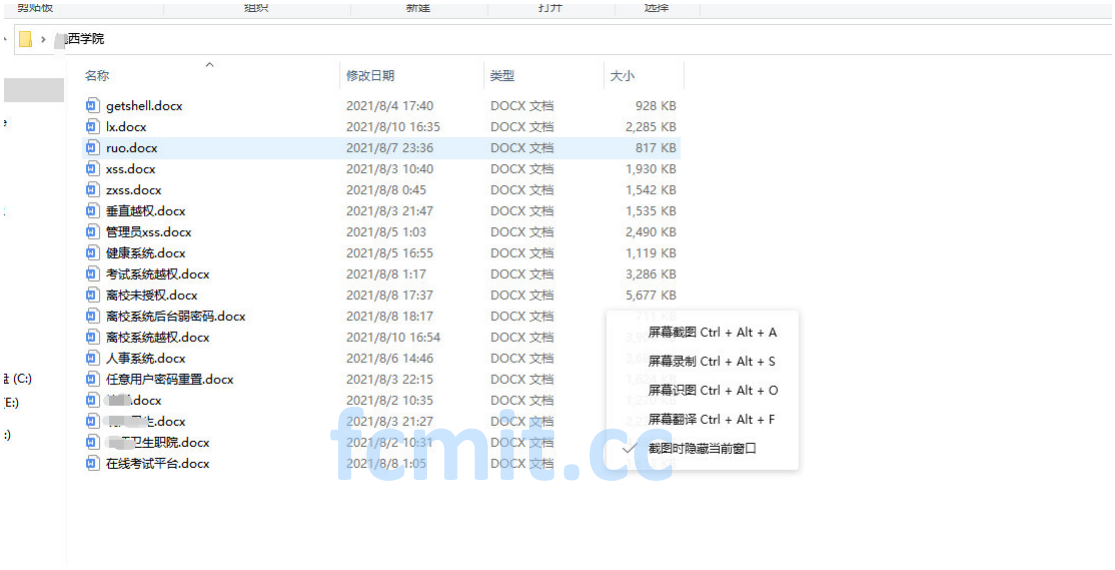
教育 SRC 日刷百分

Ps:

（对于 edu 想上分的同学有两种方式：1.挖通用 2.定点打击学校，全部日穿。此文采用的是第二种方法）

首先确定目标学校：对于学校可以在平台上选择漏洞较少的学校，因为学校可能没有被多少人挖过，很少被通报，猜测学校的安全意识比较低，所以这次我就去给这样的学校好好的上一课。这是本次的成果，edu 上分 80 多 rank，用时一天，edu 高校如此多，每天打一个，那么上分不是轻轻松松了？



目标：https://www.xxxxxx.edu.cn/

确定目标之后就是对于该学校的信息收集，主要收集：xh、SFZ、gh、电话号码等信息，因为信息收集是渗透的核心，如果信息收集几分钟，那么你挖洞就是几个星期或者几个月都不会出货，如果信息收集够多，那么挖洞就会很快出货。

1. 信息收集：

对于高校，一般可以利用谷歌语法：filetype:xls site:xxx.edu sh gh SFZ 这些去收集我们所需要的东西，也可以去当地的教育局官网查看有没有敏感信息泄露，比如贫困生补助，奖学金补助等等文件很容易泄露重要信息的，再者就是在学校官网查看看有没有信息泄露，一般有公示文件，这些文件也特别容易泄露信息，最后最后就是 sg 了，当然这个我可不介意哈哈哈哈哈（虽然 wo 特别喜欢，毕竟一个证书大学一个女朋友嘿嘿嘿）

此次突破就是该学校的官网泄露，造成此次的渗透事件，所以高校在发文时一定要做好脱敏处理

https://www.xxxx.edu.cn/xxxx/info/1017/1222.htm(可以看出是主站泄露了同学的 sfz，然

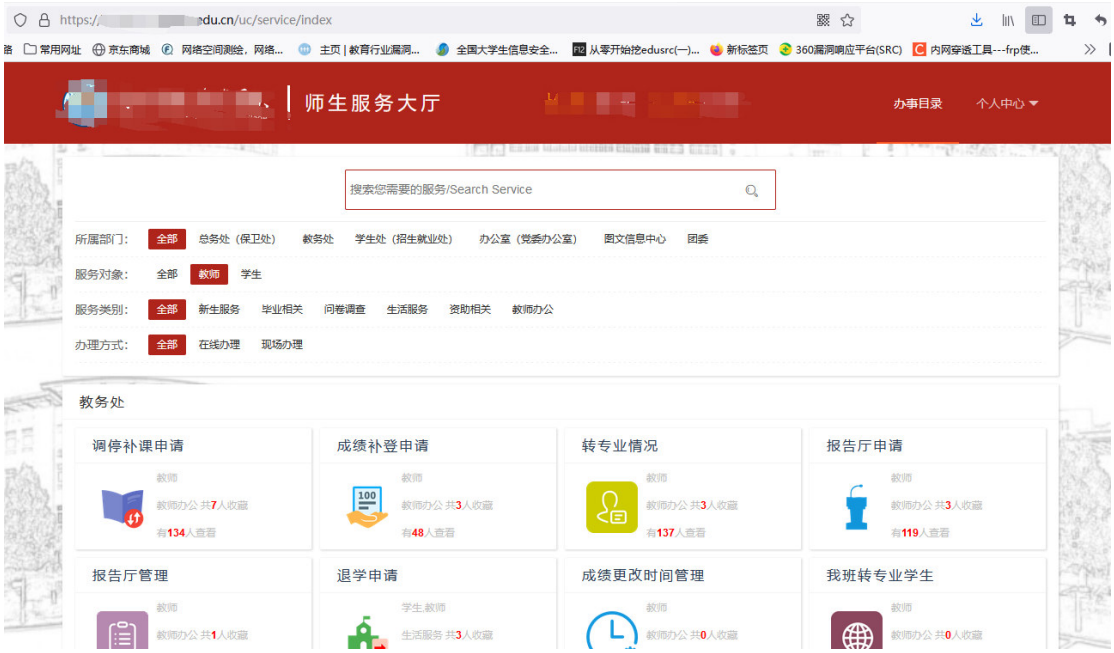
后我们再利用该信息，反查 xh，这样就可以利用 sfz 和学号的弱口令进入 webvpn，然后开始挖掘漏洞）

序号	姓名	身份证号	性别	报考单位	报考专业	准考证号
1		3424	女	大 市分校	汉语言文学	090
2	陈	34122 98		市分校	会计学	090 1
3	陶	3424	男		教育技术学	09
4	余	3408 5 0 2	男	心	汉语言文学	09
5		342 3	男	安市 心	物理学类	0
6	邢	342 2 1	女	安市 中心	财务管理及相关	9
7	张	340 4	女	中心	计算机类	3 3
8		342 3	女		汉语言文学	
9		342 0 0 2	女		数学与应用数学	09 0
10		340 0	女	心	特殊教育	0 0 0 2
11		342 2	女	心	特殊教育	09 0 0 72
12	袁	342 74	男		岩土工程	09 0
13	郭	34 10 33.	男	院	园林植物与观赏园艺	09 0
14	汪	3 088 2 1	男	院	服装设计与工程	09 0
15		34122 427 2	女	学院	区域经济学	090

2. 信息收集搞好后，就可以开始渗透之旅了，利用收集好的账号和 sfz 对官网一站式服务大厅进行爆破（高校网络安全意识差，肯定存在弱口令的），找到门户服务网站此时一定要注意门户网站的帮助说明这些，因为这里会告诉你默认密码的情况：

当我们点开帮助说明的时候，几乎就可以露出笑容了：很清楚的写出来了初始密码：

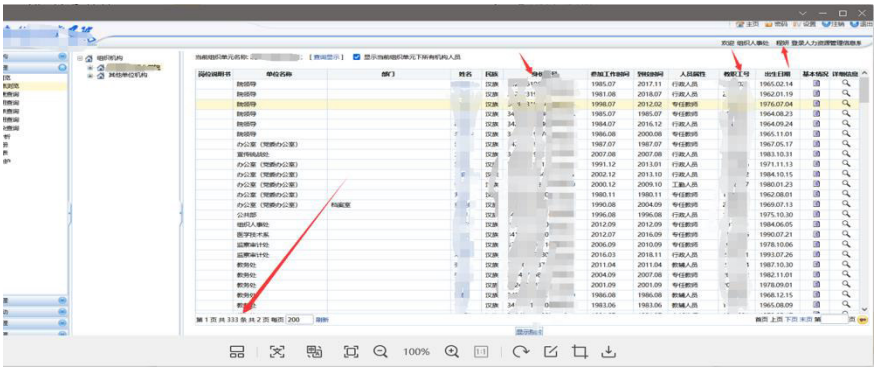
我们信息收集的也很顺利，其中很多账号都是默认口令，于是开始对系统一一进行测试：



然后开始对每一个系统都开始进行测试，当然，进去后我最喜欢的系统一般是人事系统，学生管理系统等等，这个懂的都懂：

所以我第一个打的就是人事系统了，可以继续猜测，这个学校没有任何安全意识，于是这个人事系统也可以猜测大多数为弱口令，加上刚才收集的老师和学生账号开始测试：直接抓包爆破，果然在我猜测之中，该系统全体师生都是弱口令：66xx66

当进入这个系统后，就可以宣判这个学校结束了（当然这时候才是开始）全校师生的个人的信息全部泄露：



此系统因为弱口令泄露了很多信息，其余逻辑都测试和一些不重要的 xss 我就不写了，然后

进行学工系统的测试（当然这个系统也是全校学校师生弱口令）

url 为 http://xx.xxx.xxx.xxx:8312/admin/login/index

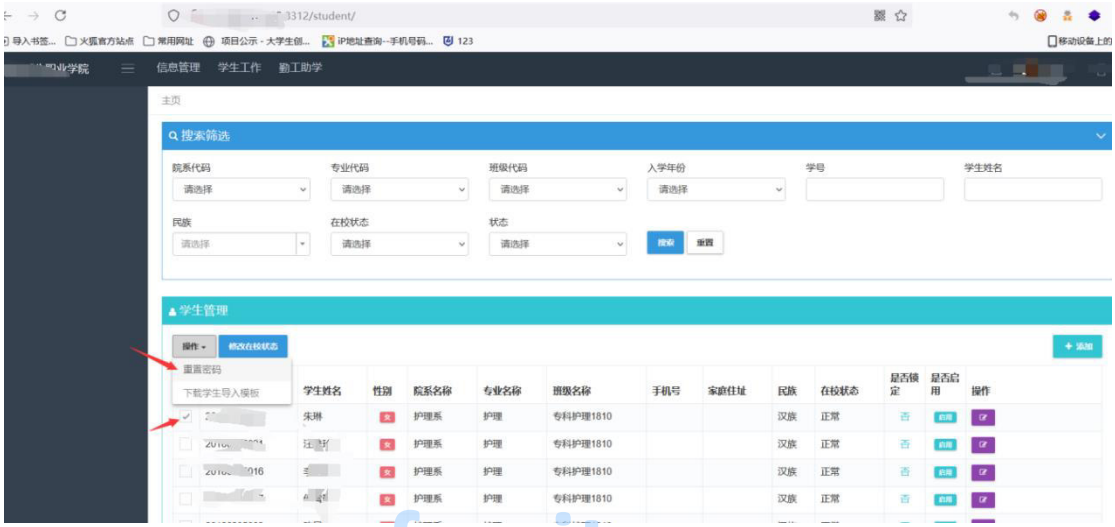
弱密码登录，密码是账号

我使用的测试账号为 202121 输入密码 202121 然后第一次登录系统会自动进行密码重置，重置密码为 Test123#

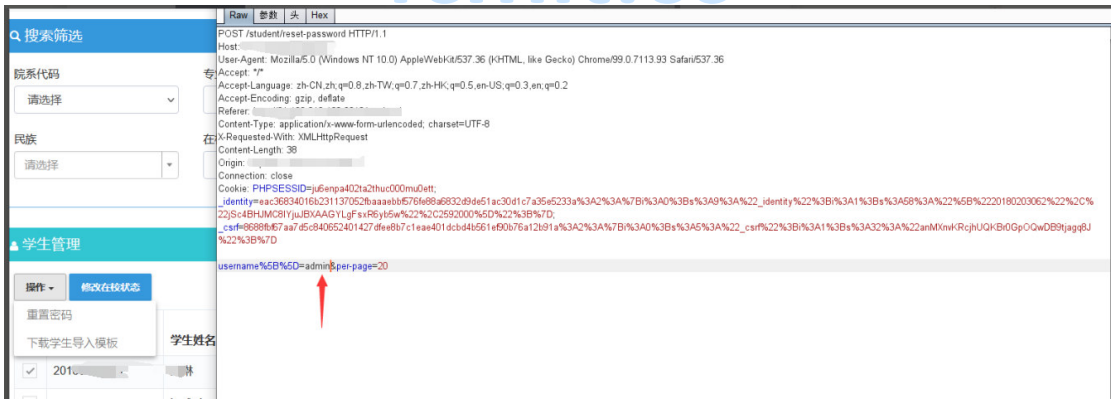
此处提供一个未重置密码的测试账号 20212121 密码 2007002(此处全是虚假信息）

我们使用学生账号登录成功后，对于该系统进行测试，没有上传点，sql 注入的 waf 也挺严的，于是我只有考虑逻辑漏洞，没想到，这个系统对于权限控制的很无语，可以水平和垂直越权：（此处直接修改 id 即可越权，然后此系统中每个功能点都能如此越权，也可以直接越权到管理员权限，此处不一一上图了）

此系统还有一个有趣的地方就是任意密码重置，可以直接将管理员密码重置：



进行抓包，然后修改数据包即可：



然后退出尝试登录，一发不可收拾：获取管理员权限后，然后又是再一次泄露全校师生个人信息，此系统共 15 个越权点和数不清的存储 xss（这个就不截图了）

请人信息

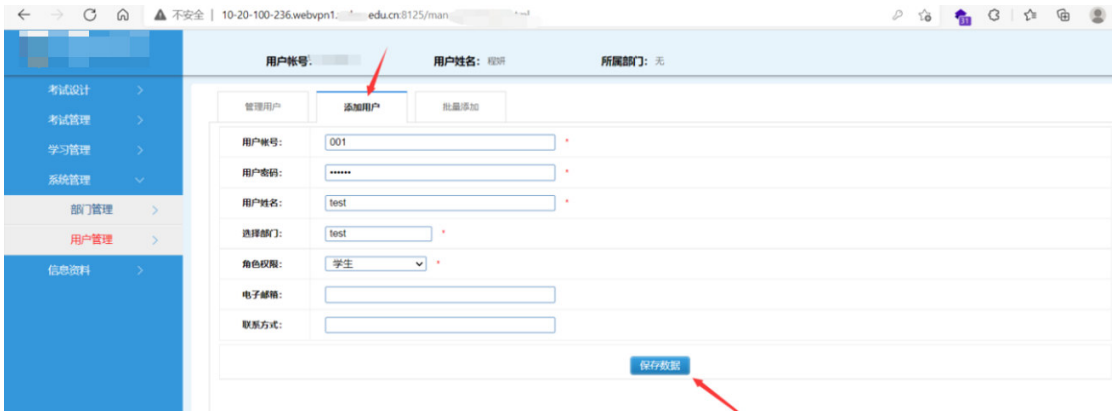
岗位名称	行政助理	用工部门	学生处（招生就业处）
院系		专业	护理
班级		班级年份	2020
姓名		性别	女
出生日期	2002-12-04	政治面貌	群众
所在校区		身份证号	
家庭地址		家庭电话	18656452319
手机号		农业银行卡账号	
宿舍楼号	1	宿舍房间号	508
家庭经济困难认定情况	未认定困难	是否助学贷款	是
是否学费减免	否	申请时间	2021-05-15 17:33:34
实践经历(获奖情况和特长)	英语B级 计算机一级 普通话二甲		

拿下系统管理员权限后，进去可以获取管理员的路径 url，然后使用学生权限的账号也可以直接越权访问，由于毕竟无聊，我就不截图了，其实还是我比较懒。。。

然后继续测试考试系统，此系统也是无数个漏洞，此文章我就写一个我个人感觉有点意思的漏洞，越权添加管理员：

url 为 http://10-20-100-236.webvpn1.xxxxx.edu.cn:8125

使用之前获取的学生账号登录后，来到用户管理，添加用户，填写用户信息。账号 001 密码 123456 点击保存



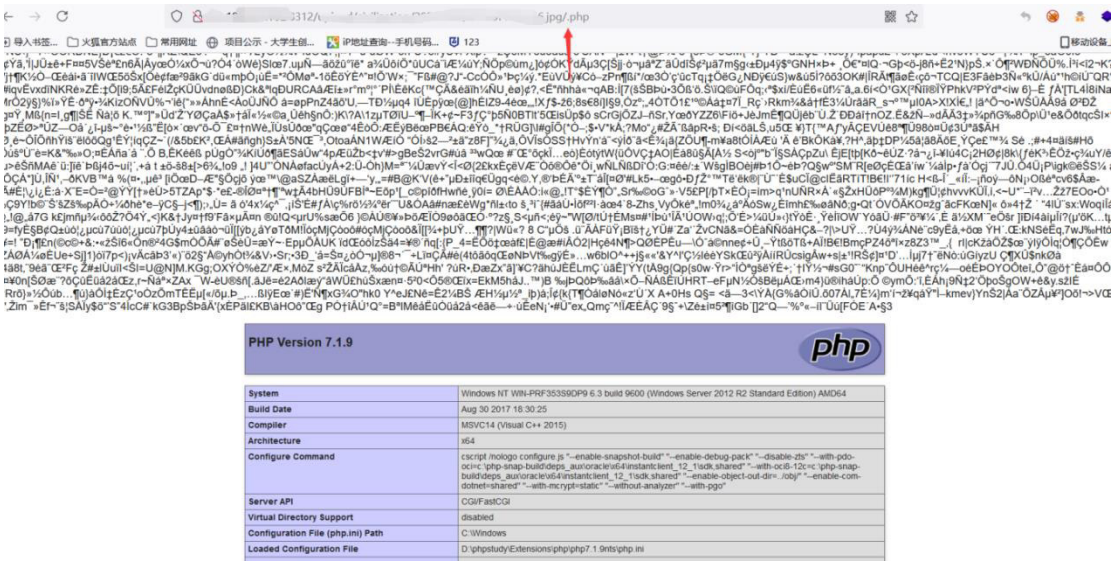
抓包，将 ddlRole 参数值改为 0，然后放包

退出登录，然后登录刚刚创建的管理员账户 001 密码 123456

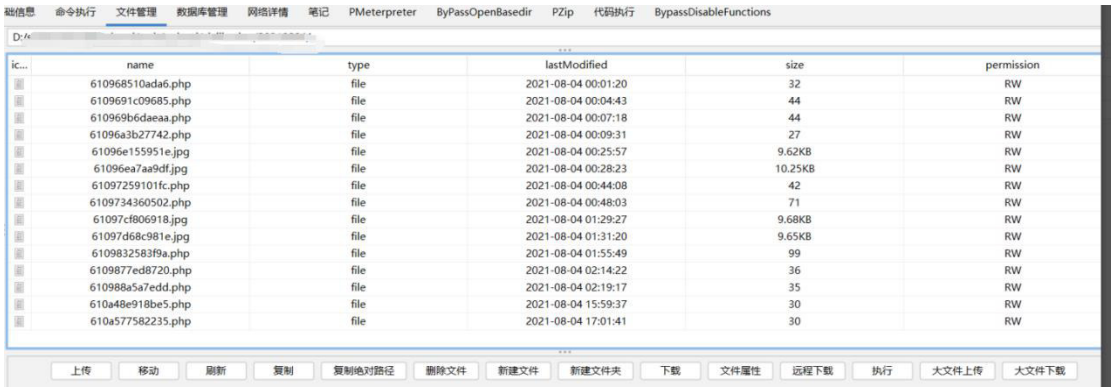
成功添加，此处还有一个修改返回包可以到达任意用户登录的漏洞我就不简单叙述了，到此还有很系统都存在如此的逻辑漏洞，我就不继续浪费大家的时间了，如果对一个学校就这样测试肯定就显得很没有意思了，在我测试逻辑测试到无聊的时候，我又返回到了学工系统，因为这个系统我用管理员账号登录的时候发现了文件上传点（不想拿 shell 的渗透测试人员都不是好的人员）

1.学工系统文明寝室评选管理文件上传存在 cgi 解析漏洞

直接上传图片马然后访问加上/.php 即可，此漏洞简单我就不讲述原理了：



当然这个解析漏洞只能命令执行不能上 webshell，然后我在继续测试的过程中发现可以直接上传 php 马子，这就让我无语了，我抓包修改后缀没有上传成功，但是我直接上传 php 的哥室拉马子反而成功，这是我到现在都很迷的：（其余马子都不能上传，一句话木马可以命令执行但是链接不了 webshell 管理器）



当拿下 shell 后，确定了不是在云服务器上，我就心想，上线 cs 看看内网如何

于是接下来的就是常规操作，上线 cs 和搭建隧道进行内网渗透，内网也是漏洞百出，下文就不再写了，在 edusrc 中也是违规操作了，所以如果想上分的小伙伴可以像我这样定点打击目标系统，进入门户网站后，对每一个系统都认真的测试，因为逻辑漏洞太多太多了，本文也算是对逻辑漏洞的一种叙述，最后此次渗透就到此结束。