

**不是不搞你 是为什么搞你**

习科道展网络信息安全顾问

最具实力的网络安全专家

# 索引

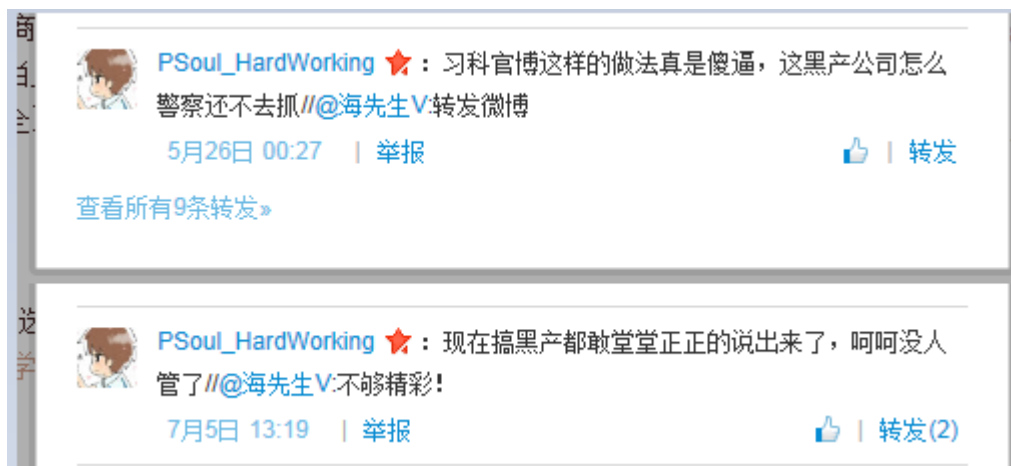
- 1) 满嘴跑火车
  - 1.1 微博作者
  - 1.2 T00ls 交流群 却之不恭
- 2) 陈永鹏
  - 2.1 基本资料
  - 2.2 所受教育
  - 2.3 如何格盘
- 3) 写在最后

## 1) 满嘴跑火车

习科官方的日常工作非常繁忙，在国内的安全圈内也极少抛头露面，即使在习科论坛也鲜有官方人员露面。偶尔会把工作中的一些心得、国际安全圈的快报和一些技术细节分享出来，努力且努力的为国家网络安全建设做出努力。然后就是这样的一个公司，也经常躺枪，成为别人网络舆论攻击的对象。这不，一个熊孩子一而再再而三的满嘴跑火车。

### 1.1 微博作者

习科偶尔会把一些技术细节分享出来，也会经常在官方微博中发出链接。一只和习科完全没有交集的熊孩子在新浪微博上，莫名其妙的就对我们进行冷嘲热讽，不知道我们哪里得罪你了，就算是某安全厂商的脑残粉也用不着连续攻击习科吧？



其他一些评论就不截图了，看到微博的这位作者 ID: **Psoul\_HardWorking**。其个人微博主页是: [weibo.com/soulapeng](http://weibo.com/soulapeng)

网络言论自由不代表你可以任意造谣、诽谤和恶意中伤他人，根据最高人民法院《关于审理名誉权案件若干问题的解答》中第七项和第八项规定，持续侵害习科公司的企业名誉权，我们有权利要求网友 soulapeng 停止侵害行为，并保留起诉的权力。

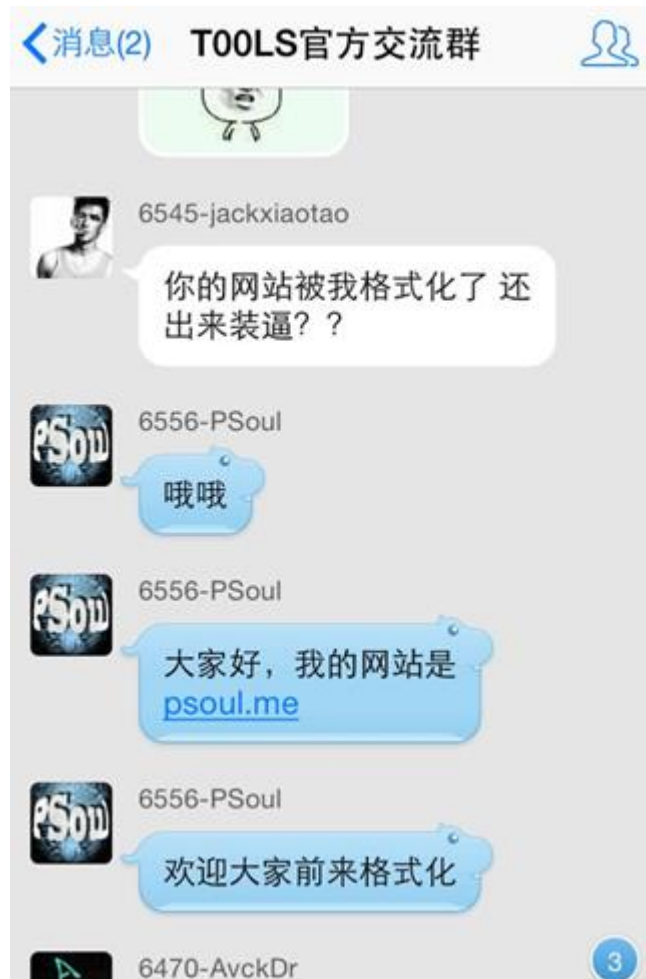
### 1.2 T00ls 官方交流群 却之不恭

这个微博作者的 ID 为什么这么眼熟？

习科论坛 VIP 交流群讨论这件躺枪事件的时候，另外一位论坛 VIP 会员发了一张截图，

*Silic Focus*

是 PSoul 在 T00ls 交流群里的聊天记录，而且刚发生不久。



根据相关法律条文，未经授权的入侵是要受到法律的制裁的。不过既然网站站长本人很担心自己网站的安全，并且对自己服务器有足够的信息，授权的安全检测如果属于非法或者所谓的“黑产”，那国内的绿\*、启\*、36\*、腾\*、百\*、恒安\*\*、天融\*、\*恒、\*天、知\*\*\*什么的，干脆都抓抓干净好了，网络安全这点事，谁不知道谁呀 ☺

既然站长欢迎，我们就却之不恭了，别说在地球上，在空间站也一样，不是搞不了你，而是为什么要搞你。

## 2) 陈永鹏

根据其微博 ID 和留下的网站域名，确认到了 PSoul 的很多基本信息。

### 2.1 基本资料

每个网站在注册域名的时候都会填写 whois 信息，有的出于隐私的需要被域名商隐藏，而国内厂商下的绝大多数域名则是公开 whois 的。

真实姓名：陈勇鹏 #QQ 群关系，xx.pw 可查

新浪微博：weibo.com/soulapeng

腾讯微博：t.qq.com/soulaten #这个很好确认

个人主页：psoul.me

QQ：263510130 #T00ls 交流群

生日：1992 年 9 月 11 日 #微博说的



学校：广州工程技术职业学院 #资料自己填的

手机：18520606584、13570959381、15917048266 #步步高 VIVO X3，绑了微信



百度 ID：irockthemost 淡定的啊鹏 #多玩

Email:

psoul1@163.com #whois 信息

psoul@live.cn #pconline 和 17173，不一定对

B\_mash@yeah.net #百度知道留

263510130@qq.com #QQ 邮箱 绑定 YY 语音

Psoul@lxc.cc

#邮箱邮件

360 云盘：绑定上面的手机号之一

#手机号确定

淘宝 ID：6556psoul

#手机号确定，绑了上面当中的两个

多玩：dandingdeapeng

#绑定 QQ

请选择验证方式 **手机+身份验证**

您的手机号码： 若当前号码已不用/丢失，或无法收到验证码？[提示](#)

验证码

证件号码

💡 请输入实名认证的证件号码

下一步

不要着急，一会还有身份证号。

其陌陌号(QQ 邮箱注册，性别女)和照片：



别人都是约炮约妹子，帅哥约帅哥真是有创意。不玩就不玩了吧，还开着距离，找了个市中心的小伙，定位到了离广州 50 公里的市郊。

## 2.2 所受教育

广东工程技术职业学院官方网站存在诸多漏洞，同样作为网络安全工作者，希望你能把在网上喷人的时间拿出一点点放到修补学校网站漏洞上，别整天拿着啊 D 给这个修补给那个修补，学习要扎实，做事要认真。



姓名：陈勇鹏

所在院系：信息工程系

所在班别：普高2011电子信息工程技术(网络安全)1班

学号：2110205101026

辅导员：

2	检测环境的简介 .....	7
2.1	“中国菜刀”管理软件的介绍 .....	7
2.2	啊 D 注入工具介绍 .....	8
2.3	Brupsuite.....	8
2.4	WVS(Web Vulnerability Scanner).....	9
2.5	本章小结 .....	9
3	漏洞检测与修复环境的构建 .....	10
3.1	信息收集 .....	10
3.2	漏洞扫描与解析.....	11
3.3	本章小结 .....	22
4	漏洞修复方案建议 .....	23
4.1	学院分站点漏洞修复方案 .....	23
4.2	学院主站点漏洞修复方案 .....	23
4.3	学院图书馆网站漏洞修复方案.....	23

根据其学籍档案，就得到了更多的资料。

所属院系：信息工程系电子信息工程技术网络安全 1 班

高考准考证号：11440205101026，毕业证号：137091201406002467

家庭住址：广东省韶关市曲江区源河汇景 3 栋 1707(邮编 512100)

身份证号码：440221199209111656

就业去向：广东省信息安全测评中心

擅长：SQL 注入，ASP 代码审计，EWEB 编辑器漏洞，ASP 一句话管理，菜刀管理连接，内网嗅探。

顺便提一句，这些信息汇总以后，发现 12306 上面绑了 5 个人（坑队友坑室友啊!），以及一个网盘也能登陆。



放这么多 webshell 是想。。。？

## 2.3 如何格盘

万事俱备只欠东风，什么是东风？就是密码。常用密码 19\*\*\*1\*，还有几个常用密码，比如说 qwert, miemie..., psoul, 但是都没有上面这个“常”。

首先看到一个用来远控上线的花生壳 psoul1.eicp.net，账号 11197562，接下来获得了其 PC 的浏览器书签。

```

"专注网络安全", "guid": "p_tzJKLUX90", "id": 72, "index": 7, "parent": 3, "dateAdded": 1392699077613000, "lastModified": 1396581446318000, "an
"expires": 4, "value": "TOOLS - 低请求发展 - Discuz! Board"}, {"type": "text/x-moz-place", "uri": "https://www.t00ls.net/index.php"},
"探索网络安全", "guid": "hnOxFiOWt6n9", "id": 73, "index": 8, "parent": 3, "dateAdded": 1392813654970000, "lastModified": 1396581446319000, "an
"expires": 4, "value": "为网络安全爱好者们提供技术交流平台。"}, {"type": "text/x-moz-place", "uri": "http://www.9lri.org/", "charset": "UTF-
Engine", "guid": "H_9Krp3x-
q_n", "id": 74, "index": 9, "parent": 3, "dateAdded": 1392893020119000, "lastModified": 1396581446321000, "annos": [{"name": "bookmarkPropert
component(forum, e-shop, editor, e.g.) Search cyber device(temporarily closed)", "type": "text/x-moz-place", "uri": "http://www.zc
4.2.0 文档 - Beautiful Soup 4.2.0
documentation", "guid": "PIh3u2B6J2qs", "id": 75, "index": 10, "parent": 3, "dateAdded": 1394367848441000, "lastModified": 1396581446322000,
"flags": 0, "expires": 4, "value": ""}], {"type": "text/x-moz-place", "uri": "http://www.crummy.com/software/BeautifulSoup/bs4/doc/index.2
8"}, {"title": "XSS'OR", "guid": "cko3a8qsihs4", "id": 76, "index": 11, "parent": 3, "dateAdded": 1395146951145000, "lastModified": 1396581446
"flags": 0, "expires": 4, "value": ""}], {"type": "text/x-moz-place", "uri": "http://evilcos.me/lab/xssor/", "charset": "gbk"}, {"title": "快
documentation", "guid": "pP5jcgQ02ftr", "id": 77, "index": 12, "parent": 3, "dateAdded": 1395562836855000, "lastModified": 1396581446326000,
"flags": 0, "expires": 4, "value": ""}], {"type": "text/x-moz-place", "uri": "http://cn.python-requests.org/en/latest/user/quickstart.html
最新漏洞 | 漏洞预报 | 漏洞工具 | 溢出利用-
漏洞预报, EXPLOIT", "guid": "xdq4MZ_OQzAo", "id": 78, "index": 13, "parent": 3, "dateAdded": 1395821470537000, "lastModified": 13965814463270
"flags": 0, "expires": 4, "value": "非安全中国网-漏洞预报, EXPLOIT, 提供安全相关的系统漏洞, WEB程序漏洞等相关漏洞信息及利用工具"}, {"type": "t
place", "uri": "http://www.sitedirsec.com/", "charset": "gbk"}, {"title": "第三章
视图和URL配置", "guid": "86cCOR81wf22", "id": 79, "index": 14, "parent": 3, "dateAdded": 1396408770956000, "lastModified": 1396581446329000,
"expires": 4, "value": ""}], {"type": "text/x-moz-place", "uri": "http://djangobook.py3k.cn/2.0/chapter03/", "charset": "UTF-
8"}, {"title": "爱淘宝", "guid": "H4hMJ6ROVYVI", "id": 80, "index": 15, "parent": 3, "dateAdded": 1396529874152000, "lastModified": 1396529874
place", "uri": "http://ai.taobao.com/?pid=mm.28347190.2425761.20444747", "keyword": "mozen:toolbar:taobao"}, {"title": "palm-la.com下
站长帮手网", "guid": "sDMWMy4eYhTF", "id": 81, "index": 16, "parent": 3, "dateAdded": 1397028958980000, "lastModified": 1397028960810000, "an
"expires": 4, "value": "站长帮手网-二级域名查询工具, 可以查看域名palm-la.com下所有二级域名, 子域名, 同时可以查看这些网站的百度收录和PR值。
place", "uri": "http://i.links.cn/subdomain/", "charset": "gbk"}], {"title": "标签", "guid": "CRpNexqNMdsk", "id": 4, "index": 3, "parent": 1
"lastModified": 1396575767985000, "type": "text/x-moz-place-container", "root": "tagsFolder", "children": []}, {"title": "未分类书签", "gu
kwPw", "id": 15, "index": 4, "parent": 1, "dateAdded": 1396575767985000, "lastModified": 13965814463218000, "type": "text/x-moz-place-containe

```

好了，激动人心的时刻就要到来了。



既然 Mr.Chen 欢迎大家给他格盘，那么先看看他的博客解析的地址是：

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\>ping psoul.me

正在 Ping psoul.me [23.224.27.108] 具有 32 字节的数据:
来自 23.224.27.108 的回复: 字节=32 时间=258ms TTL=113
来自 23.224.27.108 的回复: 字节=32 时间=237ms TTL=113
来自 23.224.27.108 的回复: 字节=32 时间=237ms TTL=113
来自 23.224.27.108 的回复: 字节=32 时间=237ms TTL=113

23.224.27.108 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 237ms, 最长 = 258ms, 平均 = 242ms
```

ip 虽然不是国内的，但是应该是国内的运营商租的。原因很简单，因为登陆上去了。



睿驰科技  
Rich Technology

用户中心首页  
账户资料管理  
账务管理与充值  
管理我的产品服务  
管理我的所有服务  
我的[VPS主机]  
我的[虚拟主机]  
我的[服务器租用]  
购买新的产品服务  
帐户升级享受优惠  
推介下线链接赚钱  
安全退出系统

管理我的VPS云主机 #988

VPS云主机信息：

编号名称：	#988(MyServer)
服务器节点：	洛杉矶G口 BV
操作系统：	Windows 2003 <a href="#">重装系统</a> <a href="#">备份/还原</a> <a href="#">光源管理</a>
主IP地址：	23.224.27.108 <a href="#">管理/添加IP地址</a>
VPS主机配置：	CPU : 2 CPUs 内存 : 1024 M 硬盘 : 20 G 端口 : 1000 M 流量 : 500 G <a href="#">升级配置</a>
流量使用情况：	Checking.....
资源状态图表：	<a href="#">CPU使用率</a> <a href="#">内存状态</a> <a href="#">磁盘I/O</a> <a href="#">网络流量</a>
VPS主机价格：	41 RMB / 1个月 帐户余额 : 0.00 RMB
到期续费日期：	2014-8-4 (请确保在日期前帐户余额充足) <input type="checkbox"/> 自动续费 <a href="#">马上续费</a>
VPS主机状态：	Checking.....
VPS管理操作：	<a href="#">(软)重启</a> <a href="#">(软)关机</a> <a href="#">开机</a> <a href="#">(硬)重启</a> <a href="#">(硬)关机</a> <a href="#">网卡控制</a>
VPS操作提示：	如果(软)操作无效,请使用(硬)操作。注意:在(硬)重启或(硬)关机之前,请先保存好相关数据!
VPS默认密码：	默认管理帐号: Windows: Administrator Linux: root 初始密码: <a href="#">查看</a> <a href="#">重置</a>

纠结一下，是格，还是不格？

### 写在最后：

安全是把双刃剑，可以做白的也可以做黑的，很遗憾，习科是白方，正规的安全厂商，对不起让你失望了。满嘴跑火车不是没有能力搞你，而是为什么要搞你。这句话顺便警告一些其他的喷子。

习科踏踏实实做技术，努力为国家网络安全做建设，你敬我一尺我敬你一丈，你给我一刀我砍你三刀。



本来 7-9 下午都到了你们单位门口想约你出来聊聊，想想还是不计较了。

//Silic.Org