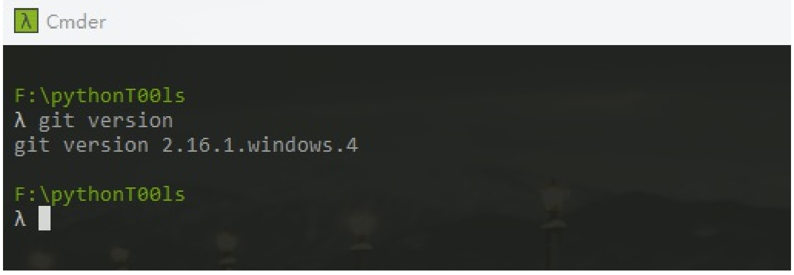
w9scan 使用介绍

w9scan是一款全能型的网站漏洞扫描器，借鉴了各位前辈的优秀代码。内置1200+插件可对网站进行一次规模的检测，功能包括但不限于web指纹检测、端口指纹检测、网站结构分析、各种流行的漏洞检测、爬虫以及SQL注入检测、XSS检测等等，w9scan会自动生成精美HTML格式结果报告。
基于python2.7，可以运行在Windows以及Linux系统上。下面教大家如何使用。

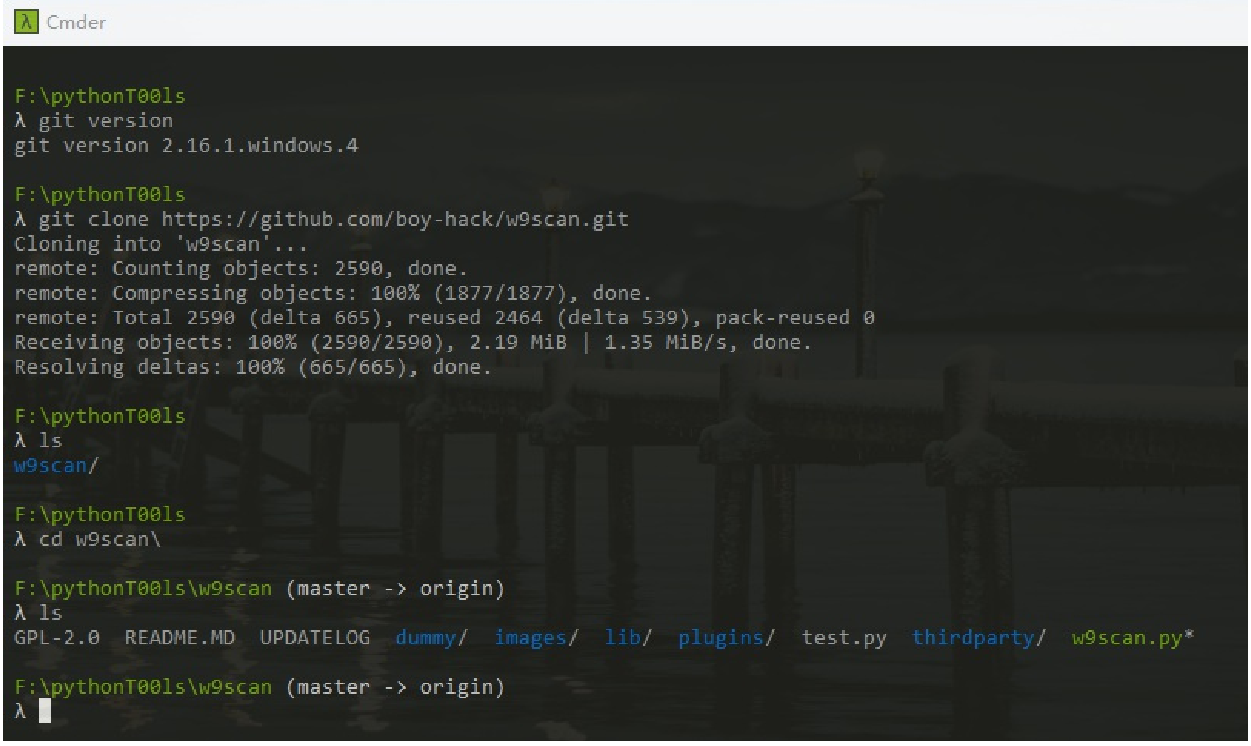
下载

笔者使用的系统是win10,使用的命令行工具是`cmder`。当然，使用系统自带的命令行工具也是可以的，但是没有git可用，推荐cmder的原因是cmder完整版会自带git，这个会为下载以及后面的更新提供很大帮助。
输入git version 出现下面信息则说明git命令可用.



```
F:\pythonT00ls
λ git version
git version 2.16.1.windows.4

F:\pythonT00ls
λ
```

然后输入 git clone https://github.com/boy-hack/w9scan.git 下载工具

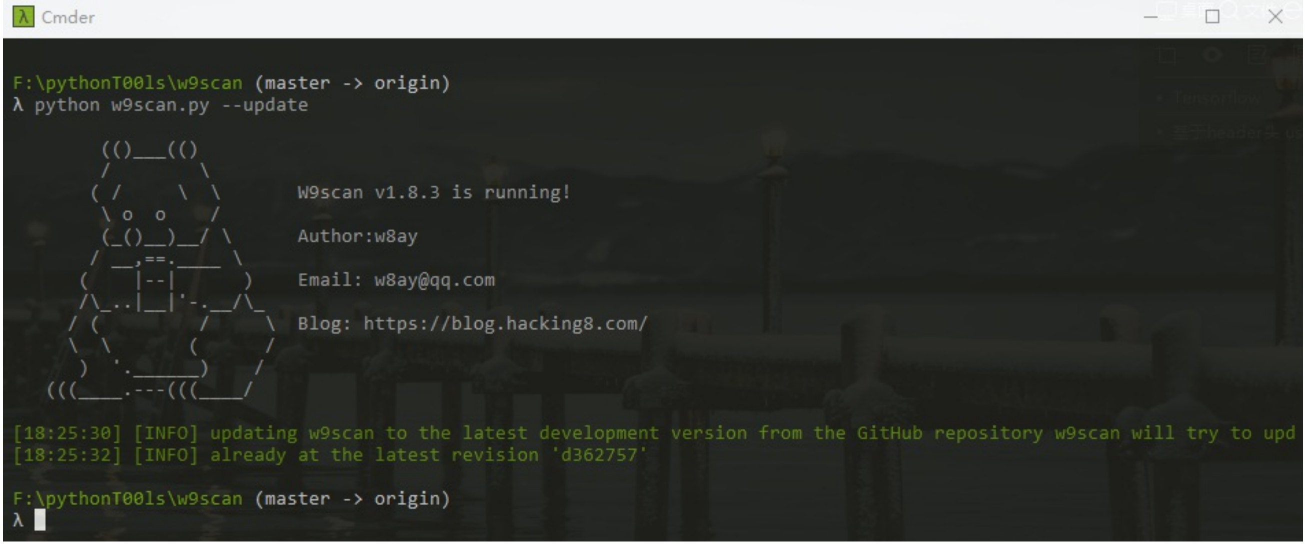


```
F:\pythonT00ls
λ git version
git version 2.16.1.windows.4

F:\pythonT00ls
λ git clone https://github.com/boy-hack/w9scan.git
Cloning into 'w9scan'...
remote: Counting objects: 2590, done.
remote: Compressing objects: 100% (1877/1877), done.
remote: Total 2590 (delta 665), reused 2464 (delta 539), pack-reused 0
Receiving objects: 100% (2590/2590), 2.19 MiB | 1.35 MiB/s, done.
Resolving deltas: 100% (665/665), done.

F:\pythonT00ls
λ ls
w9scan/

F:\pythonT00ls
λ cd w9scan\

F:\pythonT00ls\w9scan (master -> origin)
λ ls
GPL-2.0  README.MD  UPDATELOG  dummy/  images/  lib/  plugins/  test.py  thirdparty/  w9scan.py*

F:\pythonT00ls\w9scan (master -> origin)
λ
```

下载完毕后进入到w9scan目录即可。因为w9scan是不依赖任何第三方python库的，所以我们不需要额外的设置，这点是比较好的。

使用

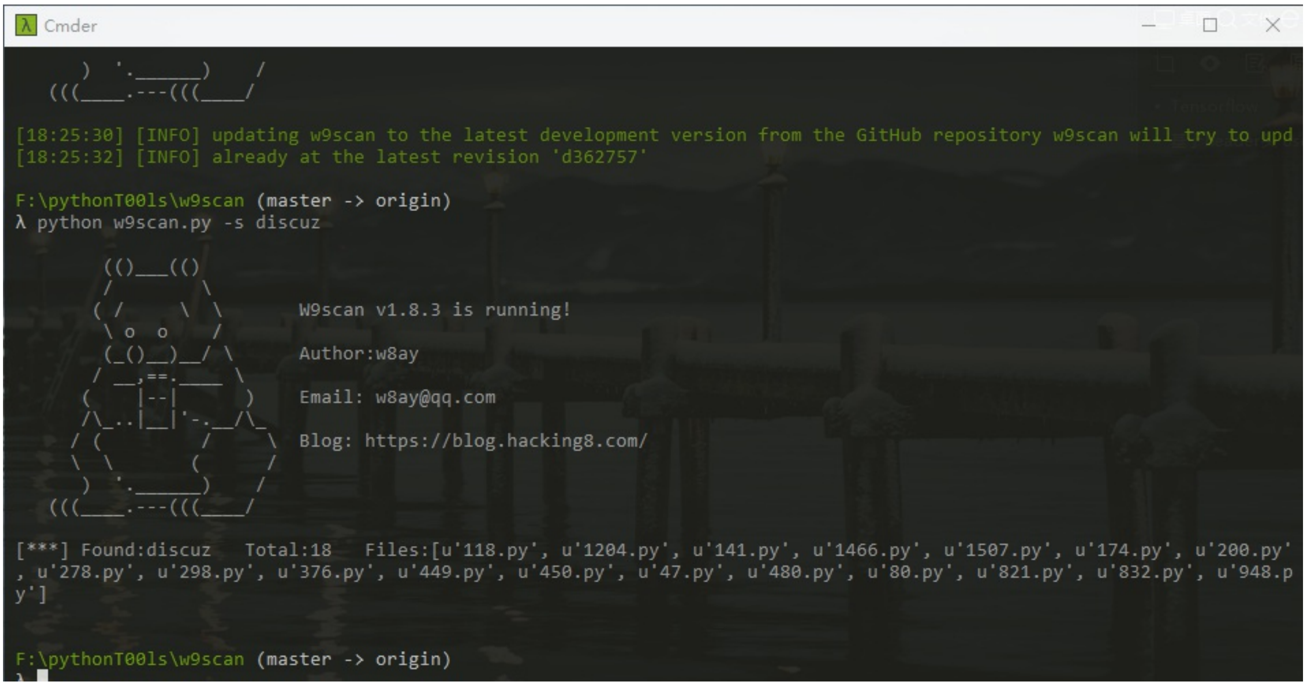
我们先试试它的更新功能，因为w9scan还在不断更新，所以我们运行之前可以输入 python w9scan.py --update 来更新。
注意：更新是基于git命令更新的所以需要git在环境变量中，这也是我推荐使用cmder的原因



```
F:\pythonT00ls\w9scan (master -> origin)
λ python w9scan.py --update

        (()___(()
        /         \
       ( /     \  \       W9scan v1.8.3 is running!
        \ o  o    /
        (_()__)__/ \      Author:w8ay
       /  __,==.____  \
      (     |--|       )   Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (         /      \  Blog: https://blog.hacking8.com/
     \  \       (       /
      )  '.______)     /
   (((____.---(((____/

[18:25:30] [INFO] updating w9scan to the latest development version from the GitHub repository w9scan will try to upd
[18:25:32] [INFO] already at the latest revision 'd362757'

F:\pythonT00ls\w9scan (master -> origin)
λ
```

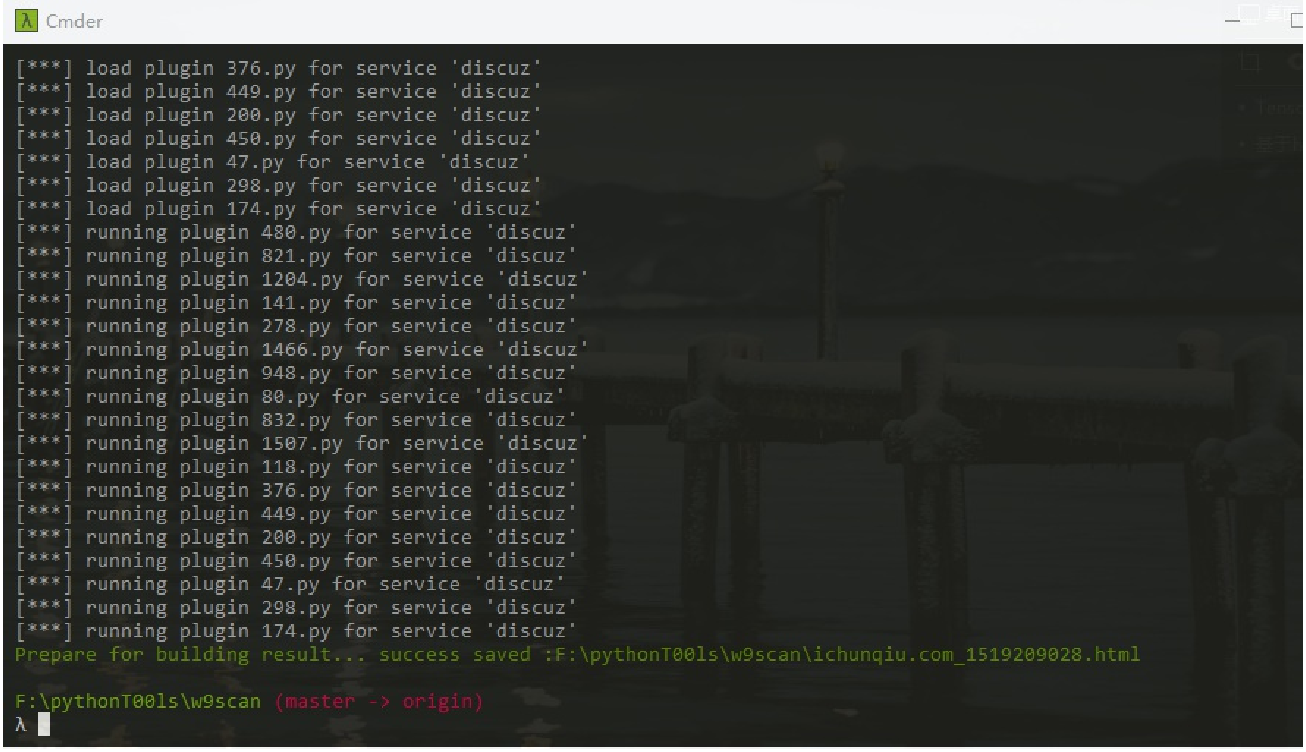
插件扫描

因为w9scan自带1200+插件，有时候我们只需要使用部分插件即可。比如我们要扫描https://bbs.ichunqiu.com/ 而且知道https://bbs.ichunqiu.com/的网站系统是discuz，我们先查找一下此插件 python w9scan.py -s discuz



```
      )  '.______)     /
   (((____.---(((____/

[18:25:30] [INFO] updating w9scan to the latest development version from the GitHub repository w9scan will try to upd
[18:25:32] [INFO] already at the latest revision 'd362757'

F:\pythonT00ls\w9scan (master -> origin)
λ python w9scan.py -s discuz

        (()___(()
        /         \
       ( /     \  \       W9scan v1.8.3 is running!
        \ o  o    /
        (_()__)__/ \      Author:w8ay
       /  __,==.____  \
      (     |--|       )   Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (         /      \  Blog: https://blog.hacking8.com/
     \  \       (       /
      )  '.______)     /
   (((____.---(((____/

[***] Found:discuz   Total:18   Files:[u'118.py', u'1204.py', u'141.py', u'1466.py', u'1507.py', u'174.py', u'200.py'
, u'278.py', u'298.py', u'376.py', u'449.py', u'450.py', u'47.py', u'480.py', u'80.py', u'821.py', u'832.py', u'948.p
y']


F:\pythonT00ls\w9scan (master -> origin)
```

得到结果，有18个相关可以扫描，然后便可以使用 python w9scan.py -u https://bbs.ichunqiu.com/ -p discuz 来指定扫描了

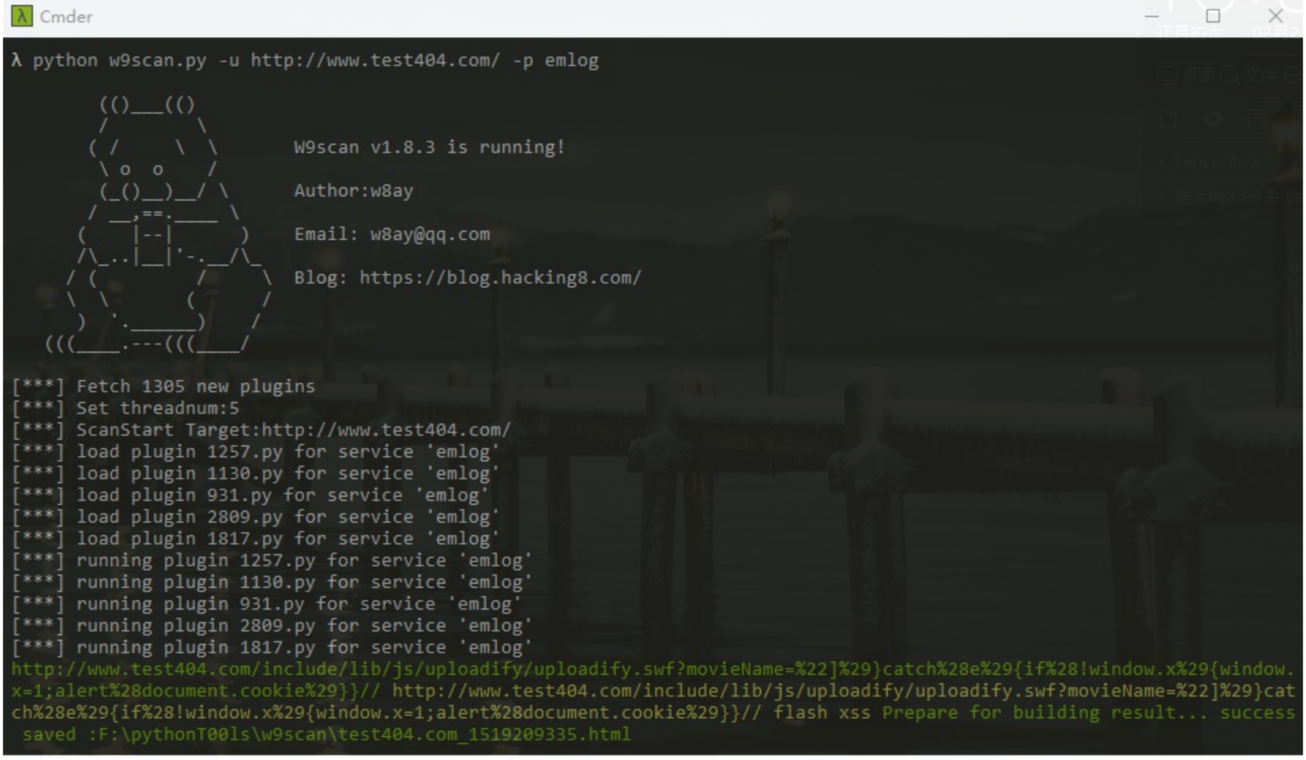


```
[***] load plugin 376.py for service 'discuz'
[***] load plugin 449.py for service 'discuz'
[***] load plugin 200.py for service 'discuz'
[***] load plugin 450.py for service 'discuz'
[***] load plugin 47.py for service 'discuz'
[***] load plugin 298.py for service 'discuz'
[***] load plugin 174.py for service 'discuz'
[***] running plugin 480.py for service 'discuz'
[***] running plugin 821.py for service 'discuz'
[***] running plugin 1204.py for service 'discuz'
[***] running plugin 141.py for service 'discuz'
[***] running plugin 278.py for service 'discuz'
[***] running plugin 1466.py for service 'discuz'
[***] running plugin 948.py for service 'discuz'
[***] running plugin 80.py for service 'discuz'
[***] running plugin 832.py for service 'discuz'
[***] running plugin 1507.py for service 'discuz'
[***] running plugin 118.py for service 'discuz'
[***] running plugin 376.py for service 'discuz'
[***] running plugin 449.py for service 'discuz'
[***] running plugin 200.py for service 'discuz'
[***] running plugin 450.py for service 'discuz'
[***] running plugin 47.py for service 'discuz'
[***] running plugin 298.py for service 'discuz'
[***] running plugin 174.py for service 'discuz'
Prepare for building result... success saved :F:\pythonT00ls\w9scan\ichunqiu.com_1519209028.html

F:\pythonT00ls\w9scan (master -> origin)
λ
```

扫描完毕，生成了html格式的网页，但是并没有扫到什么东西，说明discuz之前的漏洞以及修复了。

以此内推我们可以扫描其他网站试试

扫描一个博客，发现存在一个xss漏洞



```
λ python w9scan.py -u http://www.test404.com/ -p emlog

        (()___(()
        /         \
       ( /      \  \       W9scan v1.8.3 is running!
        \ o  o     /
        (_()__)__/ \       Author:w8ay
       /  __,==.____ \
      (     |--|      )    Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (         /     \   Blog: https://blog.hacking8.com/
     \  \       (      /
      )  '.______)    /
   (((____.---(((____/

[***] Fetch 1305 new plugins
[***] Set threadnum:5
[***] ScanStart Target:http://www.test404.com/
[***] load plugin 1257.py for service 'emlog'
[***] load plugin 1130.py for service 'emlog'
[***] load plugin 931.py for service 'emlog'
[***] load plugin 2809.py for service 'emlog'
[***] load plugin 1817.py for service 'emlog'
[***] running plugin 1257.py for service 'emlog'
[***] running plugin 1130.py for service 'emlog'
[***] running plugin 931.py for service 'emlog'
[***] running plugin 2809.py for service 'emlog'
[***] running plugin 1817.py for service 'emlog'
http://www.test404.com/include/lib/js/uploadify/uploadify.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.
x=1;alert%28document.cookie%29}}// http://www.test404.com/include/lib/js/uploadify/uploadify.swf?movieName=%22]%29}cat
ch%28e%29{if%28!window.x%29{window.x=1;alert%28document.cookie%29}}// flash xss Prepare for building result... success
 saved :F:\pythonT00ls\w9scan\test404.com_1519209335.html
```

在官方说明中也支持批量扫描 python w9scan.py -u "@1.txt" -p emlog

1.txt中存放扫描的url

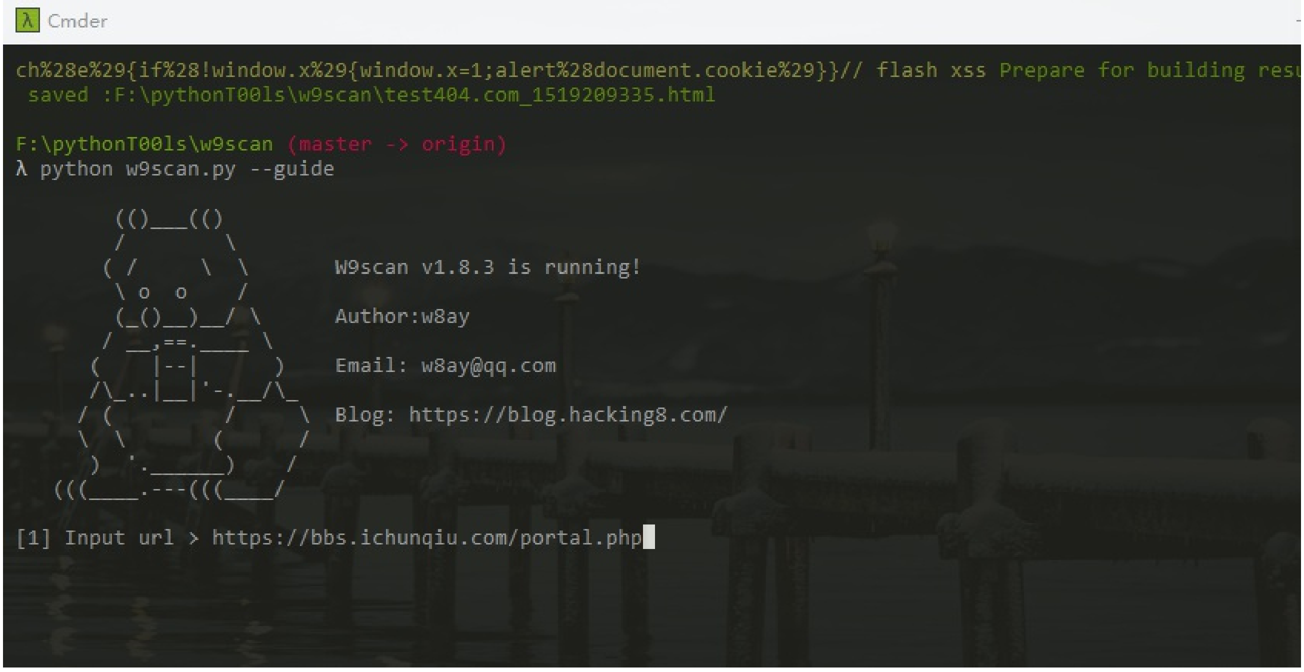
就不测试了。

全方位扫描

上面的扫描只是其中抽离出来的一小部分，现在使用w9scan最核心的部分对网站进行一次全面扫描吧

输入 python w9scan.py --guide 进入向导扫描模式，直接输入python w9scan.py 也是可以的

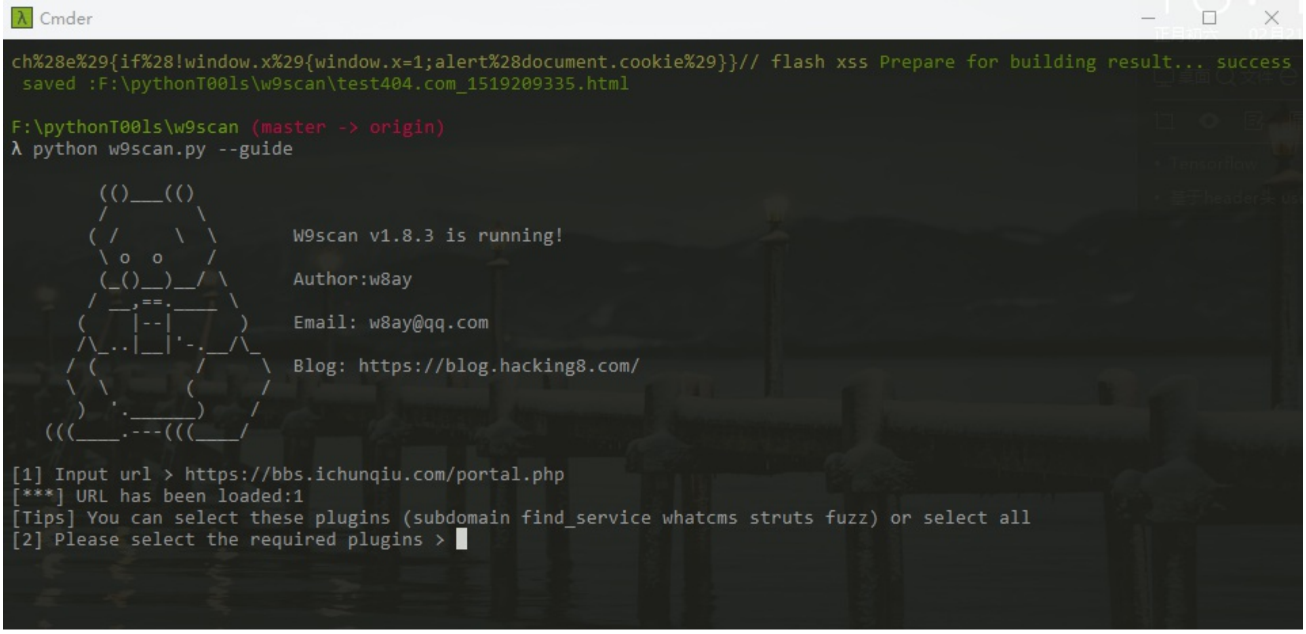
第一步输入url



```
ch%28e%29{if%28!window.x%29{window.x=1;alert%28document.cookie%29}}// flash xss Prepare for building resu
 saved :F:\pythonT00ls\w9scan\test404.com_1519209335.html

F:\pythonT00ls\w9scan (master -> origin)
λ python w9scan.py --guide

        (()___(()
        /        \
       ( /     \  \        W9scan v1.8.3 is running!
        \ o  o    /
        (_()__)__/ \       Author:w8ay
       /  __,==.____ \
      (     |--|      )    Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (        /      \   Blog: https://blog.hacking8.com/
     \  \      (       /
      )  '._______)   /
   (((____.---(((____/

[1] Input url > https://bbs.ichunqiu.com/portal.php
```

官方说明中也支持 @1.txt 的形式来批量扫描

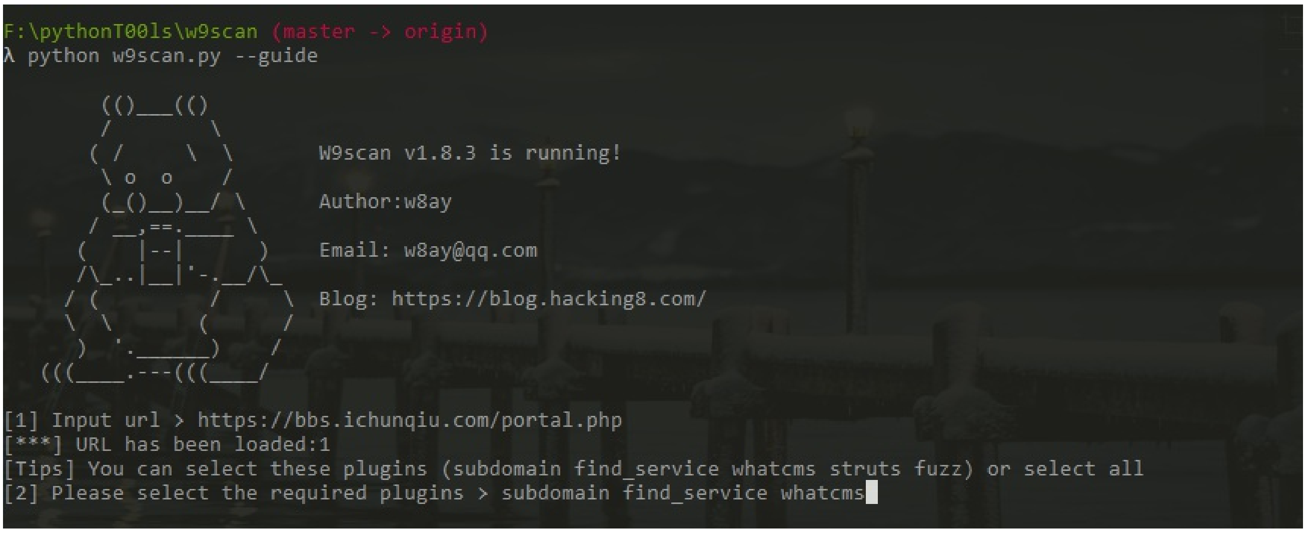
第二步选择插件



```
ch%28e%29{if%28!window.x%29{window.x=1;alert%28document.cookie%29}}// flash xss Prepare for building result... success
 saved :F:\pythonT00ls\w9scan\test404.com_1519209335.html

F:\pythonT00ls\w9scan (master -> origin)
λ python w9scan.py --guide

        (()___(()
        /        \
       ( /     \  \        W9scan v1.8.3 is running!
        \ o  o    /
        (_()__)__/ \       Author:w8ay
       /  __,==.____ \
      (     |--|      )    Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (        /      \   Blog: https://blog.hacking8.com/
     \  \      (       /
      )  '._______)   /
   (((____.---(((____/

[1] Input url > https://bbs.ichunqiu.com/portal.php
[***] URL has been loaded:1
[Tips] You can select these plugins (subdomain find_service whatcms struts fuzz) or select all
[2] Please select the required plugins >
```

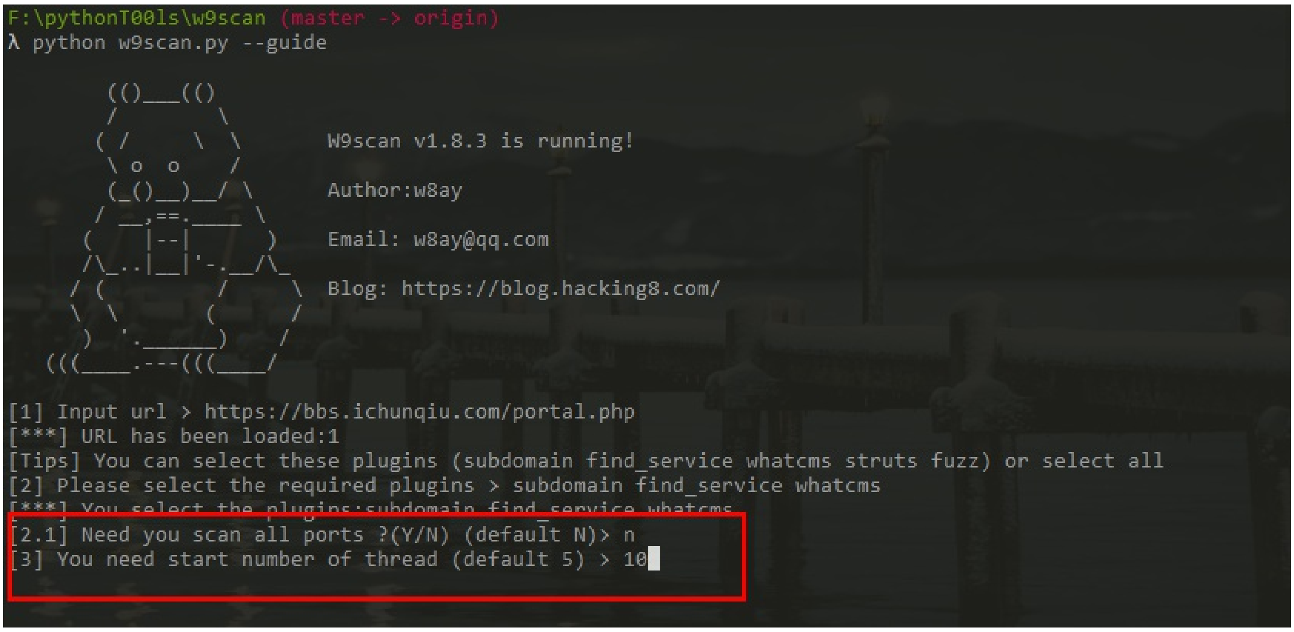
w9scan将部分插件抽离出来可以灵活的选择，比如这里我们可以选择 subdomain find_service whatcms struts fuzz 这么多插件，分别对应的是子域名扫描，端口服务扫描，网站指纹扫描/CMS识别，struts扫描，FUzz爆破

这里我们只需要子域名扫描 端口扫描 网站指纹扫描就行，如下填写即可。



```
F:\pythonT00ls\w9scan (master -> origin)
λ python w9scan.py --guide

        (()___(()
        /        \
       ( /     \  \        W9scan v1.8.3 is running!
        \ o  o    /
        (_()__)__/ \       Author:w8ay
       /  __,==.____ \
      (     |--|      )    Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (        /      \   Blog: https://blog.hacking8.com/
     \  \      (       /
      )  '._______)   /
   (((____.---(((____/

[1] Input url > https://bbs.ichunqiu.com/portal.php
[***] URL has been loaded:1
[Tips] You can select these plugins (subdomain find_service whatcms struts fuzz) or select all
[2] Please select the required plugins > subdomain find_service whatcms
```

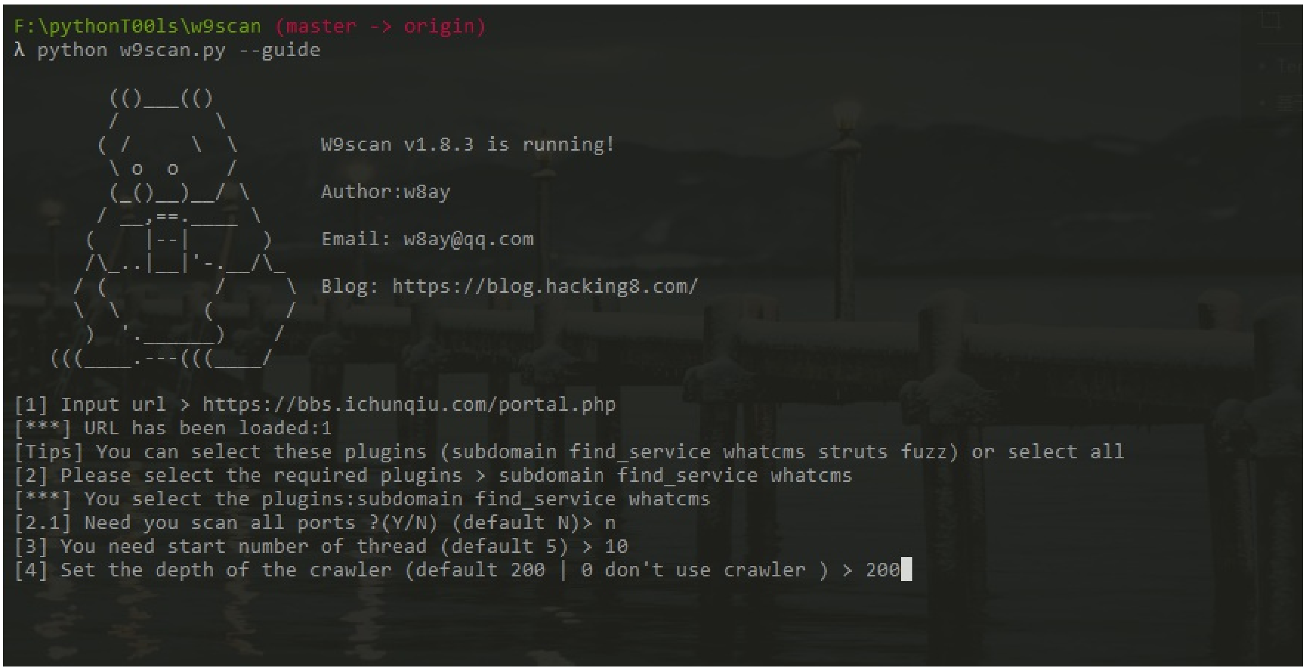
如果想全部扫描的话填写all即可



```
F:\pythonT00ls\w9scan (master -> origin)
λ python w9scan.py --guide

        (()___(()
        /        \
       ( /     \  \       W9scan v1.8.3 is running!
        \ o  o    /
        (_()__)__/ \      Author:w8ay
       / __,==.____ \
      (    |--|     )    Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (         /     \  Blog: https://blog.hacking8.com/
     \  \       (      /
      )   '._____)    /
   (((____.---(((____/

[1] Input url > https://bbs.ichunqiu.com/portal.php
[***] URL has been loaded:1
[Tips] You can select these plugins (subdomain find_service whatcms struts fuzz) or select all
[2] Please select the required plugins > subdomain find_service whatcms
[***] You select the plugins:subdomain find_service whatcms
[2.1] Need you scan all ports ?(Y/N) (default N)> n
[3] You need start number of thread (default 5) > 10
```

然后询问在扫描时候是否扫描全部端口，没必要太费时间了，我们选n，然后选择扫描线程，根据网站承受能力和自己电脑配置来定，这里选择10

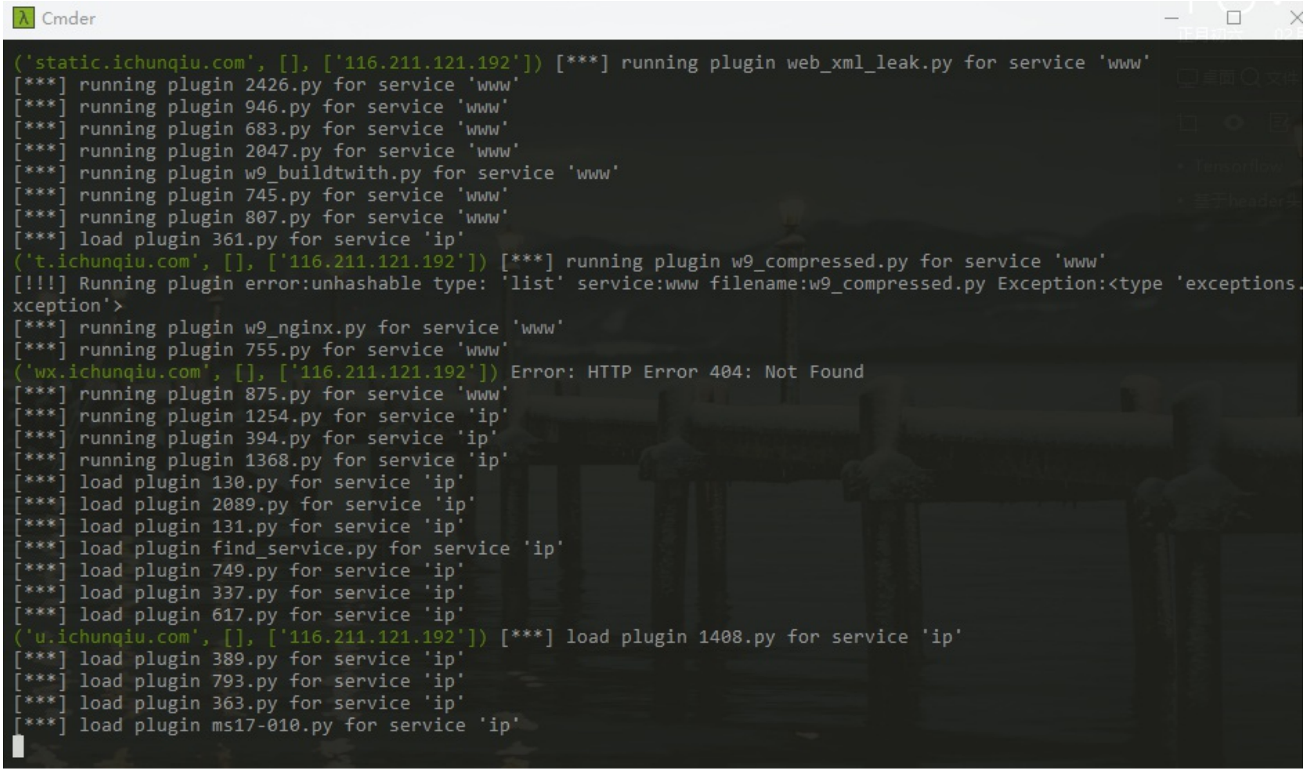
然后选择爬虫



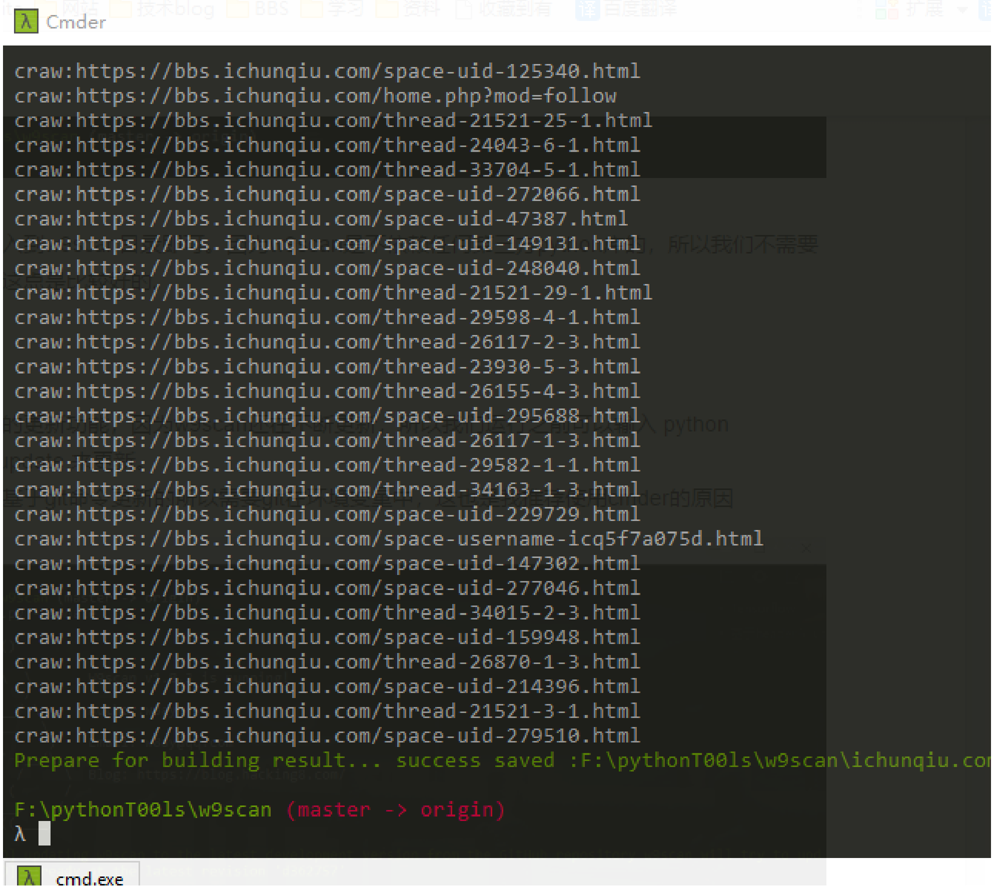
```
F:\pythonT00ls\w9scan (master -> origin)
λ python w9scan.py --guide

        (()___(()
        /        \
       ( /     \  \       W9scan v1.8.3 is running!
        \ o  o    /
        (_()__)__/ \      Author:w8ay
       / __,==.____ \
      (    |--|     )    Email: w8ay@qq.com
      /\_..|__|'-.__/\_
     / (         /     \  Blog: https://blog.hacking8.com/
     \  \       (      /
      )   '._____)    /
   (((____.---(((____/

[1] Input url > https://bbs.ichunqiu.com/portal.php
[***] URL has been loaded:1
[Tips] You can select these plugins (subdomain find_service whatcms struts fuzz) or select all
[2] Please select the required plugins > subdomain find_service whatcms
[***] You select the plugins:subdomain find_service whatcms
[2.1] Need you scan all ports ?(Y/N) (default N)> n
[3] You need start number of thread (default 5) > 10
[4] Set the depth of the crawler (default 200 | 0 don't use crawler ) > 200
```

0是不使用爬虫，大于0则是爬虫的深度，默认即可。

然后便开始了扫描。

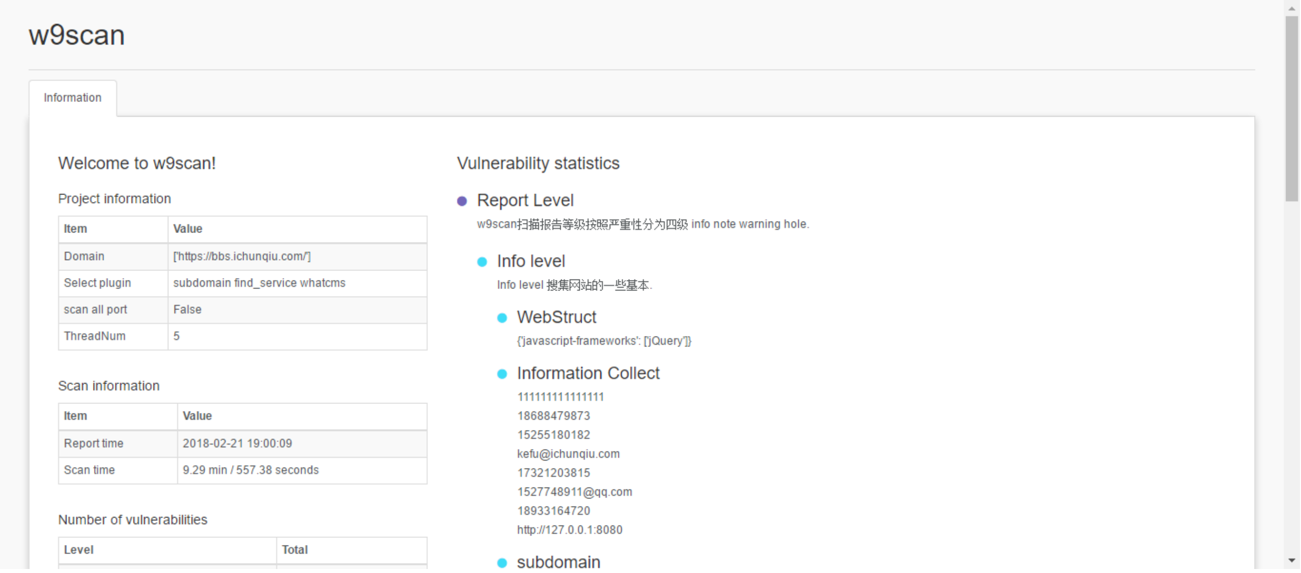


```
('static.ichunqiu.com', [], ['116.211.121.192']) [***] running plugin web_xml_leak.py for service 'www'
[***] running plugin 2426.py for service 'www'
[***] running plugin 946.py for service 'www'
[***] running plugin 683.py for service 'www'
[***] running plugin 2047.py for service 'www'
[***] running plugin w9_buildtwith.py for service 'www'
[***] running plugin 745.py for service 'www'
[***] running plugin 807.py for service 'www'
[***] load plugin 361.py for service 'ip'
('t.ichunqiu.com', [], ['116.211.121.192']) [***] running plugin w9_compressed.py for service 'www'
[!!!] Running plugin error:unhashable type: 'list' service:www filename:w9_compressed.py Exception:<type 'exceptions.
xception'>
[***] running plugin w9_nginx.py for service 'www'
[***] running plugin 755.py for service 'www'
('wx.ichunqiu.com', [], ['116.211.121.192']) Error: HTTP Error 404: Not Found
[***] running plugin 875.py for service 'www'
[***] running plugin 1254.py for service 'ip'
[***] running plugin 394.py for service 'ip'
[***] running plugin 1368.py for service 'ip'
[***] load plugin 130.py for service 'ip'
[***] load plugin 2089.py for service 'ip'
[***] load plugin 131.py for service 'ip'
[***] load plugin find_service.py for service 'ip'
[***] load plugin 749.py for service 'ip'
[***] load plugin 337.py for service 'ip'
[***] load plugin 617.py for service 'ip'
('u.ichunqiu.com', [], ['116.211.121.192']) [***] load plugin 1408.py for service 'ip'
[***] load plugin 389.py for service 'ip'
[***] load plugin 793.py for service 'ip'
[***] load plugin 363.py for service 'ip'
[***] load plugin ms17-010.py for service 'ip'
```



```
craw:https://bbs.ichunqiu.com/space-uid-125340.html
craw:https://bbs.ichunqiu.com/home.php?mod=follow
craw:https://bbs.ichunqiu.com/thread-21521-25-1.html
craw:https://bbs.ichunqiu.com/thread-24043-6-1.html
craw:https://bbs.ichunqiu.com/thread-33704-5-1.html
craw:https://bbs.ichunqiu.com/space-uid-272066.html
craw:https://bbs.ichunqiu.com/space-uid-47387.html
craw:https://bbs.ichunqiu.com/space-uid-149131.html
craw:https://bbs.ichunqiu.com/space-uid-248040.html
craw:https://bbs.ichunqiu.com/thread-21521-29-1.html
craw:https://bbs.ichunqiu.com/thread-29598-4-1.html
craw:https://bbs.ichunqiu.com/thread-26117-2-3.html
craw:https://bbs.ichunqiu.com/thread-23930-5-3.html
craw:https://bbs.ichunqiu.com/thread-26155-4-3.html
craw:https://bbs.ichunqiu.com/space-uid-295688.html
craw:https://bbs.ichunqiu.com/thread-26117-1-3.html
craw:https://bbs.ichunqiu.com/thread-29582-1-1.html
craw:https://bbs.ichunqiu.com/thread-34163-1-3.html
craw:https://bbs.ichunqiu.com/space-uid-229729.html
craw:https://bbs.ichunqiu.com/space-username-icq5f7a075d.html
craw:https://bbs.ichunqiu.com/space-uid-147302.html
craw:https://bbs.ichunqiu.com/space-uid-277046.html
craw:https://bbs.ichunqiu.com/thread-34015-2-3.html
craw:https://bbs.ichunqiu.com/space-uid-159948.html
craw:https://bbs.ichunqiu.com/thread-26870-1-3.html
craw:https://bbs.ichunqiu.com/space-uid-214396.html
craw:https://bbs.ichunqiu.com/thread-21521-3-1.html
craw:https://bbs.ichunqiu.com/space-uid-279510.html
Prepare for building result... success saved :F:\pythonT00ls\w9scan\ichunqiu.co

F:\pythonT00ls\w9scan (master -> origin)
λ
```

最后生成的扫描结果



w9scan

Welcome to w9scan!

Project information

Item	Value
Domain	['https://bbs.ichunqiu.com/']
Select plugin	subdomain find_service whatcms
scan all port	False
ThreadNum	5

Scan information

Item	Value
Report time	2018-02-21 19:00:09
Scan time	9.29 min / 557.38 seconds

Number of vulnerabilities

Level	Total

Vulnerability statistics

- Report Level

  w9scan扫描报告等级按照严重性分为四级 info note warning hole.

  - Info level

    Info level 搜集网站的一些基本.

    - WebStruct

      {'javascript-frameworks': ['jQuery']}

    - Information Collect

      1111111111111
      18688479873
      15255180182
      kefu@ichunqiu.com
      17321203815
      1527748911@qq.com
      18933164720
      http://127.0.0.1:8080

    - subdomain