Gobuster

gob uster v 3 . 0 . 1(OJ Reeves @ the Colonial)

Gobuster是一个用于暴力的工具:

网站中的URIs(目录和文件)。
域名系统子域(带通配符支持)。
目标网络服务器上的虚拟主机名称。

标签、状态等

在开放集体上建立身份支持者
哦，天哪..为什么！？

因为我想:

...一些没有强大的Java图形用户界面的东西。
...来构建只在命令行上有效的东西。
...没有递归暴力的东西。
...这让我可以一次破解文件夹和多个扩展。
...在多个平台上编译成本机的东西。
...比解释脚本(如Python)更快的东西。
...不需要运行时的东西。
...使用对并发性有好处的东西(因此使用)。
...去建造一些并非完全无用的东西。

但这是狗屎！你的实现糟透了！

是的，你可能是对的。请随意:

不要用它。
告诉我如何做得更好。

喜欢这个工具吗？退后。

如果你已经支持我们了，你就太棒了。如果你不是，那也很酷！想支持我们吗？成为支持者！

Backers

所有捐赠给这个项目的资金都将捐赠给慈善机构。慈善捐赠的完整日志将在处理过程中在此存储库中提供。

——*OJ Reeves (@TheColonial) & Christian Mehlmauer (*@FireFart*)*

来自 https://github.com/OJ/gobuster

一，官方帮助手册

可用命令:
dir使用目录/文件强制模式
dns使用dns子域bruteforce模式
帮助帮助任何命令
vhost使用vhost bruteforce模式

国旗:
-帮我帮哥们儿
-z，——无进步不显示进步
-o，——输出字符串输出文件写入结果(默认为stdout)
不要打印横幅和其他噪音
线程数int并发线程数(默认为10)
-v，——详细的详细输出(错误)
-w，——wordlist字符串路径到wordlist

使用“gobuster[命令]——帮助”来获得更多关于命令的信息。

Available Commands:
  dir   Uses directory/file brutceforcing mode
  dns   Uses DNS subdomain bruteforcing mode
  help   Help about any command
  vhost   Uses VHOST bruteforcing mode

Flags:
  -h, --help   help for gobuster
  -z, --noprogress   Don't display progress
  -o, --output string   Output file to write results to (defaults to stdout)
  -q, --quiet   Don't print the banner and other noise
  -t, --threads int   Number of concurrent threads (default 10)
  -v, --verbose   Verbose output (errors)
  -w, --wordlist string Path to the wordlist

Use "gobuster [command] --help" for more information about a command.

二，命令实例

gobuster dns -d zsdk.org.cn -w 1.txt

使用DNS 子域 bruteforcing模式，并使用单词列表字符串列表路径

```
┌──[root@parrot]─[/home/kun]
└─── #gobuster dns -d zsdk.org.cn -w 1.txt
=====================================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================================
[+] Domain:     zsdk.org.cn
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   1.txt
=====================================================================
2020/04/06 11:30:39 Starting gobuster
=====================================================================
=====================================================================
2020/04/06 11:30:41 Finished
=====================================================================
```

gobuster dir -u zsdk.org.cn -w 1.txt

使用dir 目录 brutceforcing模式

```
┌──[✗]─[root@parrot]─[/home/kun]
└─── #gobuster dir -u zsdk.org.cn -w 1.txt
=====================================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================================
[+] Url:            http://zsdk.org.cn
[+] Threads:        10
[+] Wordlist:       1.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
=====================================================================
2020/04/06 11:38:34 Starting gobuster
=====================================================================
=====================================================================
2020/04/06 11:38:34 Finished
=====================================================================
```

gobuster dns -d zsdk.org.cn -t 1000 -w 1.txt

使用dns模型线程数（-t）为1000[^默认为10]

```
└─── #gobuster dns -d zsdk.org.cn -t 1000 -w 1.txt
=====================================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================================
[+] Domain:     zsdk.org.cn
[+] Threads:    1000
[+] Timeout:    1s
[+] Wordlist:   1.txt
=====================================================================
2020/04/06 11:47:08 Starting gobuster
=====================================================================
=====================================================================
2020/04/06 11:47:10 Finished
=====================================================================
```

gobuster dns -d zsdk.org.cn -q -w 1.txt

扫描但不打印任何结果("-q")

```
#gobuster dns -d zsdk.org.cn -t 1000 -w 1.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Domain:     zsdk.org.cn
[+] Threads:    1000
[+] Timeout:    1s
[+] Wordlist:   1.txt
===============================================================
2020/04/06 11:47:08 Starting gobuster
===============================================================
===============================================================
2020/04/06 11:47:10 Finished
===============================================================
```

gobuster dns -d sogo.com -o sogo.txt -w 1.txt

将其结果输出至sogo.txt

```
#gobuster dns -d sogo.com -o sogo.txt -w 1.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Domain:     sogo.com
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   1.txt
===============================================================
2020/04/06 11:55:01 Starting gobuster
===============================================================
===============================================================
2020/04/06 11:55:03 Finished
===============================================================
```

```
#l
.txt          Desktop/    Downloads/  Pictures/  sogo.txt  Templates/  zsdk.txt
aidunetdisk/  Documents/  Music/      Public/    temp/     Videos/
-[root@parrot]-[/home/kun]
#
```

gobuster dns -d zsdk.org.cn -v -w 1.txt

详细输出

```
#gobuster dns -d zsdk.org.cn -v -w 1.txt
=====================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================
[+] Domain:     zsdk.org.cn
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   1.txt
[+] Verbose:    true
=====================================================
2020/04/06 11:58:47 Starting gobuster
=====================================================
Missed: qwertyuioplkjhgfdsazxcvbnmn.zsdk.org.cn
=====================================================
2020/04/06 11:58:48 Finished
=====================================================
```

gobuster vhost -u sogo.com -w 1

使用"vhost"粘性模式进行爆破

```
#gobuster vhost -u sogo.com -w 1
=====================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================
[+] Url:          http://sogo.com
[+] Threads:      10
[+] Wordlist:     1
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====================================================
2020/04/06 12:44:52 Starting gobuster
=====================================================
=====================================================
2020/04/06 12:44:53 Finished
=====================================================
```