

GoBuster

GoBuster scans the most common directories which are used on a WebApp / Website. To run this scan GoBuster needs to be installed first: **sudo apt-get install gobuster**

Once GoBuster is installed we can run it as following:

```
sudo gobuster dir -u http://<ip>:<port> -w /usr/share/wordlist/dirbuster/ -x php,sh.txt,cgi,html,js,css,py
```

GoBuster flag	Description
-e	Print the full URLs in your console
-u	The target URL
-w	Path to your wordlist
-U and -P	Username and Password for Basic Auth
-p <x>	Proxy to use for requests
-c <http cookies>	Specify a cookie for simulating your auth

<https://tools.kali.org/web-applications/gobuster>

After the run you see something like that:

```
root@llamasec:~# gobuster -u http://192.168.1.2/ -w /usr/share/wordlists/dirb/co
mmon.txt -fw

=====
Gobuster v2.0.1                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.2/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Timeout       : 10s
=====
2019/03/25 23:40:34 Starting gobuster
=====
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/cgi-bin/ (Status: 403)
/index.html (Status: 200)
/passwords (Status: 301)
/robots.txt (Status: 200)
=====
```

Revision #2

Created 9 July 2022 13:27:06 by Togoboi

Updated 10 July 2022 08:23:21 by Togoboi