Wfuzz

1. Introduction

WFuzz is a powerful web application fuzzing and enumeration tool. It's more flexible because you can fuzz any part of the HTTP request—URL, parameters, headers, cookies, POST data, JSON data, etc.

2. Basic directory fuzzing

- **Simple directory scan**

➔ **Command:** *wfuzz -c -u http://testphp.vulnweb.com/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt*

➔ **Description:** Replaces FUZZ with each word from the wordlist to discover hidden directories. We use -c for colored output so results are readable.

```
┌──(paxton㉿kali)-[~]
└─$ wfuzz -c -u http://testphp.vulnweb.com/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not wor
k correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://testphp.vulnweb.com/FUZZ
Total requests: 87664

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000031:   404        7 L      11 W       153 Ch      "logo"
000000007:   200        109 L    388 W      4958 Ch     "# license, visit http://creativecommons.org/licenses/by-sa/
                                                        3.0/"
000000034:   404        7 L      11 W       153 Ch      "10"
000000001:   200        109 L    388 W      4958 Ch     "# directory-list-2.3-small.txt"
000000033:   404        7 L      11 W       153 Ch      "new"
000000015:   404        7 L      11 W       153 Ch      "index"
000000003:   200        109 L    388 W      4958 Ch     "# Copyright 2007 James Fisher"
000000036:   404        7 L      11 W       153 Ch      "faq"
000000037:   404        7 L      11 W       153 Ch      "rss"
000000035:   403        9 L      28 W       276 Ch      "cgi-bin"
000000030:   404        7 L      11 W       153 Ch      "11"
000000029:   404        7 L      11 W       153 Ch      "privacy"
000000028:   404        7 L      11 W       153 Ch      "spacer"
000000027:   404        7 L      11 W       153 Ch      "search"
000000032:   404        7 L      11 W       153 Ch      "blog"
000000025:   404        7 L      11 W       153 Ch      "contact"
000000026:   404        7 L      11 W       153 Ch      "about"
000000024:   404        7 L      11 W       153 Ch      "12"
000000023:   404        7 L      11 W       153 Ch      "full"
000000022:   404        7 L      11 W       153 Ch      "warez"
000000021:   404        7 L      11 W       153 Ch      "serial"
000000020:   404        7 L      11 W       153 Ch      "crack"
000000019:   404        7 L      11 W       153 Ch      "news"
000000018:   404        7 L      11 W       153 Ch      "2006"
000000017:   404        7 L      11 W       153 Ch      "download"
000000014:   200        109 L    388 W      4958 Ch     "http://testphp.vulnweb.com/"
000000016:   301        7 L      11 W       169 Ch      "images"
000000013:   200        109 L    388 W      4958 Ch     "#"
```

3. Filtering results

- **Hide specific responses**

➔ **Command:** *wfuzz -c -u http://testphp.vulnweb.com/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --hc 404*

➔ **Description:** --hc hides unwanted status codes like 404 to reduce noise. This makes it easier to focus on valid directories that your server actually returns.

```
┌──(paxton㉿kali)-[~]
└─$ wfuzz -c -u http://testphp.vulnweb.com/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --hc 404
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might no
t work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://testphp.vulnweb.com/FUZZ
Total requests: 87664

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        109 L    388 W      4958 Ch     "# directory-list-2.3-small.txt"
000000003:   200        109 L    388 W      4958 Ch     "# Copyright 2007 James Fisher"
000000007:   200        109 L    388 W      4958 Ch     "# license, visit http://creativecommons.org/licenses/b
                                                        y-sa/3.0/"
000000035:   403        9 L      28 W       276 Ch      "cgi-bin"
000000014:   200        109 L    388 W      4958 Ch     "http://testphp.vulnweb.com/"
000000016:   301        7 L      11 W       169 Ch      "images"
000000005:   200        109 L    388 W      4958 Ch     "# This work is licensed under the Creative Commons"
000000012:   200        109 L    388 W      4958 Ch     "# on atleast 3 different hosts"
000000013:   200        109 L    388 W      4958 Ch     "#"
000000011:   200        109 L    388 W      4958 Ch     "# Priority ordered case sensative list, where entries
                                                        were found"
000000010:   200        109 L    388 W      4958 Ch     "#"
000000004:   200        109 L    388 W      4958 Ch     "#"
000000006:   200        109 L    388 W      4958 Ch     "# Attribution-Share Alike 3.0 License. To view a copy
                                                        of this"
000000008:   200        109 L    388 W      4958 Ch     "# or send a letter to Creative Commons, 171 Second Str
                                                        eet,"
000000009:   200        109 L    388 W      4958 Ch     "# Suite 300, San Francisco, California, 94105, USA."
000000002:   200        109 L    388 W      4958 Ch     "#"
000000259:   301        7 L      11 W       169 Ch      "admin"
000000466:   301        7 L      11 W       169 Ch      "pictures"
000001480:   301        7 L      11 W       169 Ch      "vendor"
000002281:   301        7 L      11 W       169 Ch      "Templates"
```

- **Show Only Specific Status Codes**

➔ **Command:** *wfuzz -c -u http://testphp.vulnweb.com/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --sc 200,301*

➔ **Description:** --sc shows only matching status codes, helping you filter for “real” directories or redirects.

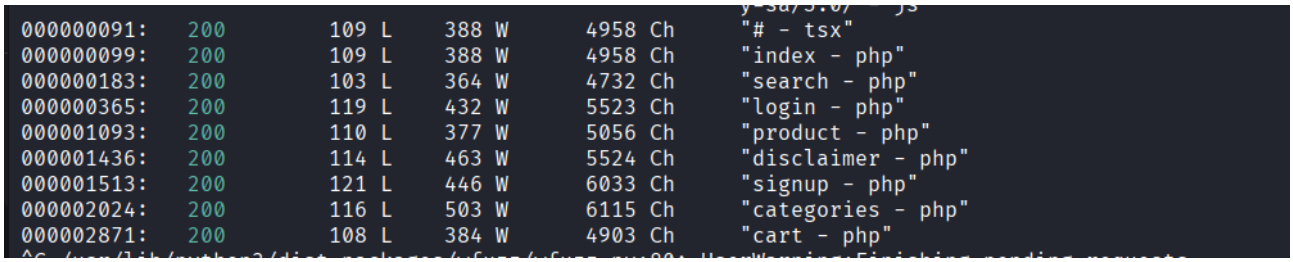
```
┌──(paxton㉿kali)-[~]
└─$ wfuzz -c -u http://testphp.vulnweb.com/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --sc 200,
301
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might no
t work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://testphp.vulnweb.com/FUZZ
Total requests: 87664

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        109 L    388 W      4958 Ch     "# directory-list-2.3-small.txt"
000000007:   200        109 L    388 W      4958 Ch     "# license, visit http://creativecommons.org/licenses/b
                                                        y-sa/3.0/"
000000003:   200        109 L    388 W      4958 Ch     "# Copyright 2007 James Fisher"
000000016:   301        7 L      11 W       169 Ch      "images"
000000014:   200        109 L    388 W      4958 Ch     "http://testphp.vulnweb.com/"
000000013:   200        109 L    388 W      4958 Ch     "#"
000000002:   200        109 L    388 W      4958 Ch     "#"
000000004:   200        109 L    388 W      4958 Ch     "#"
000000005:   200        109 L    388 W      4958 Ch     "# This work is licensed under the Creative Commons"
000000010:   200        109 L    388 W      4958 Ch     "#"
000000012:   200        109 L    388 W      4958 Ch     "# on atleast 3 different hosts"
000000009:   200        109 L    388 W      4958 Ch     "# Suite 300, San Francisco, California, 94105, USA."
000000011:   200        109 L    388 W      4958 Ch     "# Priority ordered case sensative list, where entries
                                                        were found"
000000006:   200        109 L    388 W      4958 Ch     "# Attribution-Share Alike 3.0 License. To view a copy
                                                        of this"
000000008:   200        109 L    388 W      4958 Ch     "# or send a letter to Creative Commons, 171 Second Str
                                                        eet,"
000000259:   301        7 L      11 W       169 Ch      "admin"
000000466:   301        7 L      11 W       169 Ch      "pictures"
000001480:   301        7 L      11 W       169 Ch      "vendor"
000002281:   301        7 L      11 W       169 Ch      "Templates"
```

4. File extension brute force

- **File extension brute force**

➔ **Command:** *wfuzz -c -u http://testphp.vulnweb.com/FUZZ.FUZ2Z -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -w extensions.txt --sc 200,301*

➔ **Description:** This allows fuzzing both filename and extension by using two wordlists (FUZZ and FUZZ2). Useful for discovering hidden files such as admin.php or backup.txt.



5. Fuzzing parameter and post data

- **Fuzzing query parameter**

➔ **Command:** *wfuzz -c -w wordlist.txt http://yourlab.com/page.php?user=FUZZ*

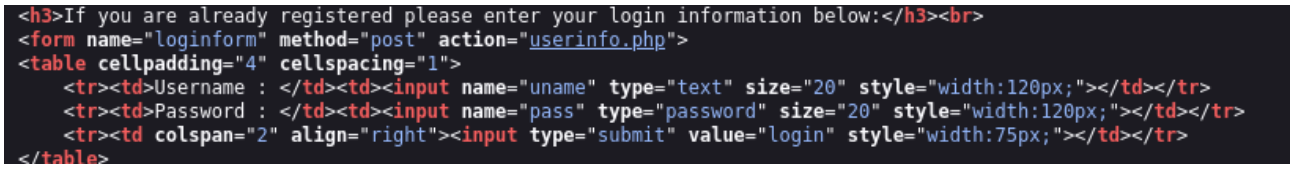
➔ **Description:** Replaces the GET parameter value with each payload from the wordlist. Used to test for parameter discovery, error messages, or unexpected behavior.

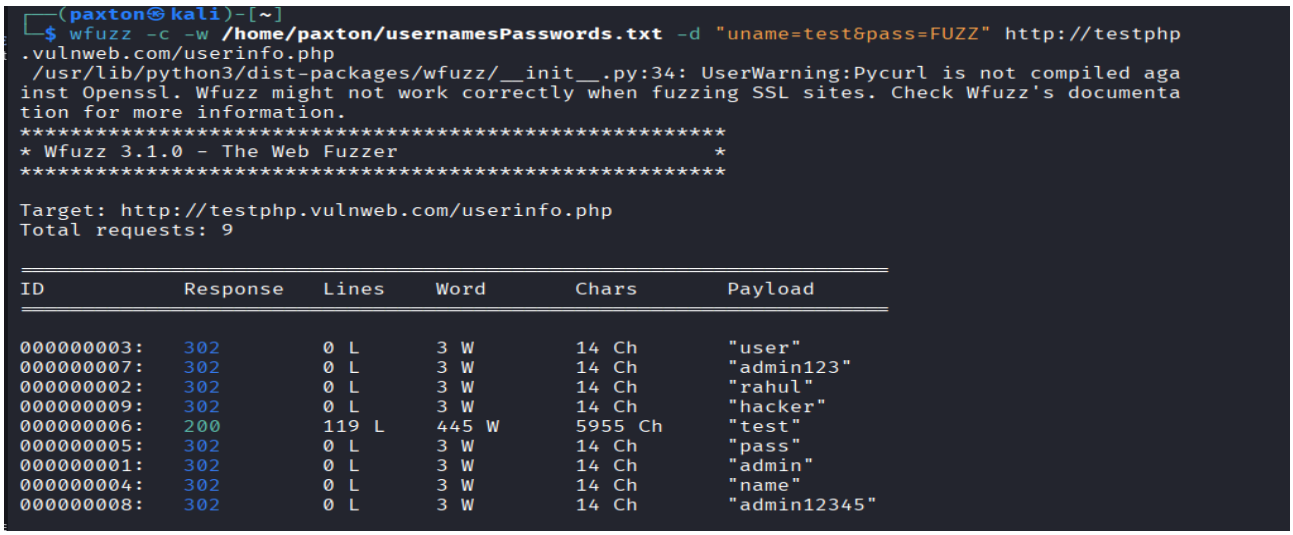
- **Fuzzing post data**

➔ **Command:** *wfuzz -c -w /home/paxton/usernamesPasswords.txt -d "uname=test&pass=FUZZ" http://testphp.vulnweb.com/userinfo.php*

➔ **Description:** Sends POST requests where the password field is fuzzed. Useful for testing login pages, error behavior, or lockout settings in your own lab.

➔ **Note:** Here, i used url where the login page goes after sumitting. Not the actual login page url.





- **JSON body fuzzing**

→ **Command:** *wfuzz -c -w wordlist.txt -H "Content-Type: application/json" -d '{"id":"FUZZ"}' http://yourlab.com/api/user*

→ **Description:** Fuzzes JSON request bodies, commonly used in APIs. Helps you analyze how your API handles unexpected input.

6. Header fuzzing

- **User-agent header fuzzing**

→ **Command:** *wfuzz -c -w agents.txt -H "User-Agent: FUZZ" http://yourlab.com*

→ **Description:** Tests how your server behaves with different User-Agent headers. Good for learning how firewalls respond to different client types.

- **Cookie fuzzing**

→ **Command:** *wfuzz -c -w wordlist.txt -H "Cookie: session=FUZZ" http://yourlab.com*

→ **Description:** Fuzzes session ID cookies to test whether your session management is secure inside your lab.

7. Firewall-aware scanning

- **Reduce speed (low threding)**

→ **Command:** *wfuzz -c -w wordlist.txt -t 5 http://yourlab.com/FUZZ*

→ **Description:** Reduces concurrent threads to avoid triggering rate limits. Firewalls often block high concurrency traffic.

- **Add delay between requests**

→ **Command:** *wfuzz -c -w wordlist.txt -s 0.3 http://yourlab.com/FUZZ*

→ **Description:** Adds a 300ms delay between each request. This simulates realistic browsing patterns and allows you to study firewall tolerance.

- **Randomized user-agent**

→ **Command:** *wfuzz -c -w agents.txt -H "User-Agent: FUZZ" http://yourlab.com*

→ **Description:** Tests how your server responds to different client types. Firewalls sometimes treat unknown agents as suspicious, so this helps learning detection rules.

- **Use HEAD instead of get**

➔ **Command:** *wfuzz -c -w wordlist.txt --hh 0 -X HEAD http://yourlab.com/FUZZ*

➔ **Description:** HEAD requests return headers only, producing less traffic and smaller logs. Useful for learning how WAFs classify light-weight requests.

- **Hide length-based responses (Content-length filter)**

➔ **Command:** *wfuzz -c -w wordlist.txt --hh 0 -X HEAD http://yourlab.com/FUZZ*

➔ **Description:** Filters results by response size. Many WAFs return uniform error pages, so filtering lets you identify unique behavior safely.