Basic Usage

Fuzzing Paths and Files

Wfuzz can be used to look for hidden content, such as files and directories, within a web server, allowing to find further attack vectors. It is worth noting that, the success of this task depends highly on the dictionaries used.

However, due to the limited number of platforms, default installations, known resources such as logfiles, administrative directories, a considerable number of resources are located in predictable locations. Therefore, brute forcing these contents becomes a more feasible task.

Wfuzz contains some dictionaries, other larger and up to date open source word lists are:

- fuzzdb
- seclists

Below is shown an example of wfuzz looking for common directories:

```
$ wfuzz -w wordlist/general/common.txt http://testphp.vulnweb.com/FUZZ
```

Below is shown an example of wfuzz looking for common files:

```
$ wfuzz -w wordlist/general/common.txt http://testphp.vulnweb.com/FUZZ.php
```

Fuzzing Parameters In URLs

You often want to fuzz some sort of data in the URL's query string, this can be achieved by specifying the FUZZ keyword in the URL after a question mark:

```
$ wfuzz -z range,0-10 --hl 97 http://testphp.vulnweb.com/listproducts.php?cat=FUZZ
```

Fuzzing POST Requests

If you want to fuzz some form-encoded data like an HTML form will do, simply pass a -d command line argument:

```
$ wfuzz -z file,wordlist/others/common_pass.txt -d "uname=FUZZ&pass=FUZZ"  --hc 302 http
********************************************************
* Wfuzz 2.2 - The Web Fuzzer                           *
********************************************************

Target: http://testphp.vulnweb.com/userinfo.php
Total requests: 52

=====================================================================
ID      Response   Lines      Word         Chars          Request
=====================================================================

00044:  C=200    114 L       356 W         5111 Ch        "test"

Total time: 2.140146
Processed Requests: 52
Filtered Requests: 51
Requests/sec.: 24.29739
```

Fuzzing Cookies

To send your own cookies to the server, for example, to associate a request to HTTP sessions, you can use the -b parameter (repeat for various cookies):

```
$ wfuzz -z file,wordlist/general/common.txt -b cookie=value1 -b cookie2=value2 http://te
```

The command above will generate HTTP requests such as the one below:

```
GET /attach HTTP/1.1
Host: testphp.vulnweb.com
Accept: */*
Content-Type:  application/x-www-form-urlencoded
Cookie:  cookie=value1; cookie2=value2
User-Agent:  Wfuzz/2.2
Connection: close
```

Cookies can also be fuzzed:

```
$ wfuzz -z file,wordlist/general/common.txt -b cookie=FUZZ http://testphp.vulnweb.com/
```

Fuzzing Custom headers

If you'd like to add HTTP headers to a request, simply use the -H parameter (repeat for various headers):

```
$ wfuzz -z file,wordlist/general/common.txt -H "myheader: headervalue" -H "myheader2: he
```

The command above will generate HTTP requests such as the one below:

```
GET /agent HTTP/1.1
Host: testphp.vulnweb.com
Accept: */*
Myheader2:  headervalue2
Myheader:  headervalue
Content-Type:  application/x-www-form-urlencoded
```

```
User-Agent:  Wfuzz/2.2
Connection: close
```

You can modify existing headers, for example, for specifying a custom user agent, execute the following:

```
$ wfuzz -z file,wordlist/general/common.txt -H "myheader: headervalue" -H "User-Agent: G
```

The command above will generate HTTP requests such as the one below:

```
GET /asp HTTP/1.1
Host: testphp.vulnweb.com
Accept: */*
Myheader:  headervalue
Content-Type:  application/x-www-form-urlencoded
User-Agent:  Googlebot-News
Connection: close
```

Headers can also be fuzzed:

```
$ wfuzz -z file,wordlist/general/common.txt -H "User-Agent: FUZZ" http://testphp.vulnweb
```

Fuzzing HTTP Verbs

HTTP verbs fuzzing can be specified using the -X switch:

```
$ wfuzz -z list,GET-HEAD-POST-TRACE-OPTIONS -X FUZZ http://testphp.vulnweb.com/
********************************************************
* Wfuzz 2.2 - The Web Fuzzer                           *
********************************************************

Target: http://testphp.vulnweb.com/
Total requests: 5

=====================================================================
ID      Response   Lines      Word         Chars          Request
=====================================================================

00002:  C=200      0 L         0 W           0 Ch        "HEAD"
00004:  C=405      7 L        12 W         172 Ch        "TRACE"
```

```
00005:  C=405      7 L        12 W          172 Ch        "OPTIONS"
00001:  C=200    104 L       296 W         4096 Ch        "GET"
00003:  C=200    104 L       296 W         4096 Ch        "POST"

Total time: 1.030354
Processed Requests: 5
Filtered Requests: 0
Requests/sec.: 4.852696
```

If you want to perform the requests using a specific verb you can also use "-X HEAD".

Proxies

If you need to use a proxy, simply use the -p parameter:

```
$ wfuzz -z file,wordlist/general/common.txt -p localhost:8080 http://testphp.vulnweb.com
```

In addition to basic HTTP proxies, Wfuzz also supports proxies using the SOCKS4 and SOCKS5 protocol:

```
$ wfuzz -z file,wordlist/general/common.txt -p localhost:2222:SOCKS5 http://testphp.vuln
```

Multiple proxies can be used simultaneously by supplying various -p parameters:

```
$ wfuzz -z file,wordlist/general/common.txt -p localhost:8080 -p localhost:9090 http://t
```

Each request will be performed using a different proxy each time.

Authentication

Wfuzz can set an authentication headers by using the --basic/ntlm/digest command line switches.

For example, a protected resource using Basic authentication can be fuzzed using the following command:

```
$ wfuzz -z list,nonvalid-httpwatch --basic FUZZ:FUZZ https://www.httpwatch.com/httpgalle
********************************************************
* Wfuzz 2.2 - The Web Fuzzer                           *
********************************************************
```

```
Target: https://www.httpwatch.com/httpgallery/authentication/authenticatedimage/default.
Total requests: 2

=====================================================================
ID      Response   Lines      Word         Chars          Request
=====================================================================

00001:  C=401      0 L        11 W           58 Ch        "nonvalid"
00002:  C=200     20 L        91 W         5294 Ch        "httpwatch"

Total time: 0.820029
Processed Requests: 2
Filtered Requests: 0
Requests/sec.: 2.438938
```

If you want to fuzz a resource from a protected website you can also use "--basic user:pass".

Recursion

The -R switch can be used to specify a payload recursion's depth. For example, if you want to search for existing directories and then fuzz within these directories again using the same payload you can use the following command:

```
$ wfuzz -z list,"admin-CVS-cgi\-bin"  -R1 http://testphp.vulnweb.com/FUZZ
********************************************************
* Wfuzz 2.2 - The Web Fuzzer                           *
********************************************************

Target: http://testphp.vulnweb.com/FUZZ
Total requests: 3

=====================================================================
ID      Response   Lines      Word         Chars          Request
=====================================================================

00003:  C=403     10 L        29 W          263 Ch        "cgi-bin"
00002:  C=301      7 L        12 W          184 Ch        "CVS"
|_ Enqueued response for recursion (level=1)
00001:  C=301      7 L        12 W          184 Ch        "admin"
|_ Enqueued response for recursion (level=1)
00008:  C=404      7 L        12 W          168 Ch        "admin - CVS"
00007:  C=404      7 L        12 W          168 Ch        "admin - admin"
```

```
00005:  C=404      7 L        12 W          168 Ch        "CVS - CVS"
00006:  C=404      7 L        12 W          168 Ch        "CVS - cgi-bin"
00009:  C=404      7 L        12 W          168 Ch        "admin - cgi-bin"
00004:  C=404      7 L        12 W          168 Ch        "CVS - admin"
```

Perfomance

Several options lets you fine tune the HTTP request engine, depending on the performance impact on the application, and on your own processing power and bandwidth.

You can increase or decrease the number of simultaneous requests to make your attack proceed faster or slower by using the -t switch.

You can tell Wfuzz to stop a given number of seconds before performing another request using the -s parameter.

Writing to a file

Wfuzz supports writing the results to a file in a different format. This is performed by plugins called "printers". The available printers can be listed executing:

```
$ wfuzz -e printers
```

For example, to write results to an output file in JSON format use the following command:

```
$ wfuzz -f /tmp/outfile,json -w wordlist/general/common.txt http://testphp.vulnweb.com/F
```

Different output

Wfuzz supports showing the results in various formats. This is performed by plugins called "printers". The available printers can be listed executing:

```
$ wfuzz -e printers
```

For example, to show results in JSON format use the following command:

```
$ wfuzz -o json -w wordlist/general/common.txt http://testphp.vulnweb.com/FUZZ
```

When using the default or raw output you can also select additional FuzzResult's fields to show, using --efield, together with the payload description:

```
$ wfuzz -z range --zD 0-1 -u http://testphp.vulnweb.com/artists.php?artist=FUZZ --efield
...
000000001:   200        99 L     272 W    3868 Ch   0 | GET /artists.php?artist=0 HTTP/1
                                                     Content-Type: application/x-www-form
                                                     User-Agent: Wfuzz/2.4
                                                     Host: testphp.vulnweb.com

...
```

The above command is useful, for example, to debug what exact HTTP request Wfuzz sent to the remote Web server.

To completely replace the default payload output you can use --field instead:

```
$ wfuzz -z range --zD 0-1 -u http://testphp.vulnweb.com/artists.php?artist=FUZZ --field
...
000000001:   200        104 L    364 W    4735 Ch     "http://testphp.vulnweb.com/artist
...
```

--efield and --field can be repeated to show several fields:

```
$ wfuzz -z range --zD 0-1 -u http://testphp.vulnweb.com/artists.php?artist=FUZZ --efield
...
000000001:   200        104 L    364 W    4735 Ch     "0 | http://testphp.vulnweb.com/ar
...
```

The field printer can be used with a --efield or --field expression to list only the specified filter expressions without a header or footer:

```
$ wfuzz -z list --zD https://www.airbnb.com/ --script=links --script-args=links.regex=.*
https://a0.muscache.com/airbnb/static/packages/4e8d-d5c346ee.js
https://a0.muscache.com/airbnb/static/packages/7afc-ac814a17.js
https://a0.muscache.com/airbnb/static/packages/7642-dcf4f8dc.js
```

The above command is useful, for example, to pipe wfuzz into other tools or perform console scripts.

--efield and --field are in fact filter expressions. Check the filter language section in the advance usage document for the available fields and operators.