

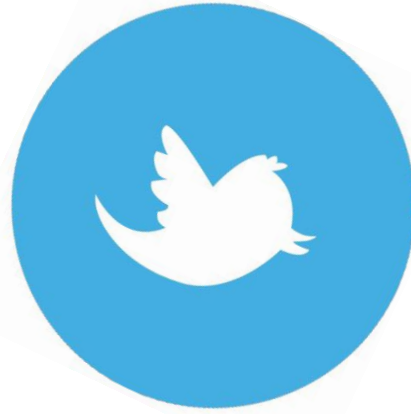
Introduction to Burp Suite



OWASP

Open Web Application
Security Project

whoami



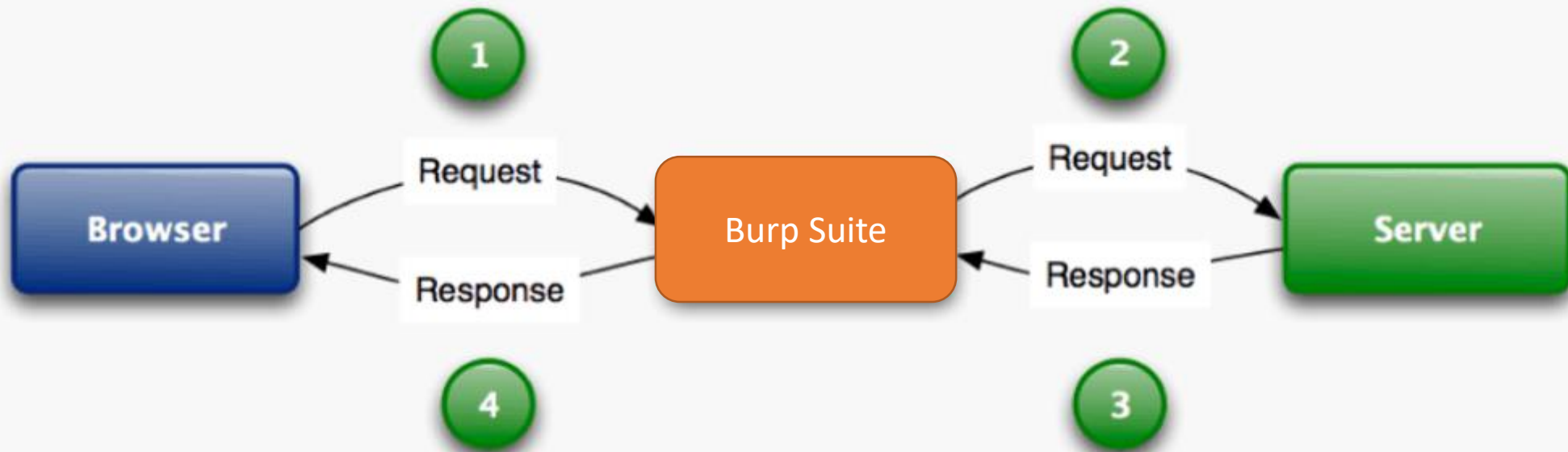
@Higgs0x



<https://www.hackthebox.eu/profile/13547>

- Web application security testing tool
- Developed by PortSwigger
- Heavily used by Bug Hunters
- Extendable
- Runs on MacOS, GNU/Linux, Windows
- Intuitive
- Free version available

- Builtwith
- Wappalyzer
- FoxyProxy
- Wfuzz





Firefox Add-ons

დათვალიერება

გაფართოებები

თემები

სხვა... ▾



სასურველი

FoxyProxy Standard

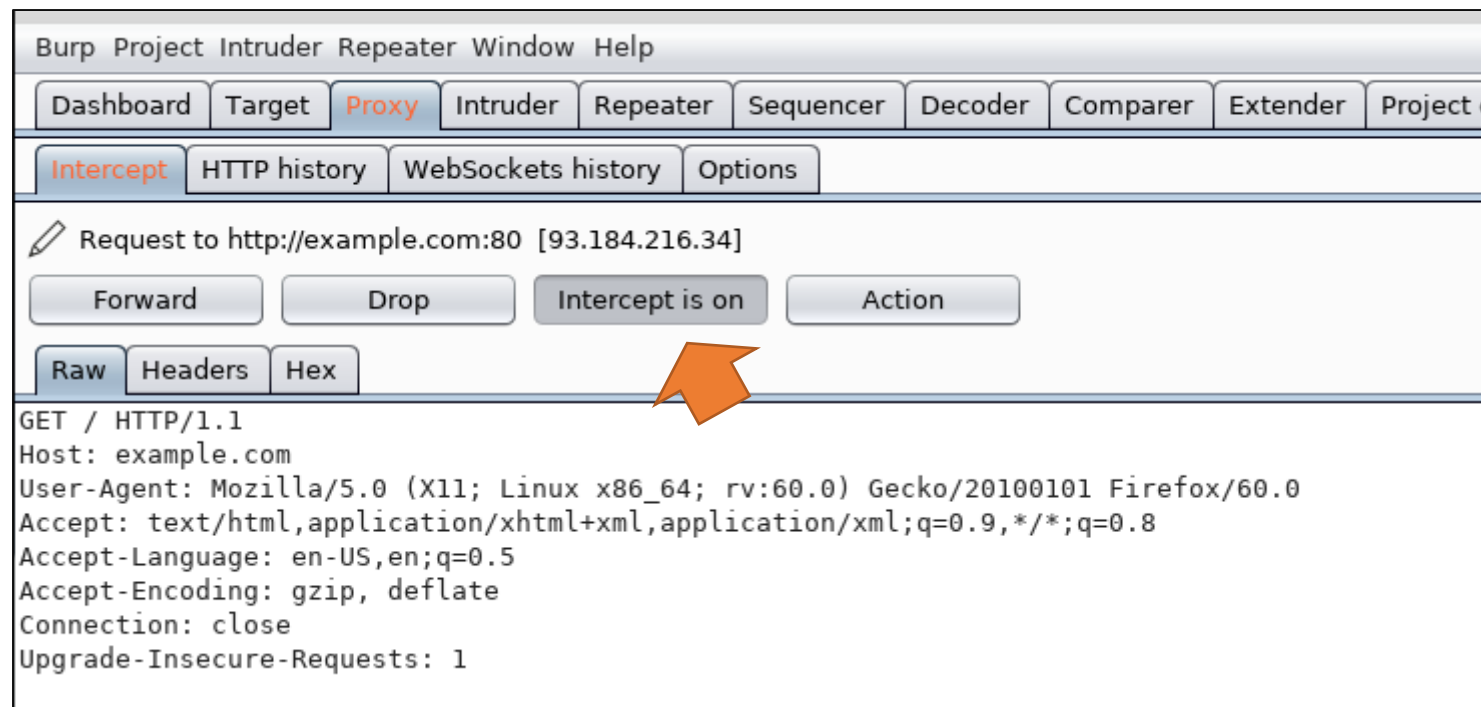
ავტორი [Eric H. Jung](#)

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Tab	Description
Proxy	Intercepts requests and Responses
Intruder	Fuzzing
Repeater	Catch, Modify, Send, Re-edit, re-send
Sequencer	Analyzing session token randomness
Decoder	Encoder/Decoder to various encoding form
Comparer	Compare two requests/responses
Extender	Extend burp suite



Button	Description
Forward	Send to webserver
Drop	Drop caught request
Intercept is on	On/Off intercept mode
Action	Send request to one of the Burp Tab

Burp Project Intruder Repeater Window Help


[Dashboard](#) [Target](#) [Proxy](#) [Intruder](#) [Repeater](#) [Sequencer](#) [Decoder](#) [Comparer](#) [Extender](#) [Project options](#) [User options](#)

1 x 2 x ...

[Target](#) [Positions](#) [Payloads](#) [Options](#)

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see h

Attack type: 

```
GET /$FUZZ$ HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

\$FUZZ\$

Placeholder for fuzzing

Wfuzzer replaces Burp Suite Intruder

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# wfuzz -c -z file,/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt http://example.com/FUZZ  
  
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.  
  
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payloads/shodanp.py Exception, msg=No module named 'shodan'  
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payloads/bing.py Exception, msg=No module named 'shodan'  
*****  
* Wfuzz 2.4 - The Web Fuzzer *  
*****  
  
Target: http://example.com/FUZZ  
Total requests: 87664  
  
=====
```

ID	Response	Lines	Word	Chars	Payload
000000001:	200	50 L	120 W	1270 Ch	"# directory-list-2.3-small.txt"
000000011:	200	50 L	120 W	1270 Ch	"# Priority ordered case sensitive list, where entries were found"
000000012:	200	50 L	120 W	1270 Ch	"# on atleast 3 different hosts"
000000013:	200	50 L	120 W	1270 Ch	"#"
000000014:	200	50 L	120 W	1270 Ch	""
000000015:	404	50 L	120 W	1270 Ch	"index"
000000016:	404	50 L	120 W	1270 Ch	"images"

```
^C  
Finishing pending requests...
```

Burp Project Intruder Repeater Window Help

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Project options

User options

1 x

2 x

...

Target

Positions

Payloads

Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are in different ways.

Payload set: 1

Payload count: 81,643

Payload type: Simple list

Request count: 81,643

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

directory-list-lowercase-2.3-small.txt

#

Copyright 2007 James Fisher

#

This work is licensed under the Creative Com...

Attribution-Share Alike 3.0 License. To view a ...

license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

or send a letter to Creative Commons, 171 Se

Enter a new item

Add from list ... [Pro version only]

Intruder attack 1

Attack Save Columns

[Results](#) [Target](#) [Positions](#) [Payloads](#) [Options](#)

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		404	<input type="checkbox"/>	<input type="checkbox"/>	1535	
1	# directory-list-lowercase-2.3-...	200	<input type="checkbox"/>	<input type="checkbox"/>	1627	
2	#	200	<input type="checkbox"/>	<input type="checkbox"/>	1627	
3	# Copyright 2007 James Fisher	200	<input type="checkbox"/>	<input type="checkbox"/>	1632	

Send

Cancel

< ▼

> ▼

Request

Raw

Headers

Hex

```
GET / HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Target: <http://example.com>

Response

Raw

Headers

Hex

HTML

Render

```
HTTP/1.1 200 OK
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Thu, 05 Sep 2019 18:19:32 GMT
Etag: "1541025663+gzip"
Expires: Thu, 12 Sep 2019 18:19:32 GMT
Last-Modified: Fri, 09 Aug 2013 23:54:35 GMT
Server: ECS (dcb/7F5C)
Vary: Accept-Encoding
X-Cache: HIT
```

Burp Suite Community Edition v2.1.02 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard		Target	Proxy	Intruder		
Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options

OWASp meeting

☒ Text ☐ Hex ?

Decode as ...

Encode as ...

Hash ...

Smart decode

T1dBU3AgbWVldGluZw==

☒ Text ☐ Hex

Decode as ...

Encode as ...

Hash ...

Smart decode