Burp Suite Advanced

Bugcrowd University

bugcrowd.com

Burp Suite Advanced - Part #1

- Tips and tricks
- Improving workflow

Burp Suite Advanced - Part #2

- Deep dive in Intruder
- Using macros and session handling rules
- Useful extensions

Module Trainer

- Jasmin Landry - @JR0ch17
- Sr. Cybersecurity Engineer at SecureOps
- Pentester, Bug Bounty Hunter & hockey player

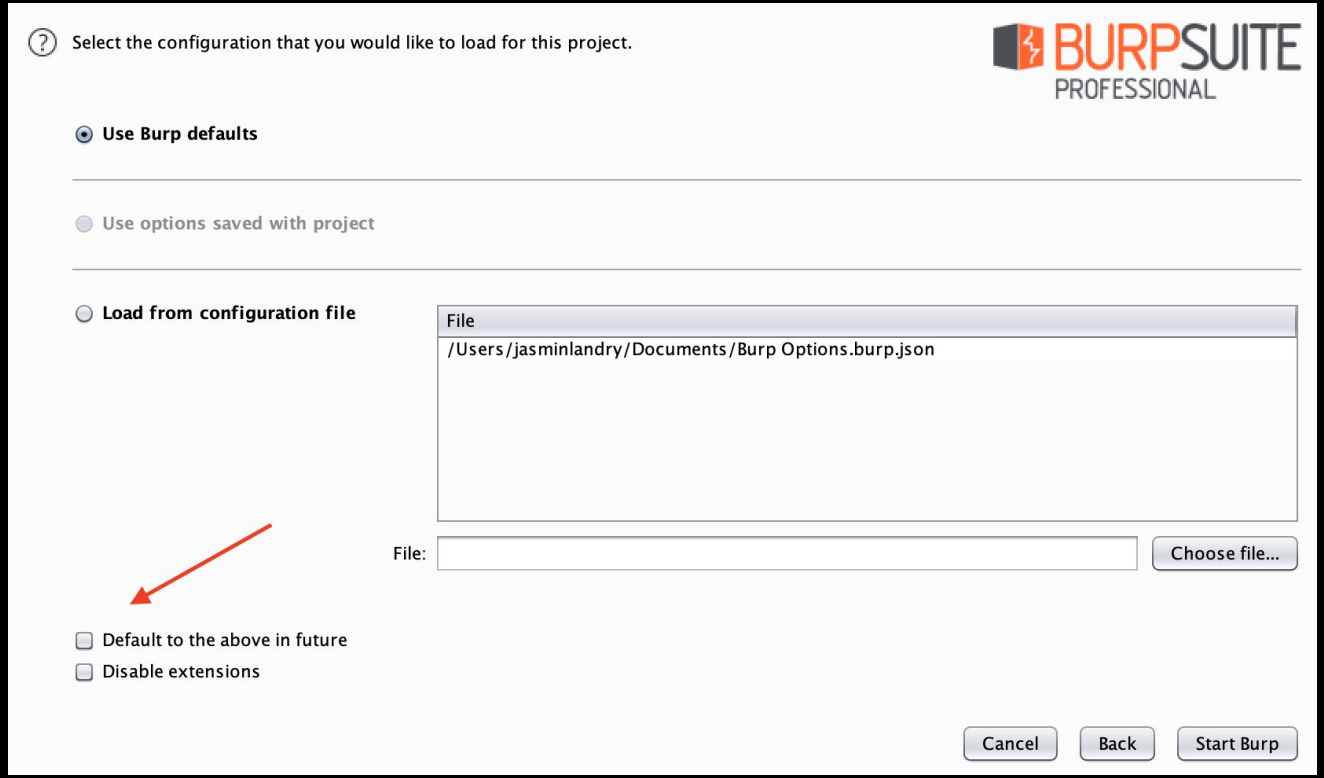
Module Outline

1. Configuration & Settings
2. Ctrl + Shift + T (Target)
3. Ctrl + Shift + P (Proxy)
4. Ctrl + Shift + R (Repeater)
5. Ctrl + Shift + I (Intruder)
6. HotKeys/Hackvertor
7. Logger++
8. Resources & References

Configuration and Settings

Startup

Disable extensions?



Project Options vs User Options

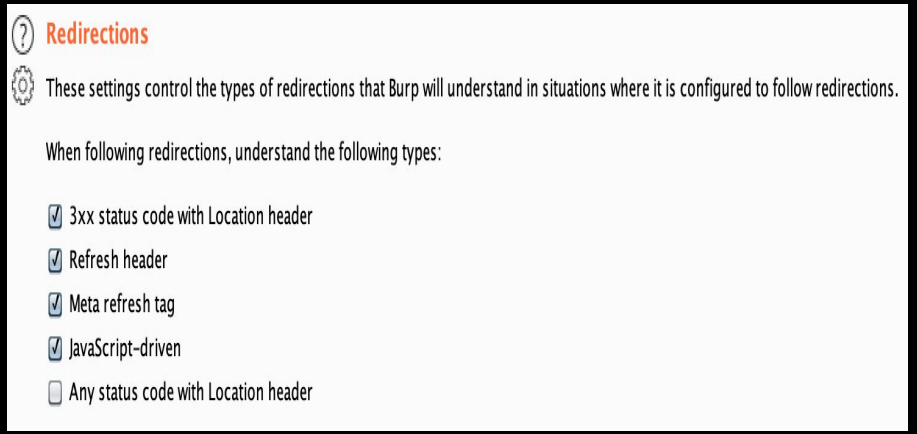
Project: Configuration and settings that apply to what you are hacking (Macros, Session Handling Rules, etc)

User: Configuration and settings that apply to Burp (Upstream proxy, UI theme, Hotkeys, etc)

Useful Project Options

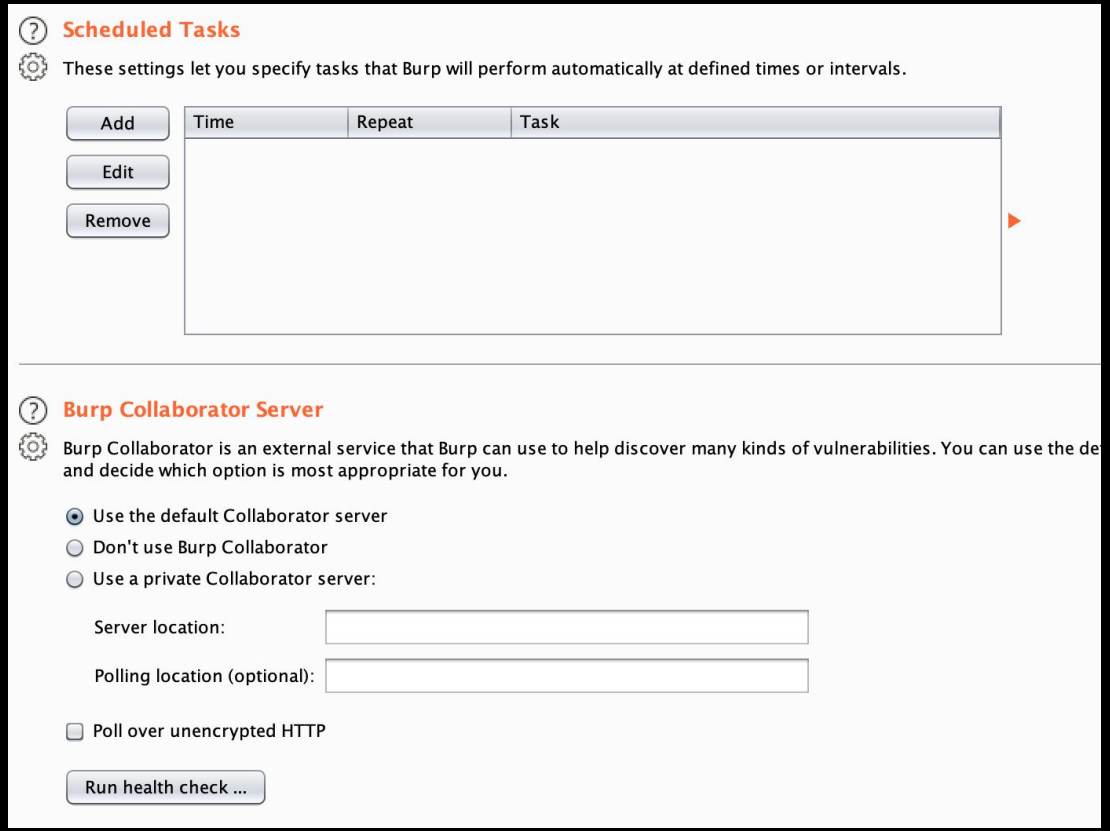
Project Options -> HTTP -> Redirections

JavaScript-driven not enabled by default



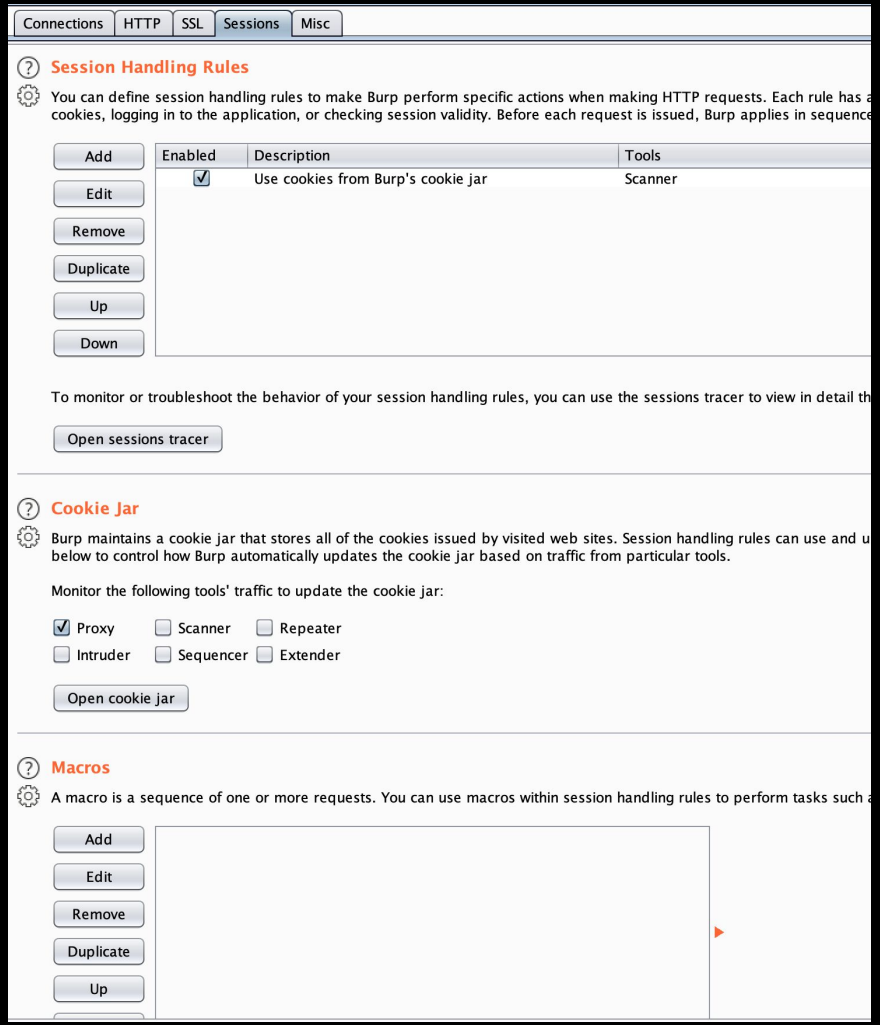
Useful Project Options

Project Options -> Misc -> Scheduled Tasks, Burp Collaborator Server



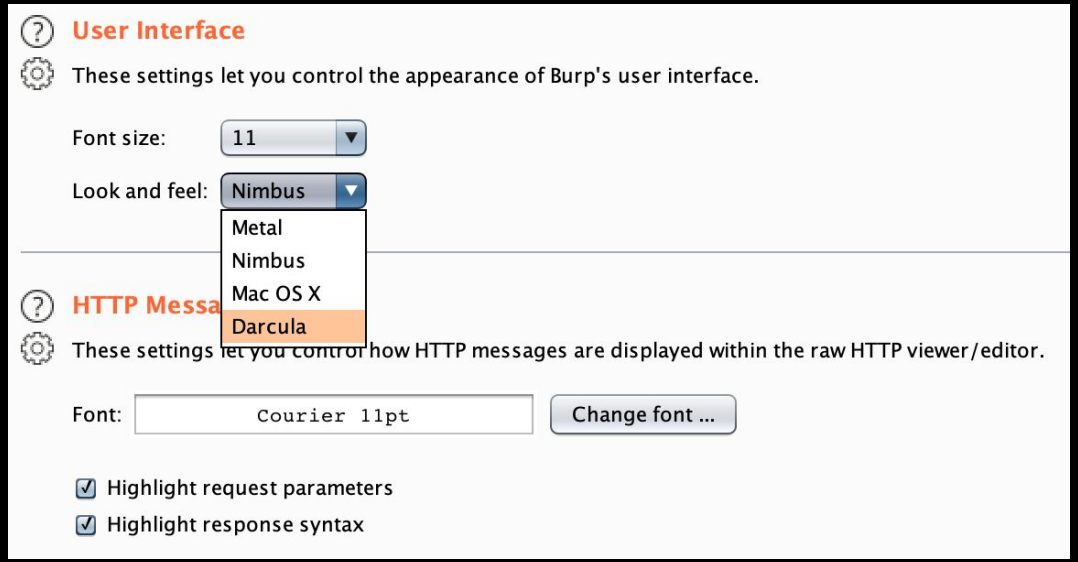
Useful Project Options

Project Options -> Sessions -> Session Handling Rules / Cookie Jar / Macros



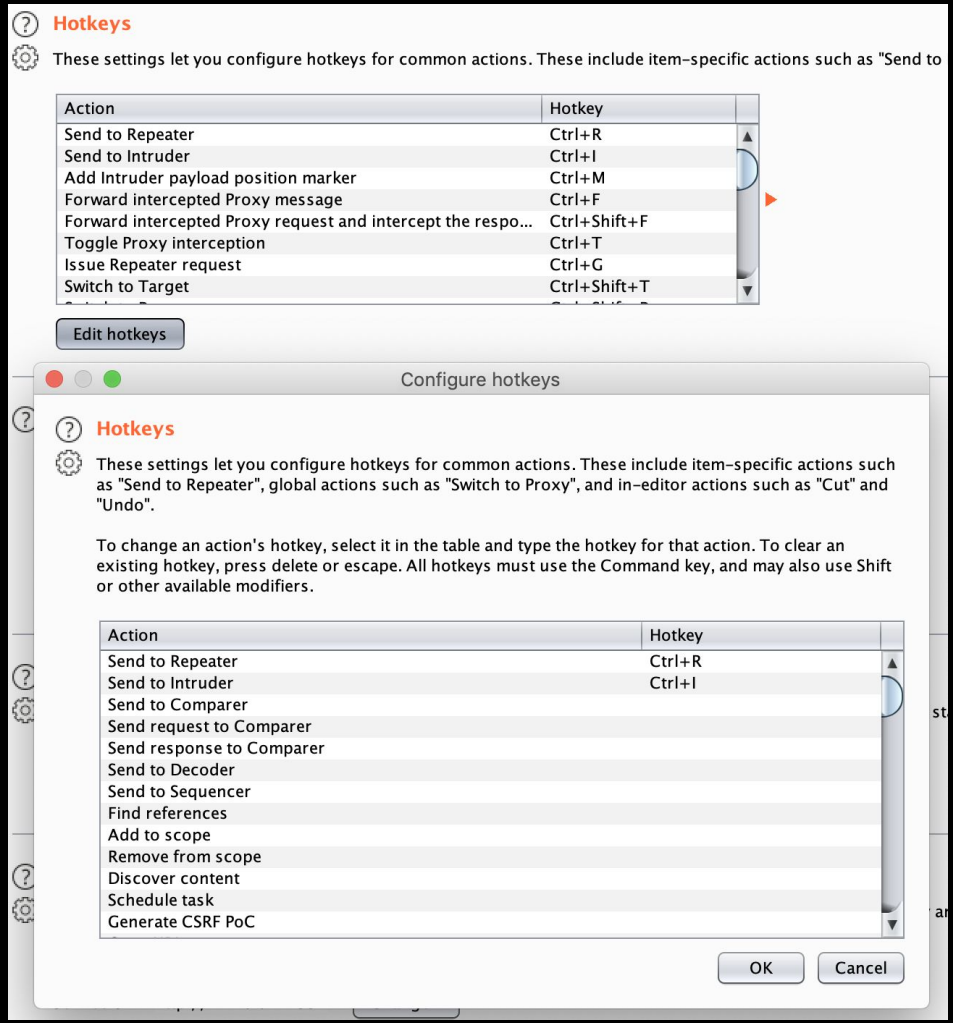
Useful User Options

User Options -> Display -> User Interface / HTTP Message Display



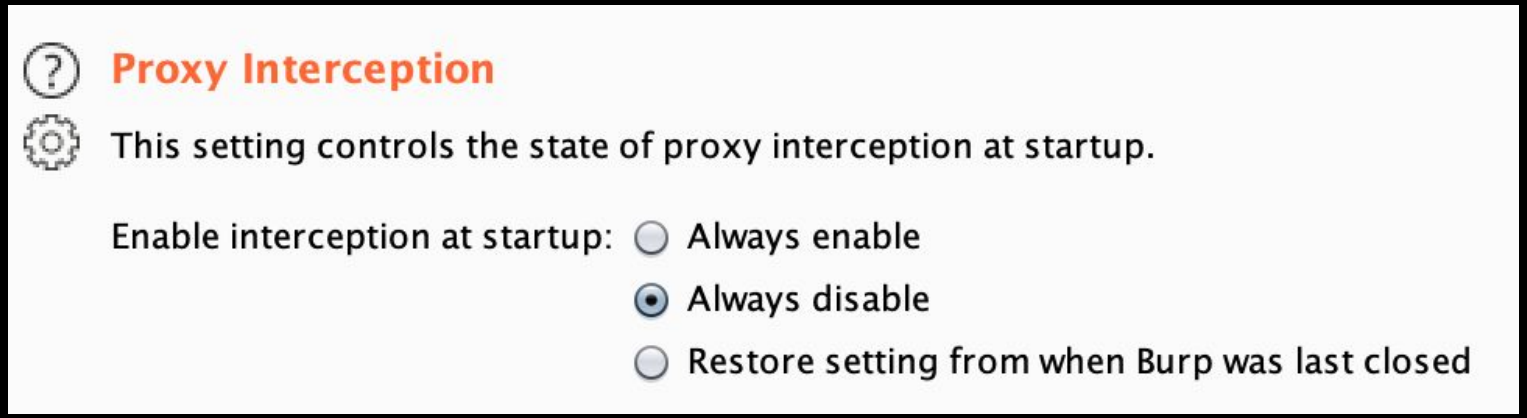
Useful User Options

User Options ->
Misc ->
Hotkeys /
Edit hotkeys

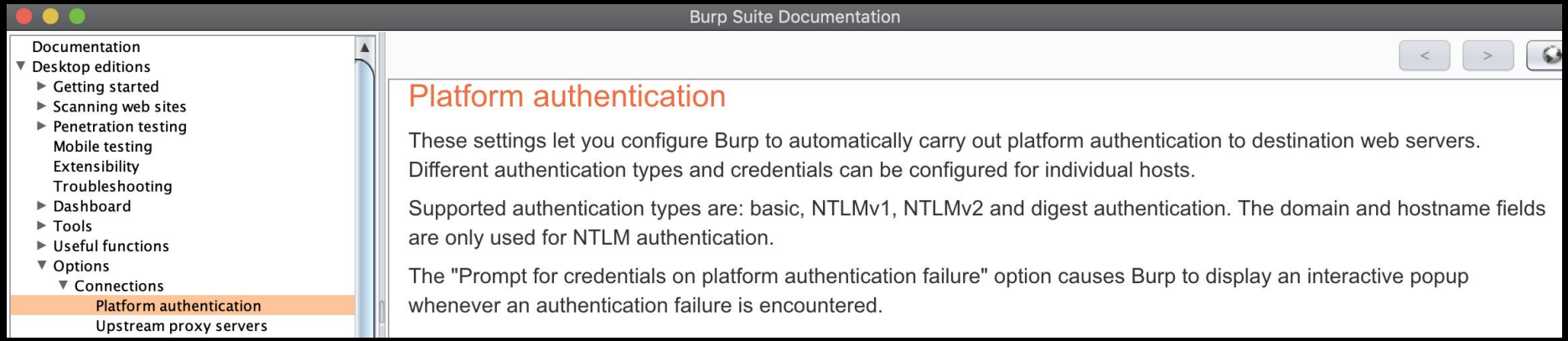


Useful User Options

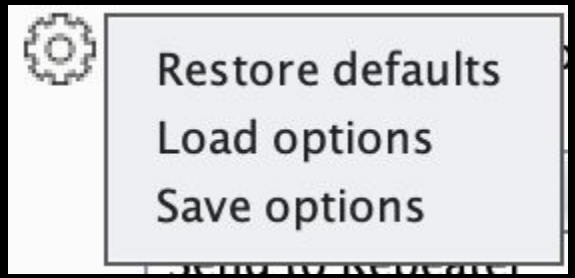
User Options ->
Misc ->
Proxy Interception

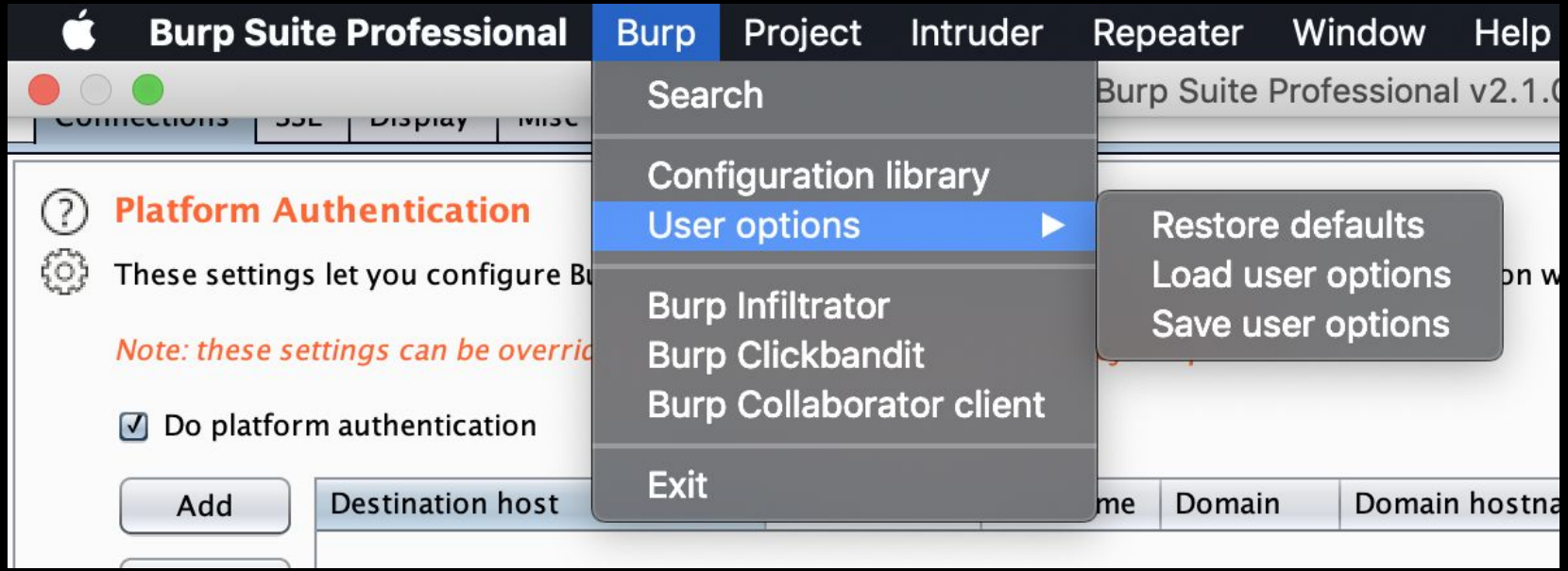


What is this option for?



How do I save these options for future use?



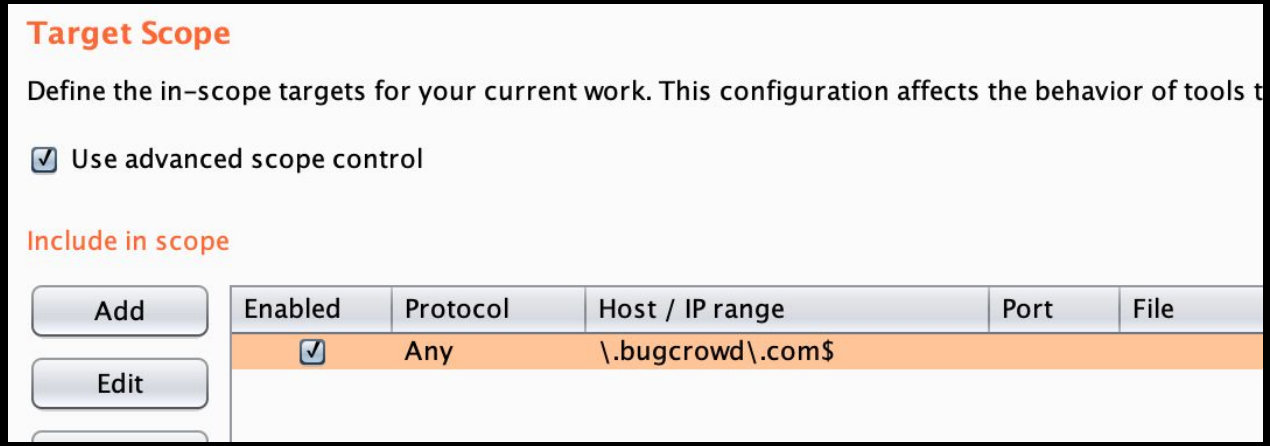


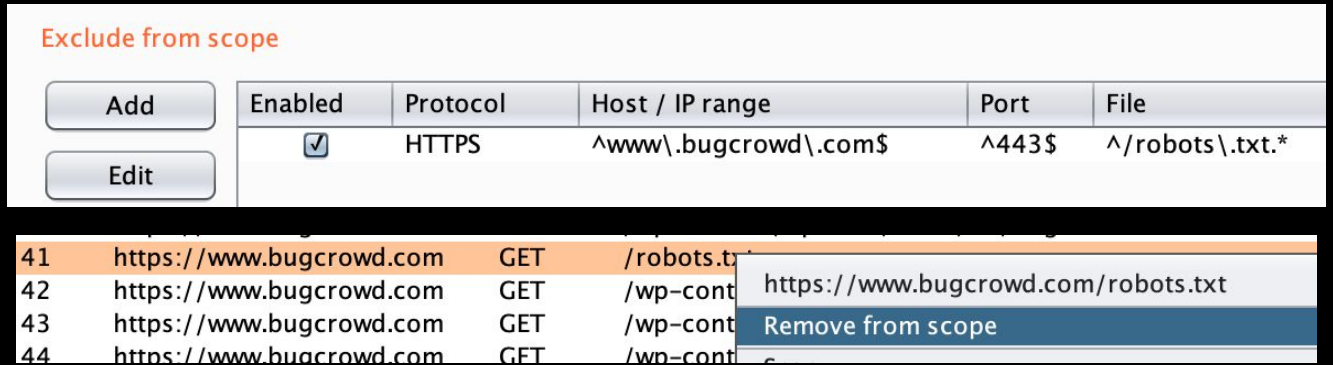

root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
Ctrl + Shift + T

Ctrl + Shift + T -> Scope

Advanced Scope Control with Regex

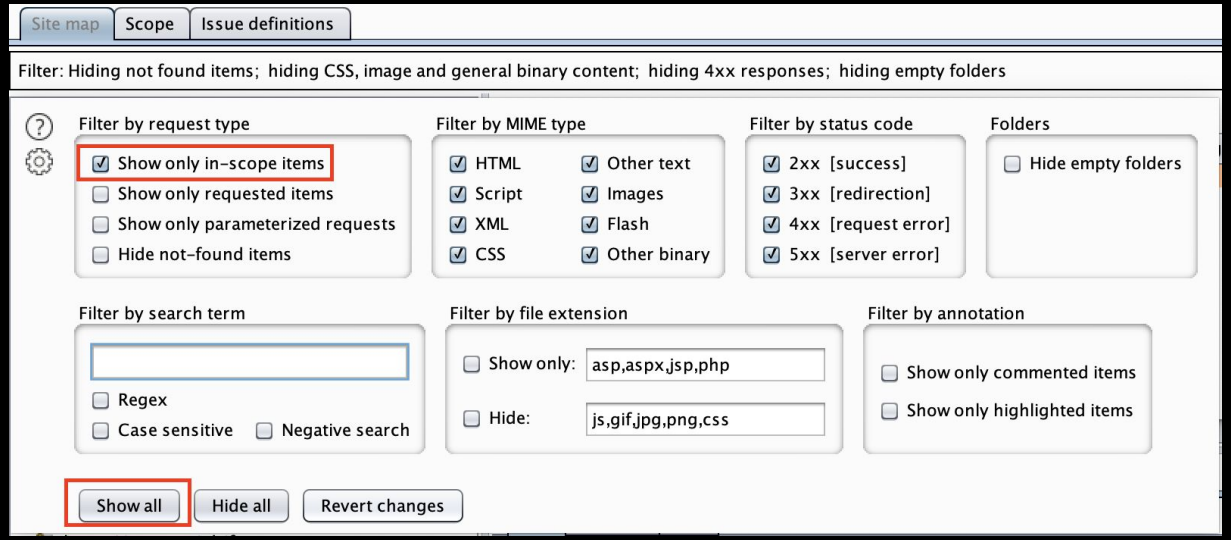
Exclude from scope





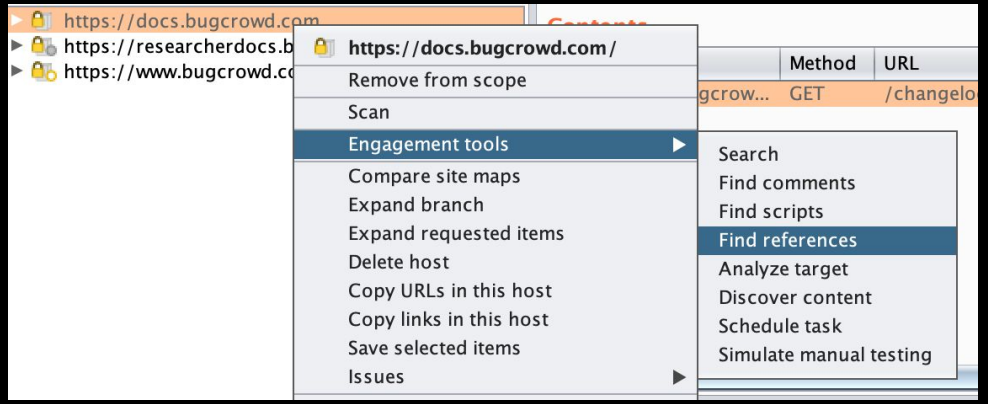
...

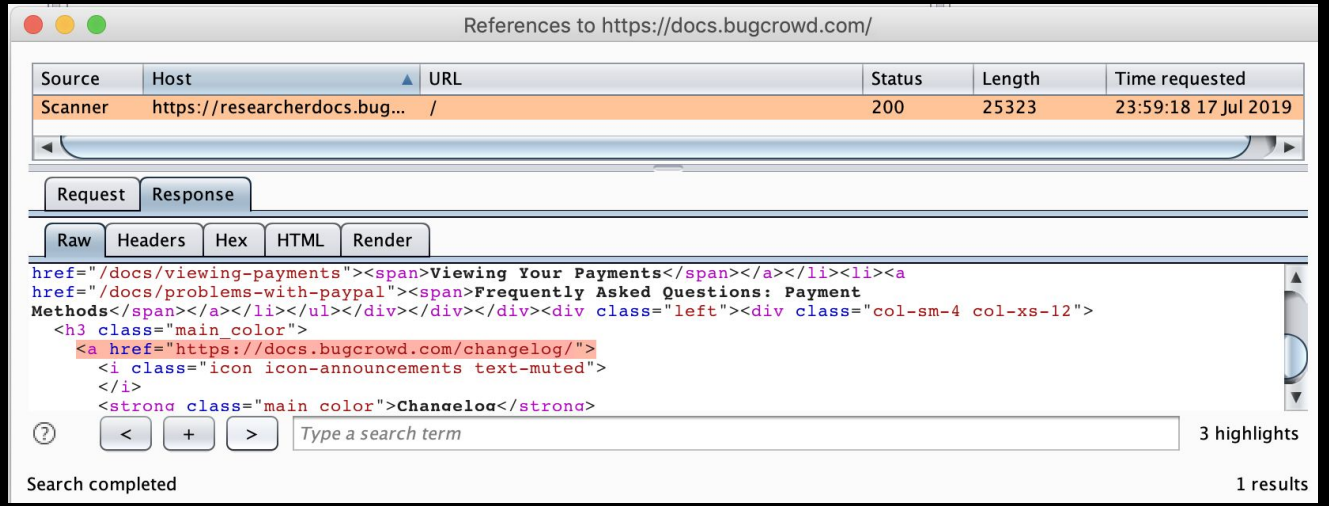
Ctrl - ->
Filter



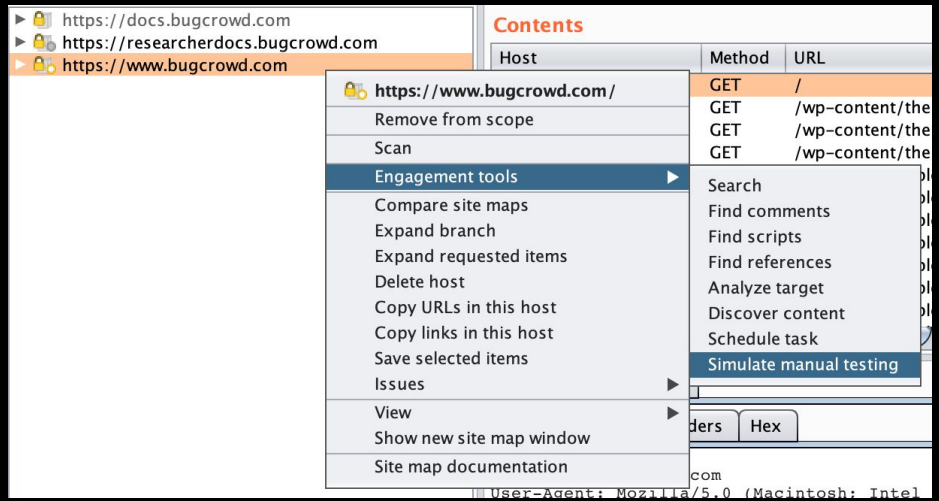
Similar Filter in Proxy History

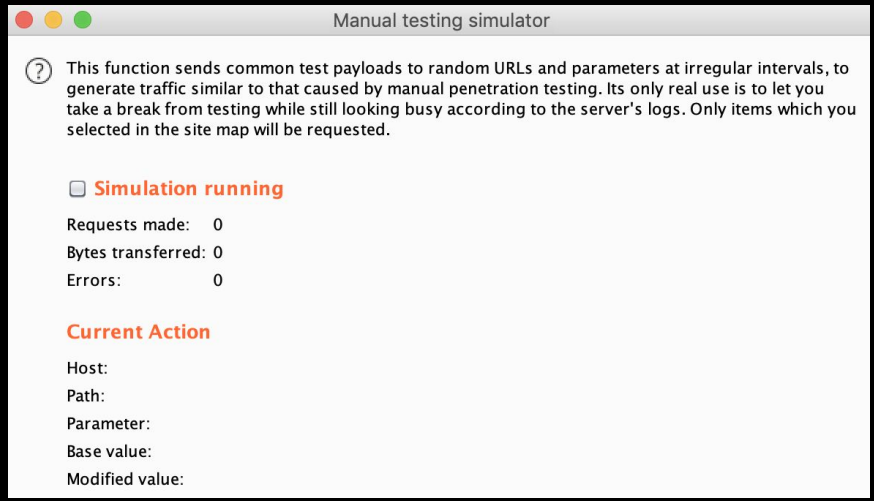
Engagement Tools -> Find References





Engagement Tools ->
Simulate manual testing

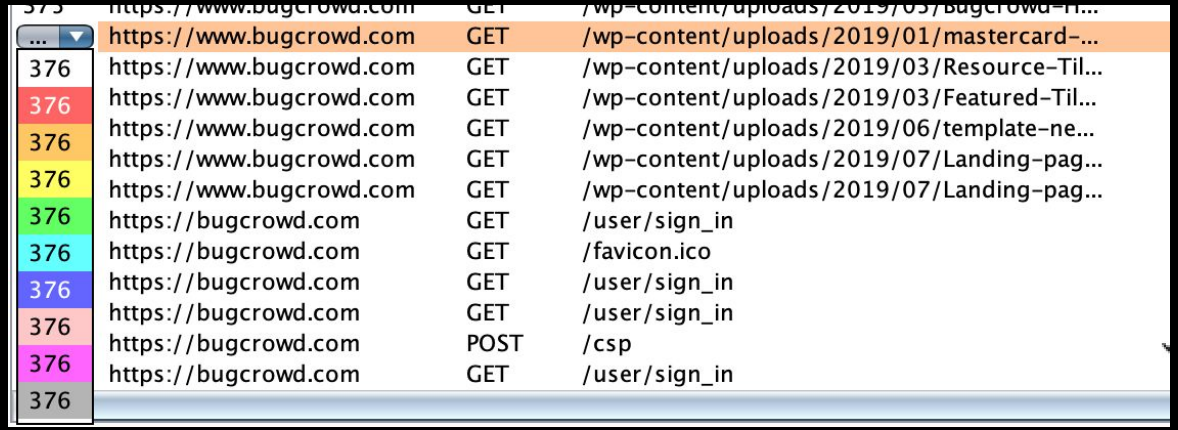


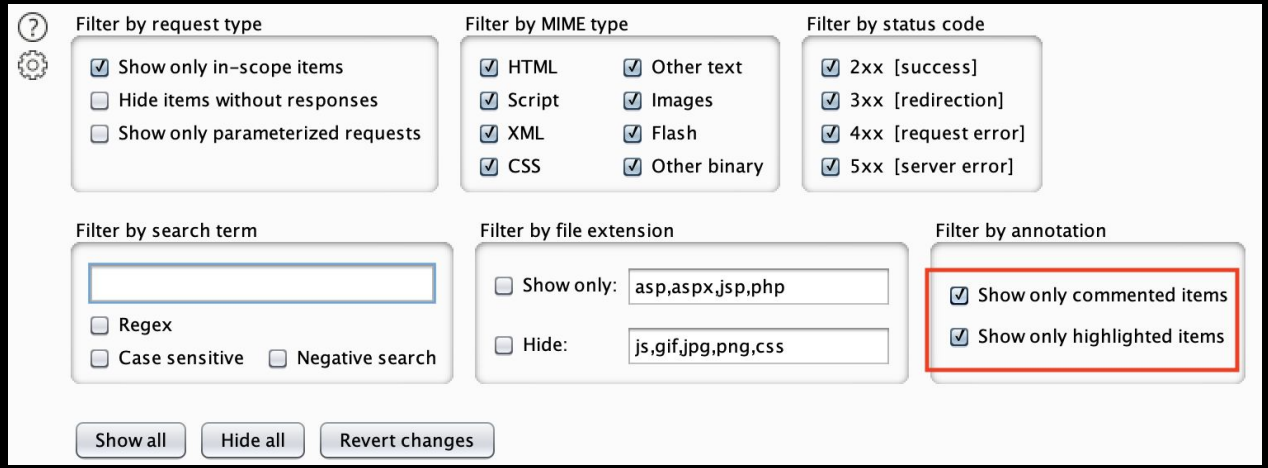



root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
Ctrl + Shift + P

HTTP History

Highlight and/or Comment requests

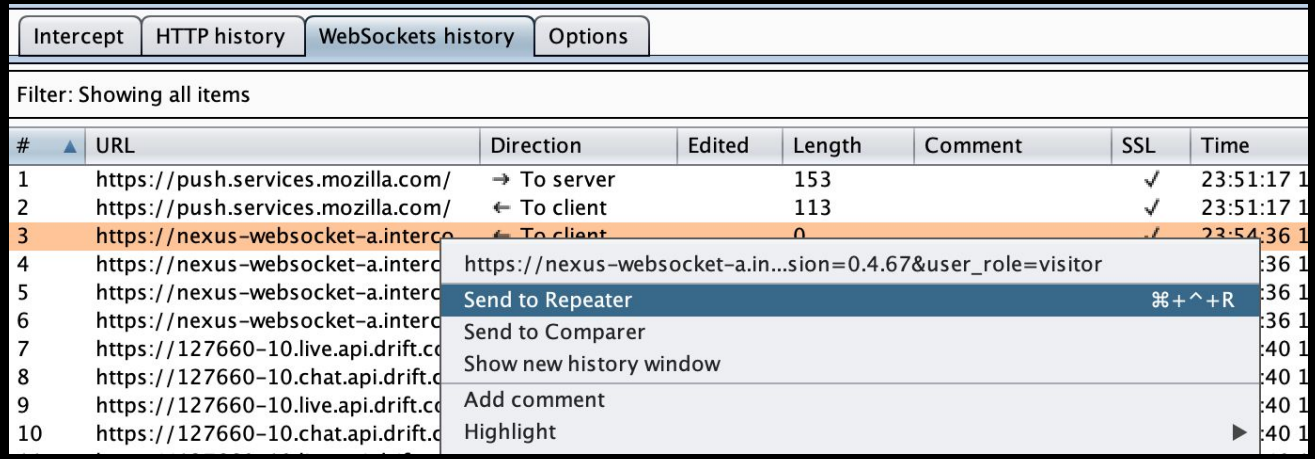




...

Ctrl +

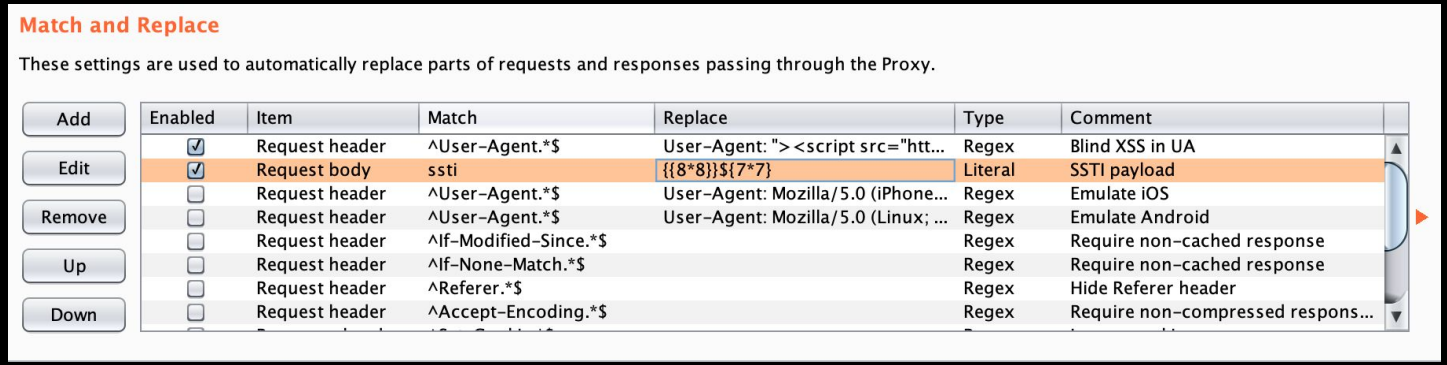
Websockets requests can now be sent to Repeater!!!

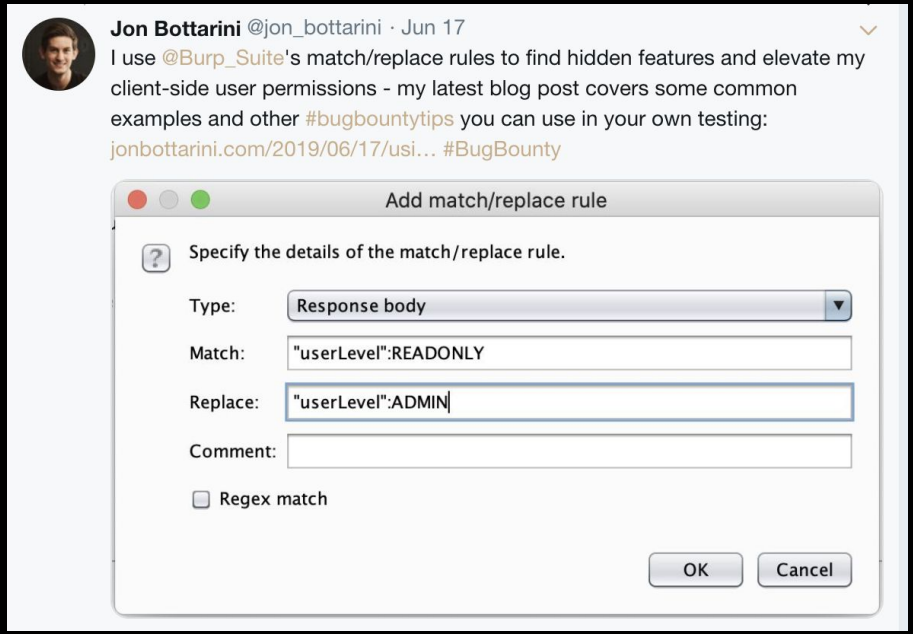


...

Ctrl +

Match and Replace



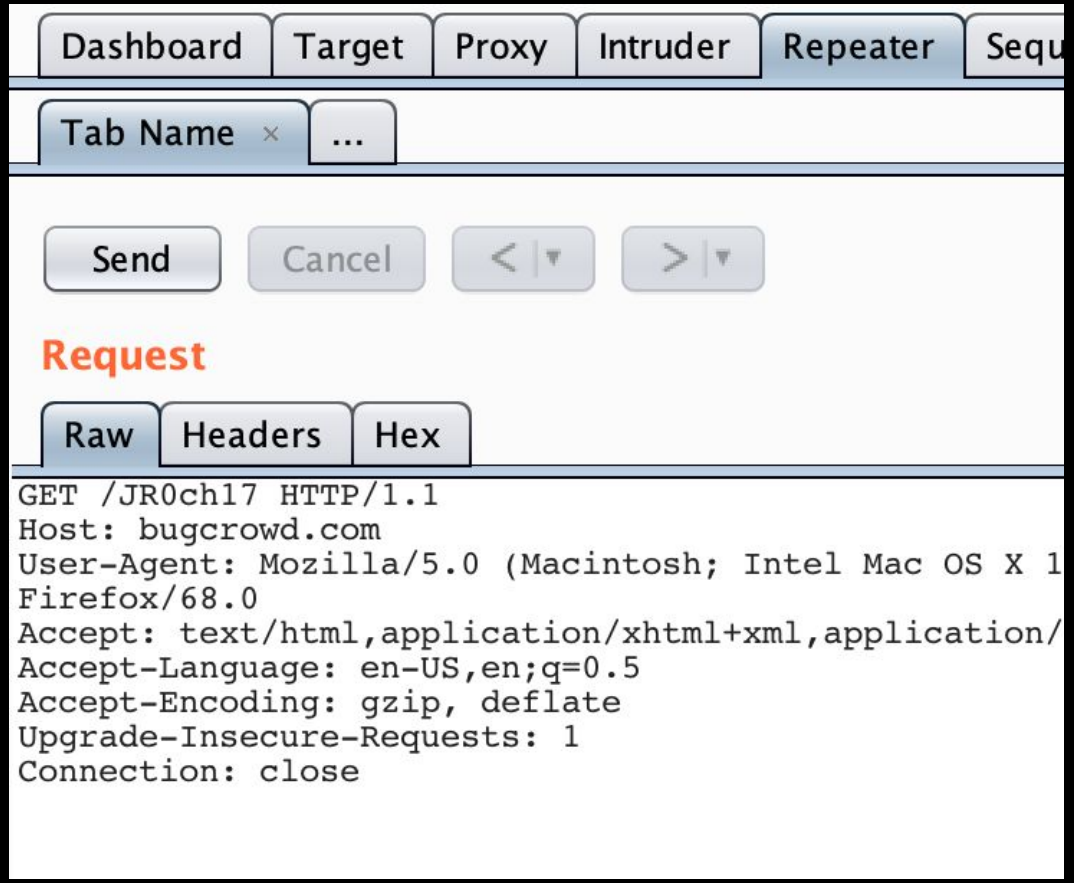



root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
Ctrl + Shift + R

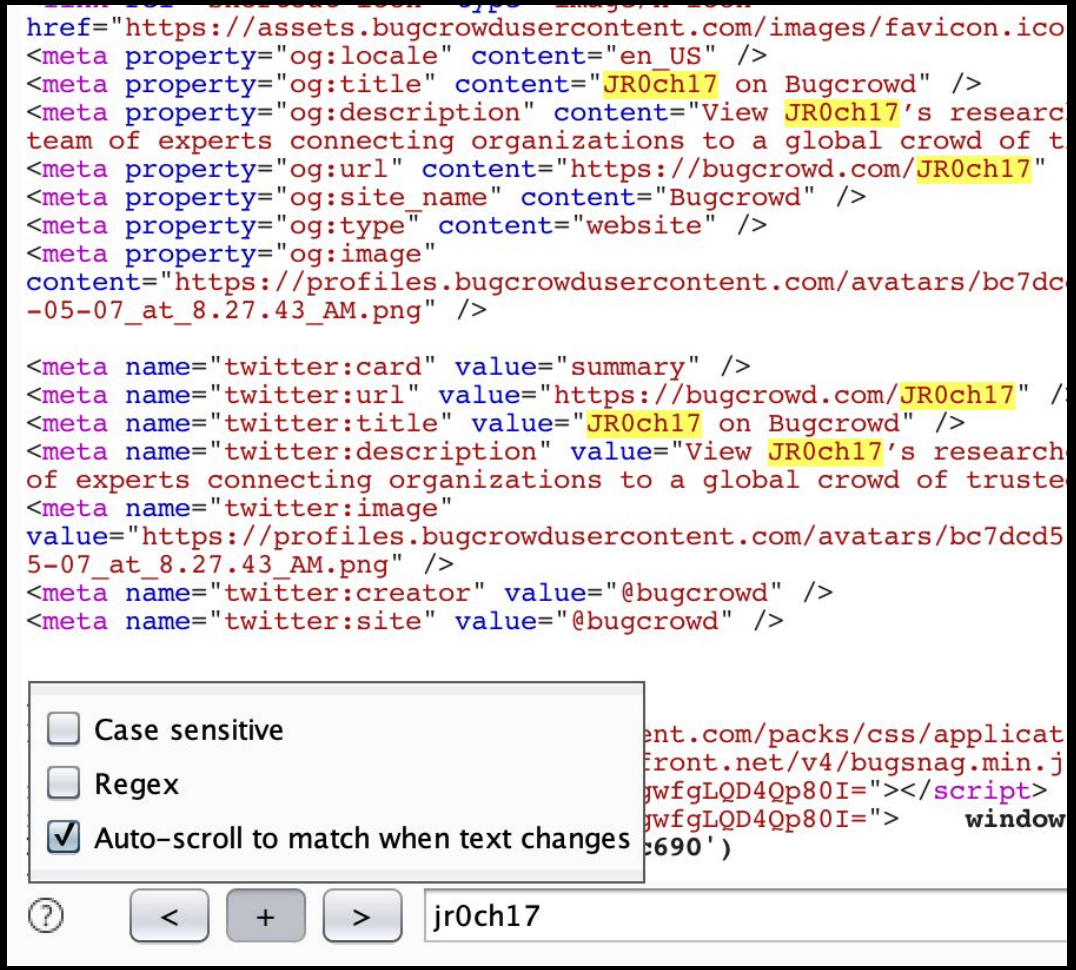
Playing with tabs

Use Ctrl - and Ctrl + to switch Repeater tabs

Configure shortcuts to go back and forward in Repeater requests and a shortcut to the Send button



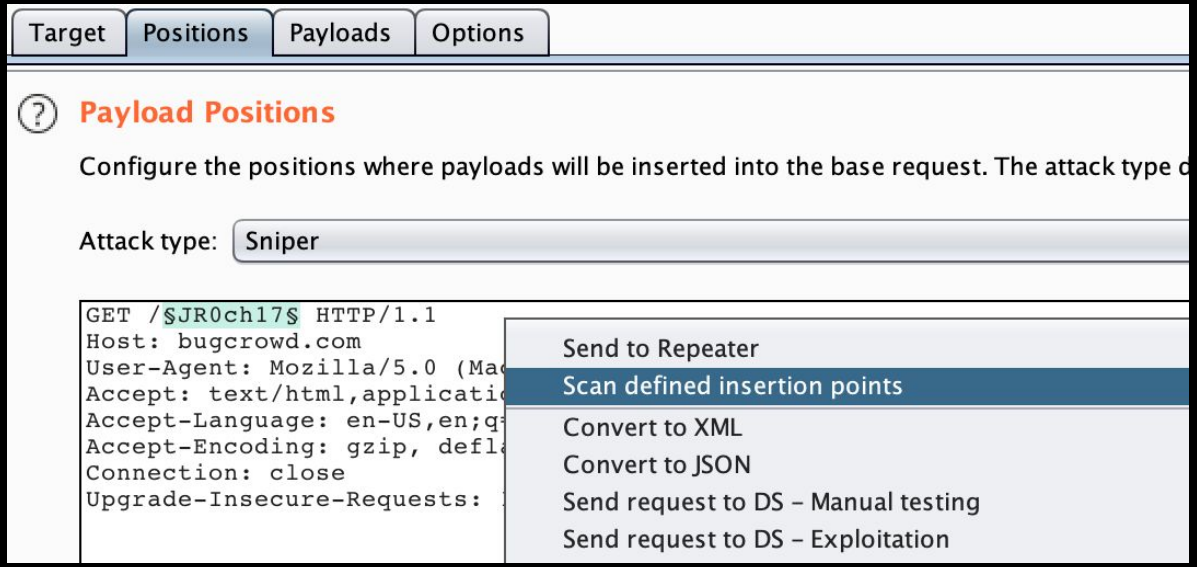
Autoscroll to search for strings when replaying requests




root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
Ctrl + Shift + I

Intruder Positions

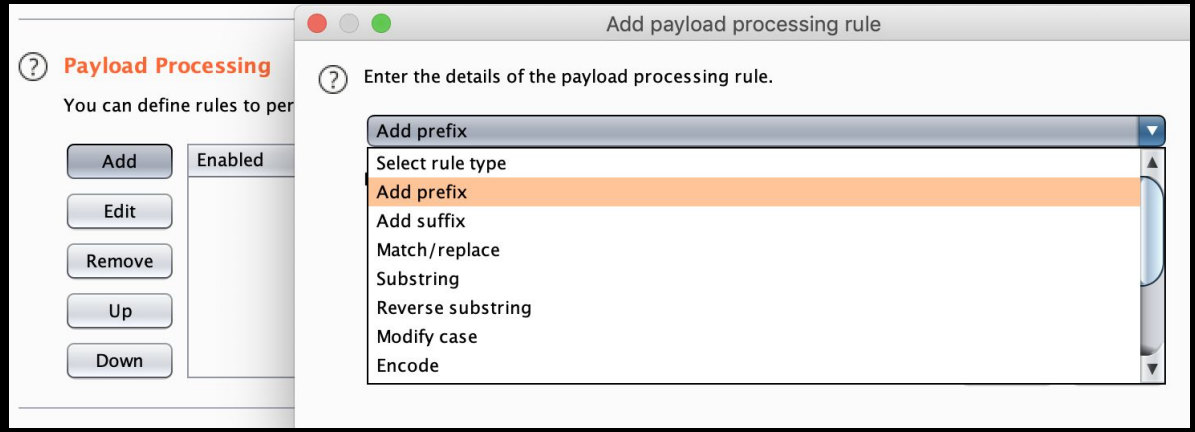
Add insert point ->
Right click ->
Scan defined insertion point



Intruder Payloads

Payload Processing

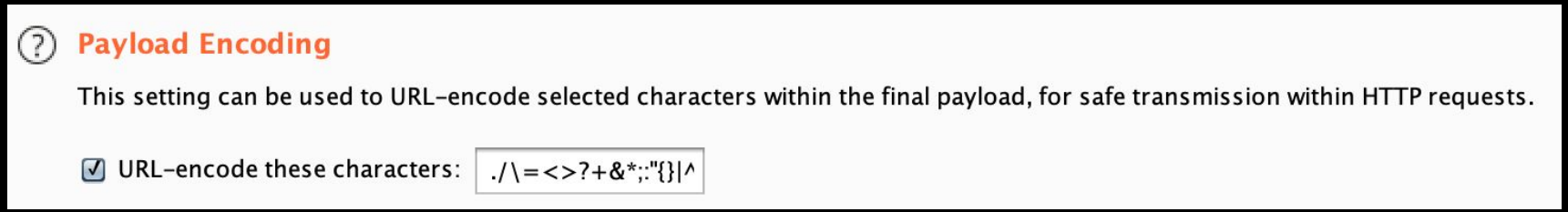
Useful for encoding, prefix, suffix, match and replace, etc



Intruder Payloads

Payload Encoding

If you have payloads with these characters, don't forget to enable/disable or add/remove certain characters

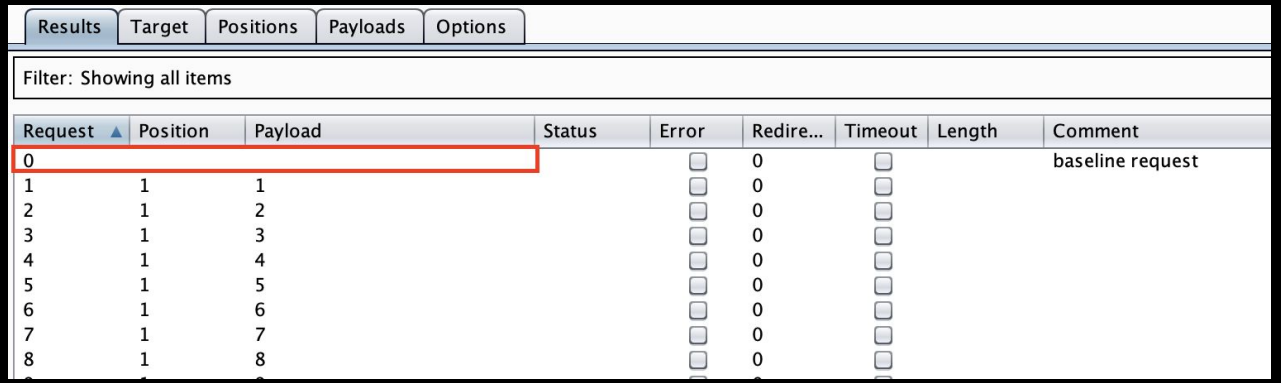


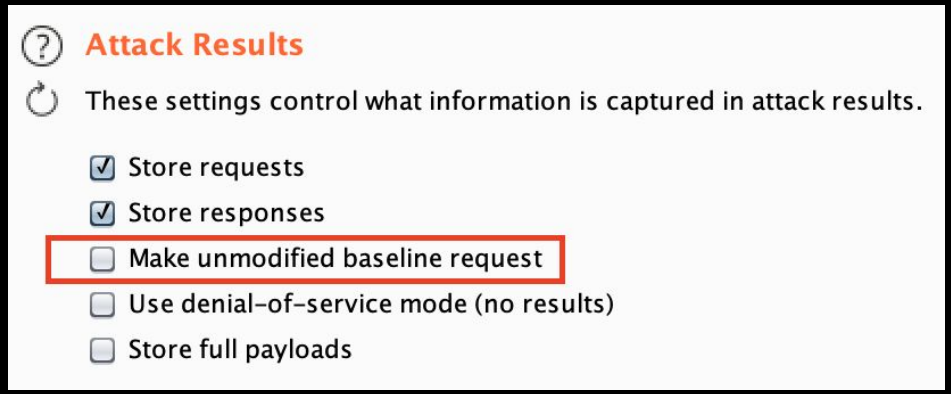
Intruder Options

Attack Results

Remove the blank line/baseline request:

Uncheck “Make unmodified baseline request”

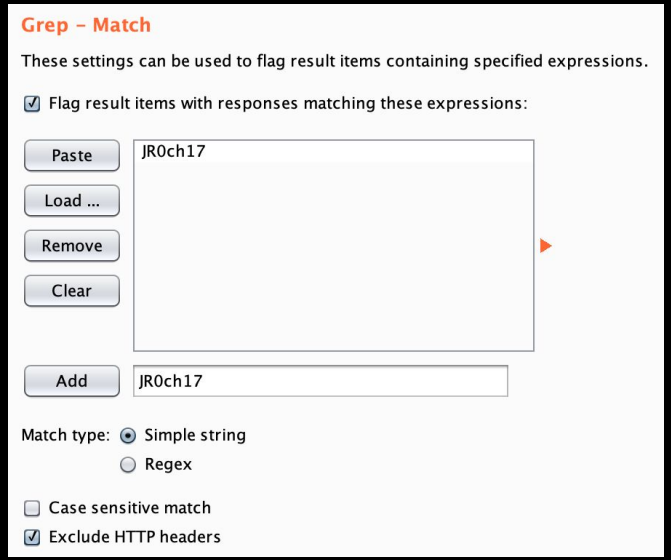


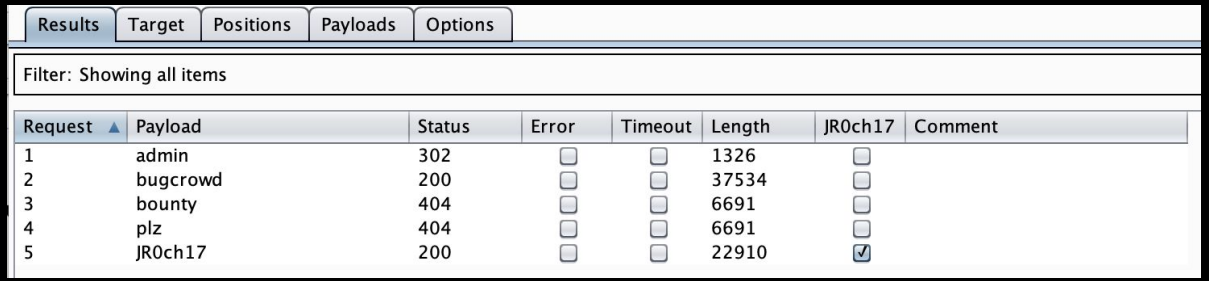


Intruder Options

If you know what to expect, use:

Grep - Match

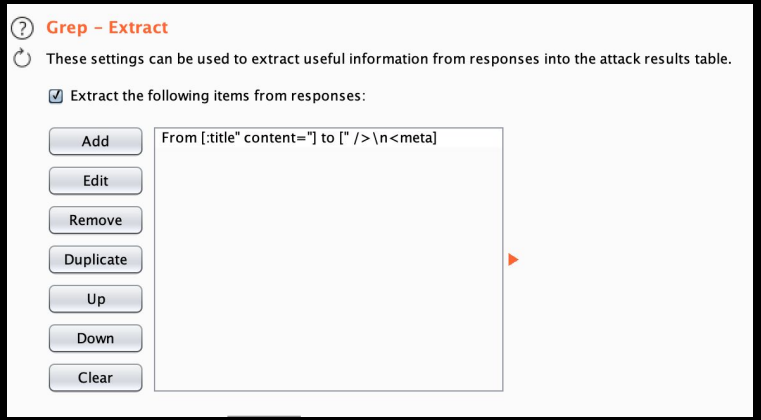


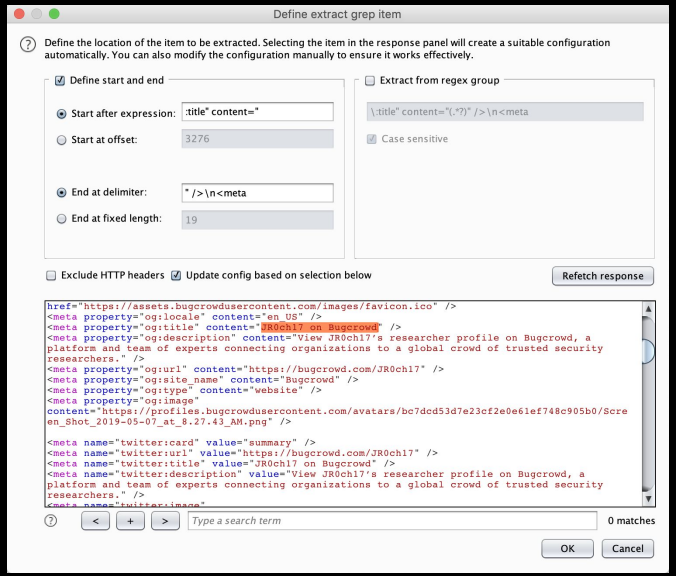


Intruder Options

If you don't know what to expect, use:

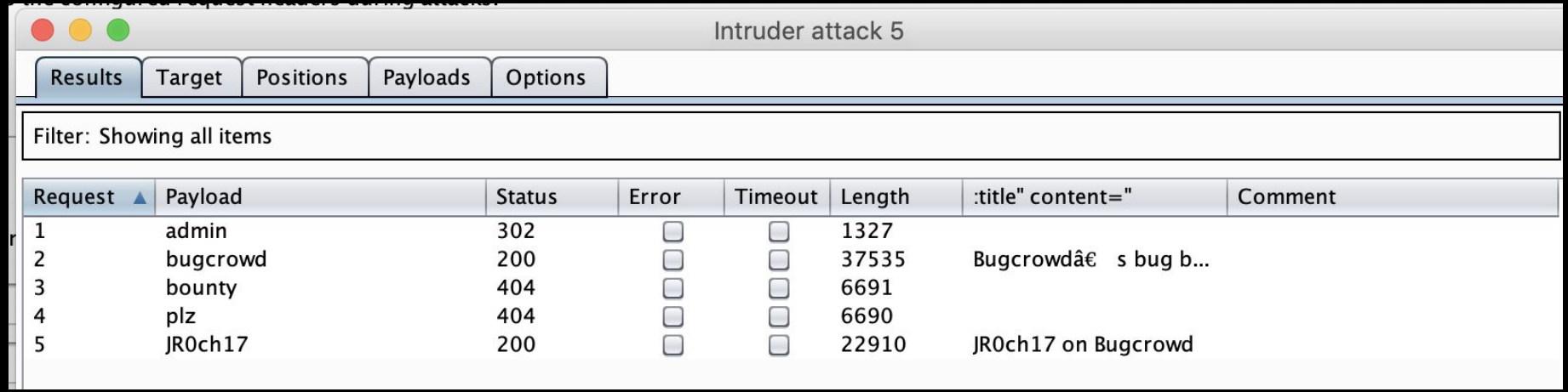
Grep - Extract





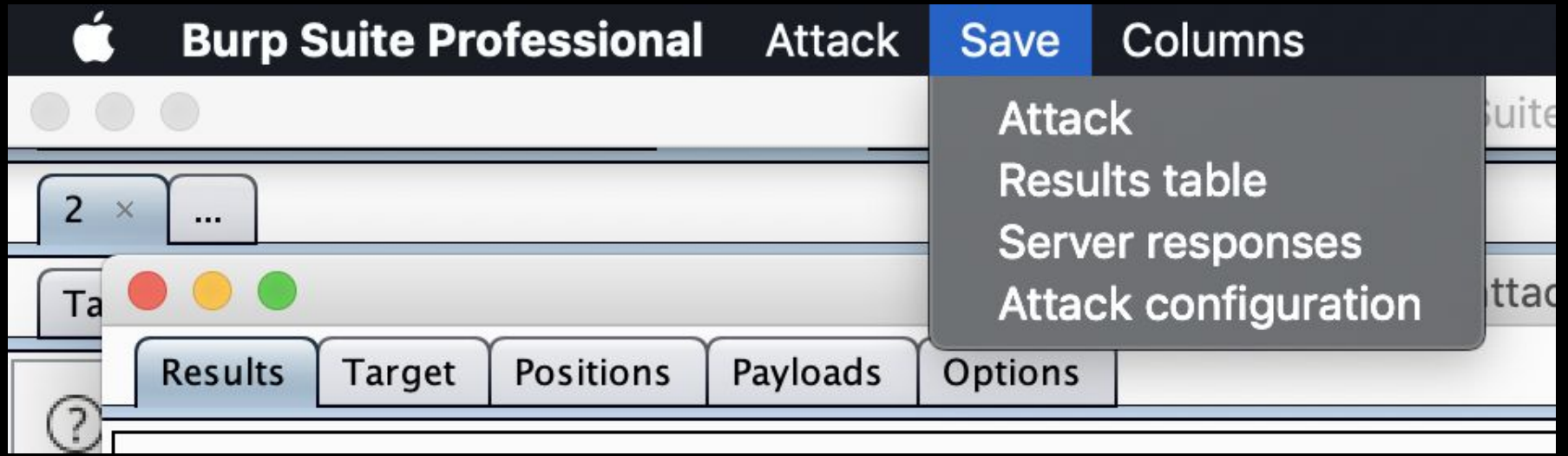
Intruder Options

Grep - Extract



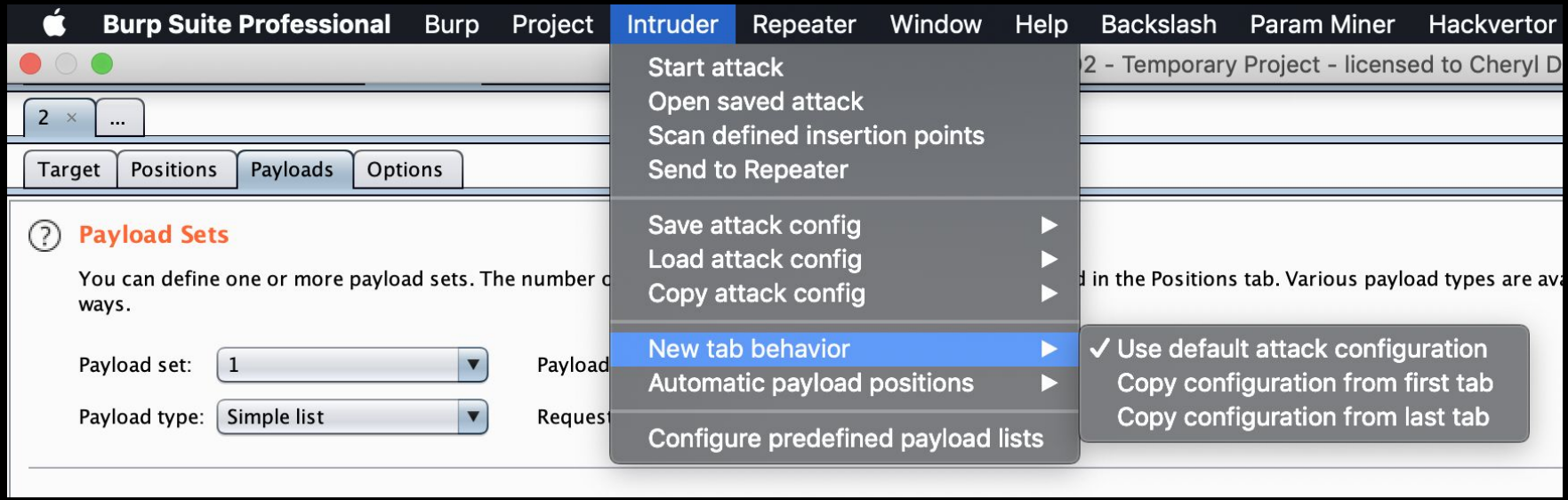
Intruder

Menu options



Intruder

Menu options



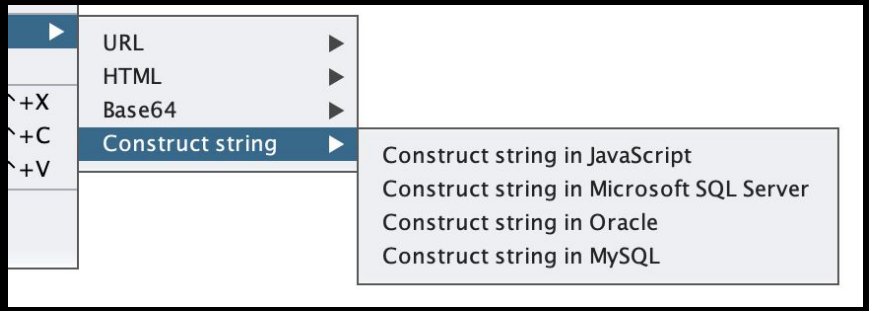
Beeder

Hotkeys/Hackvertor

Use ~~Burp Decoder~~

For common encoding/decoding (URL, HTML, Base64), use shortcuts instead

- Faster
- Prevents mistake by avoiding copy/paste



Use ~~Burp Decoder~~

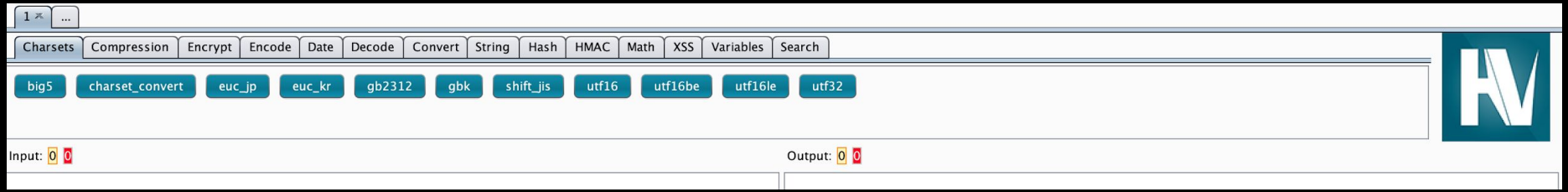
Decoder has limited functionality, replace it with Hackvertor

Hackvertor

Hackvertor is a tag-based conversion tool that supports various escapes and encodings including HTML5 entities, hex, octal, unicode, url encoding etc.

- It uses XML-like tags to specify the type of encoding/conversion used.
- You can use multiple nested tags to perform conversions.
- Tags can also have arguments allowing them to behave like functions.
- It has an auto decode feature allowing it to guess the type of conversion required and automatically decode it multiple times.
- Multiple tabs
- Character set conversion

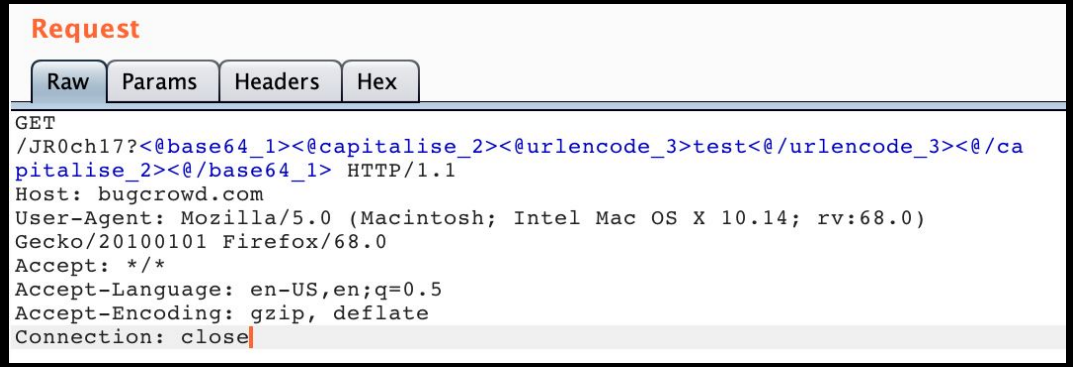
Author: Portswigger Web Security – Gareth Heyes
Version: 0.6.12
Source:
Updated: 19 Mar 2019
Rating: ☆☆☆☆☆ Submit rating
Popularity:

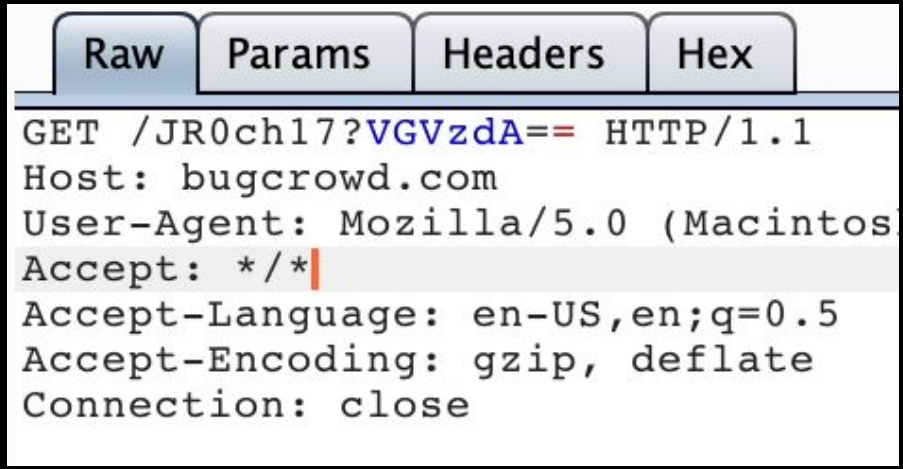


Hackvertor

https://portswigger.net/blog/bypassing-wafs-and-cracking-xor-with-hackvertor

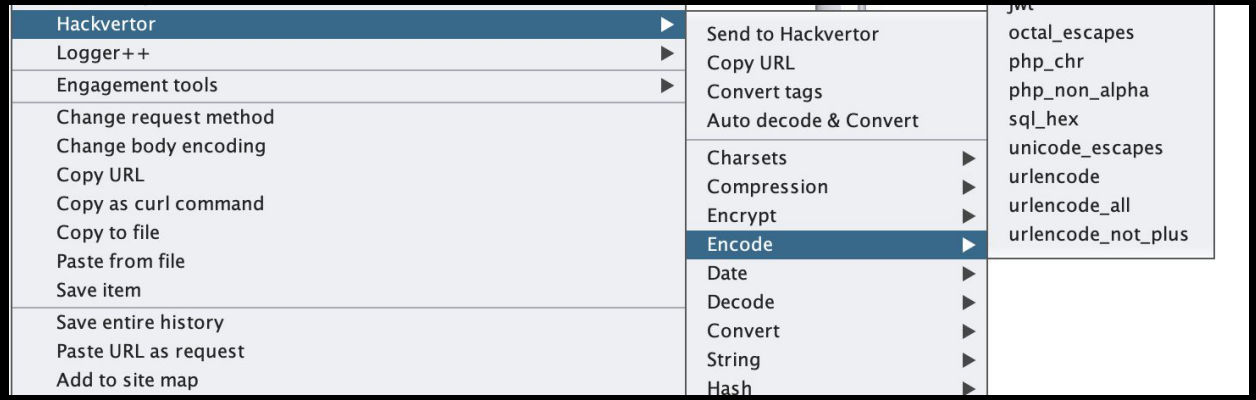
- ~150 Hackvertors (encoding/decoding, hashing, charsets, compression, encryption, conversion, etc
- No need to use online tools
- No scripting needed
- Can be used from the Repeater/Intruder contextual menu (right-click on request)
- Useful for WAF bypasses
- Extremely useful in complex encoding scenarios (ie. Base64 string inside a JSON array which is URL encoded)
- Use the Auto decode & convert

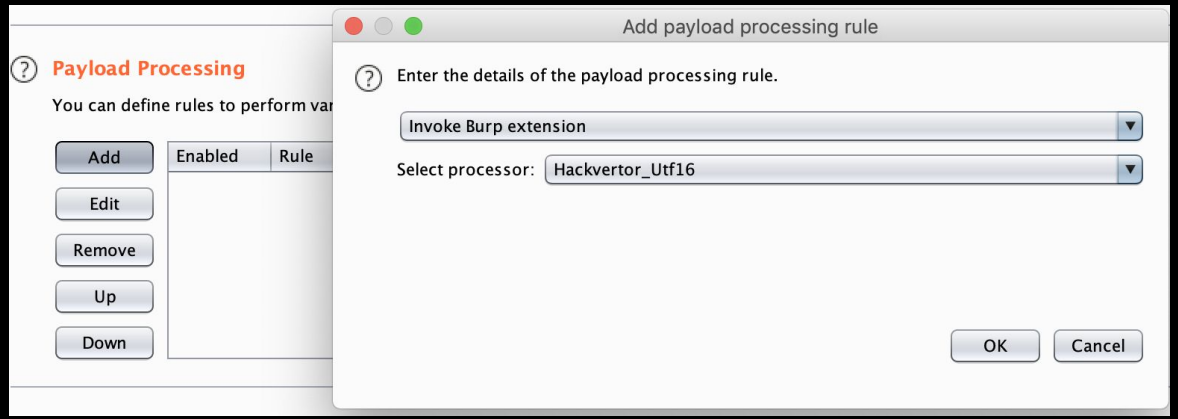




Hackvertor

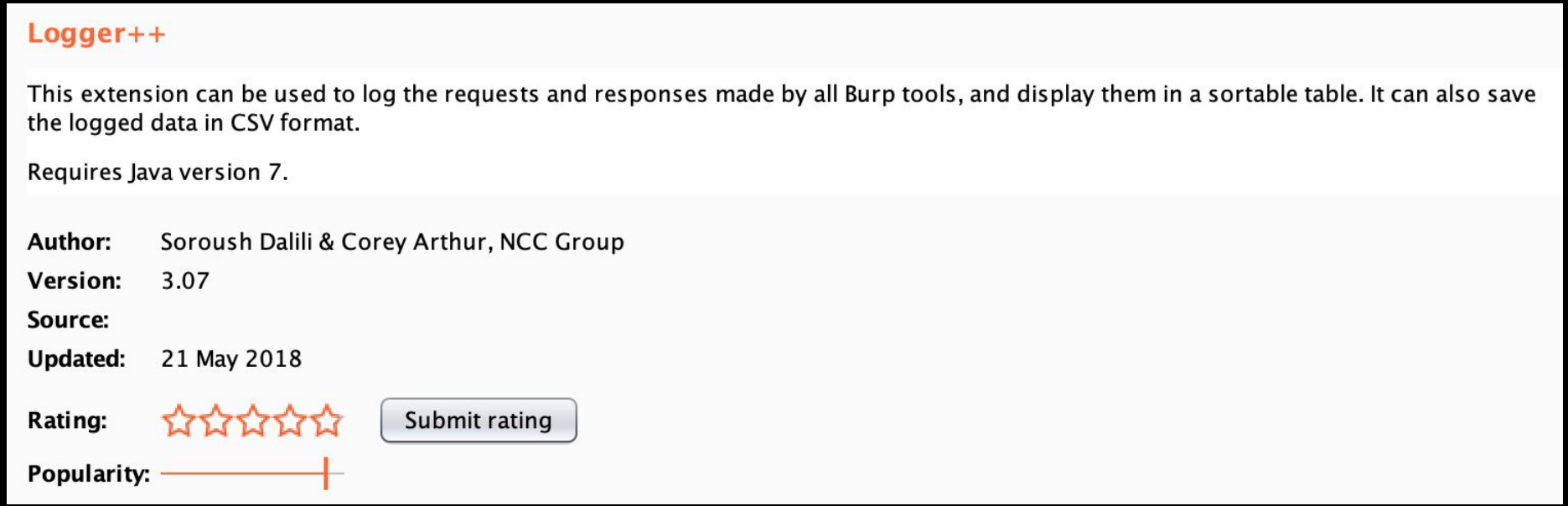
- Can be used directly in Repeater
- Can be invoked from Intruder as Payload Processing





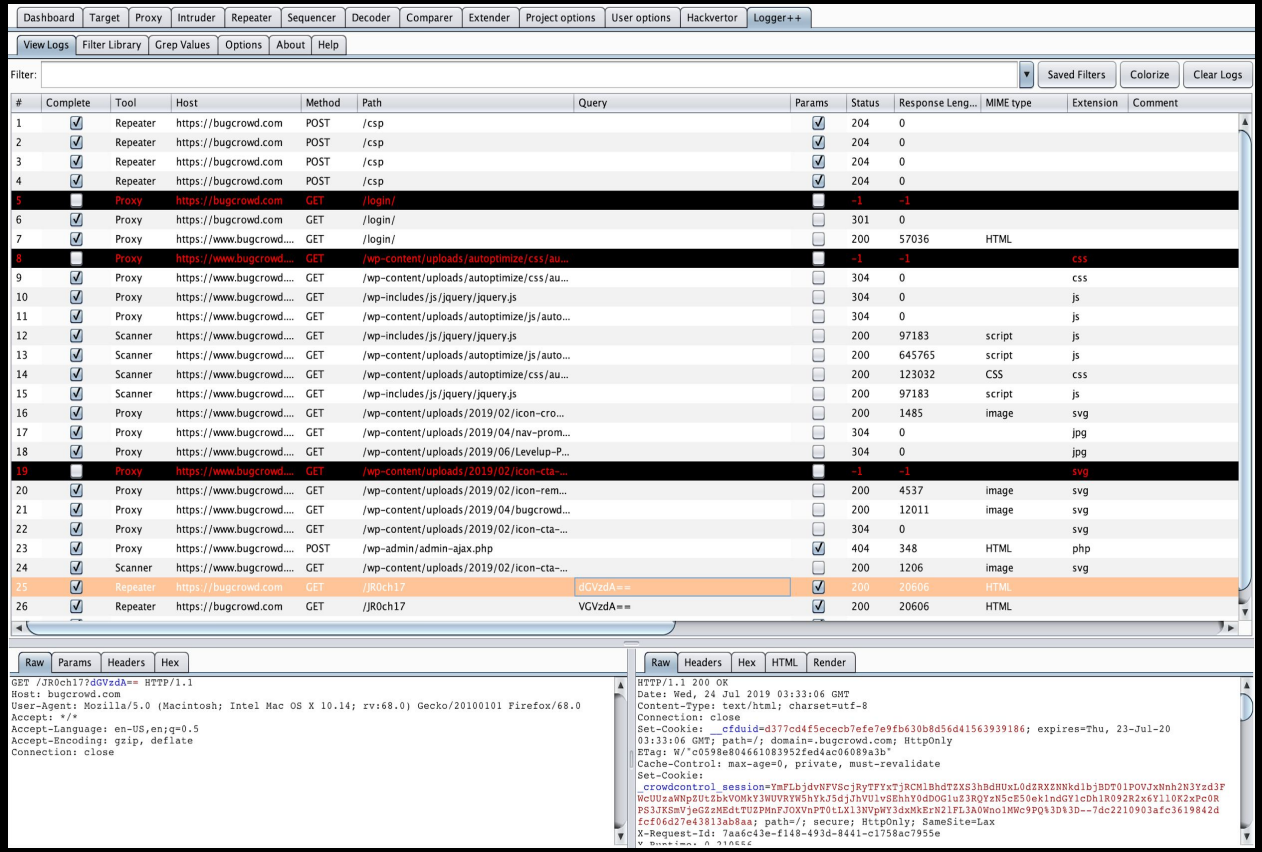

root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
Logger++

Logger++

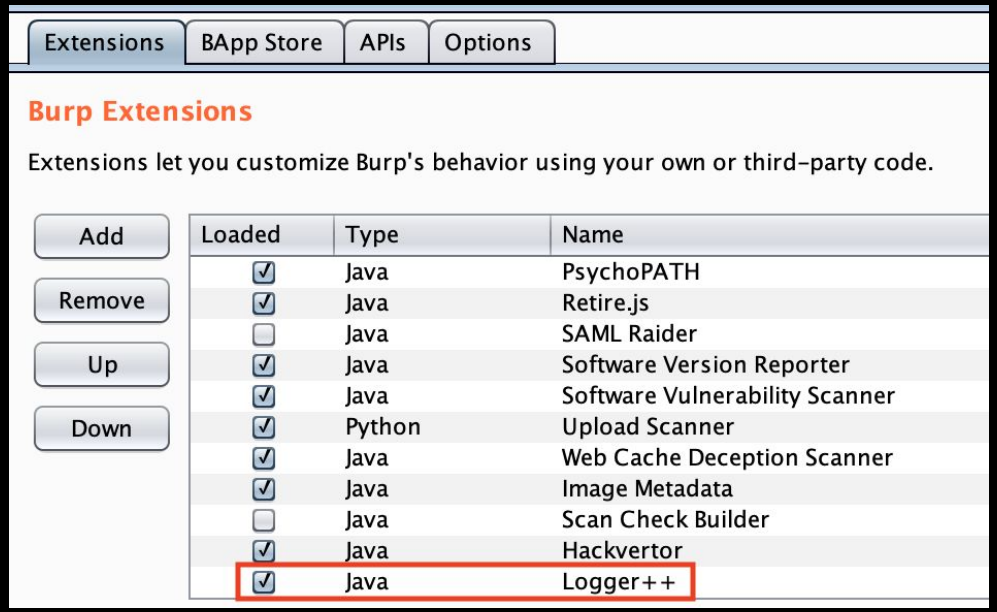

Logger++
This extension can be used to log the requests and responses made by all Burp tools, and display them in a sortable table. It can also save the logged data in CSV format.
Requires Java version 7.
Author: Soroush Dalili & Corey Arthur, NCC Group
Version: 3.07
Source:
Updated: 21 May 2018
Rating:
Submit rating
Popularity:

Logger++

- View all requests sent by Spider, Repeater, Scanner, extensions, etc
- Logs can be saved to CSV or sent to ElasticSearch cluster
- Use Regex to grep for values in filters which can then be saved for later use

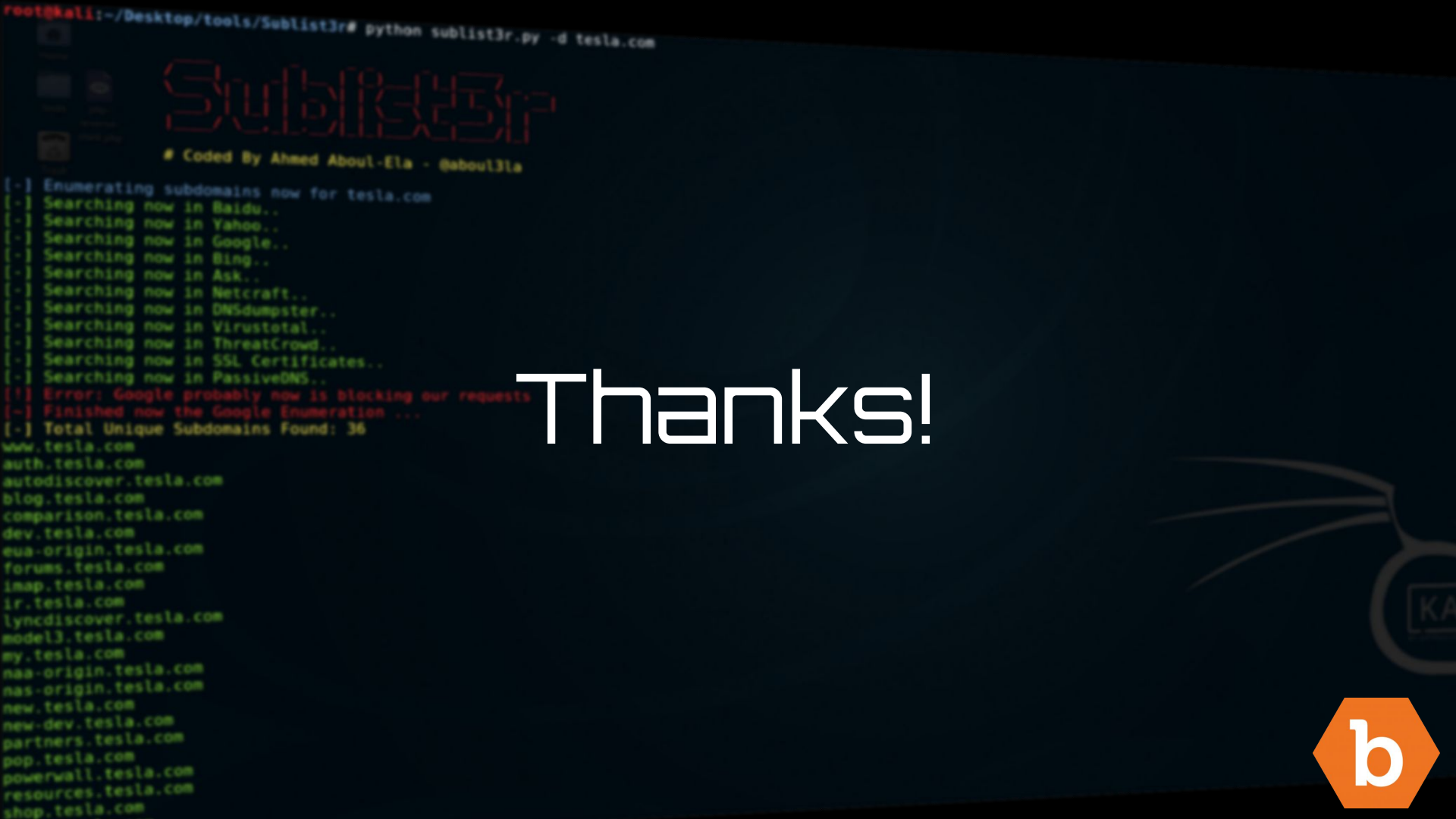


Logger++



Needs. To. Be. The. Last. Extension. In. The. List.

Resources & References


root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
Thanks!