Burp Suite Introduction

Bugcrowd University

bugcrowd.com

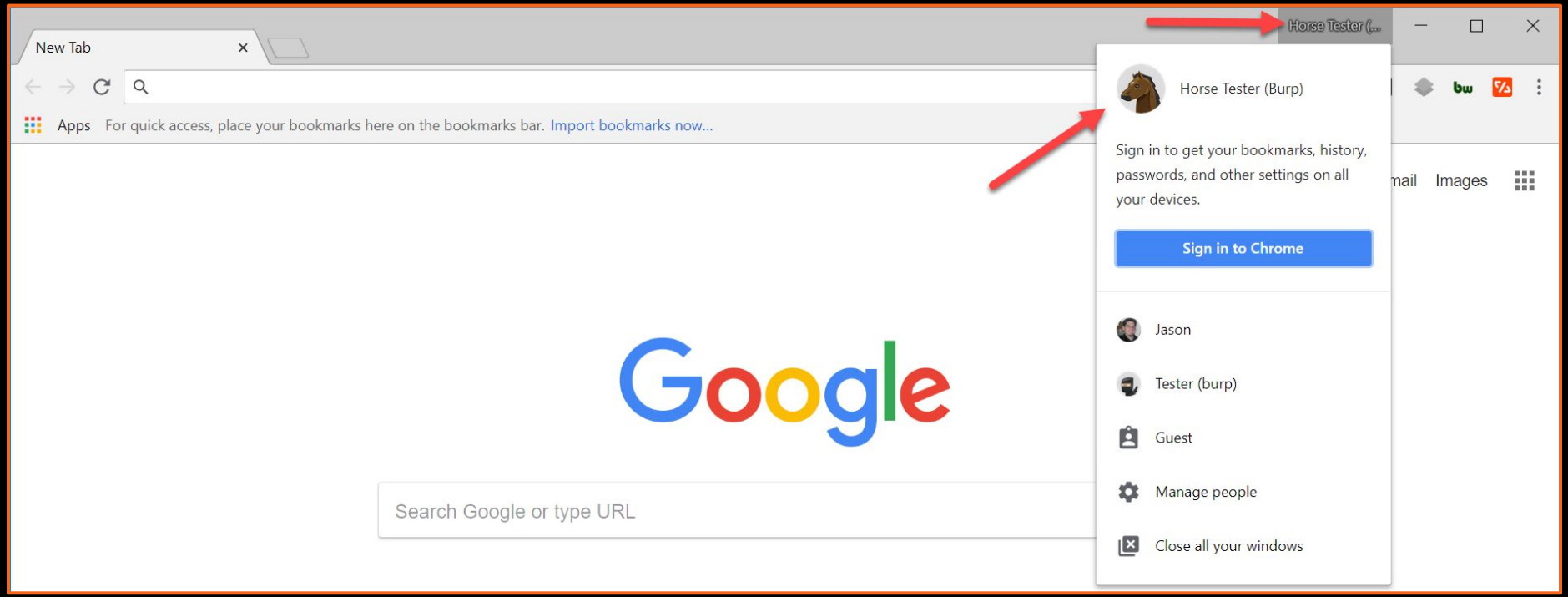
Module Trainer

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

Browser Setup

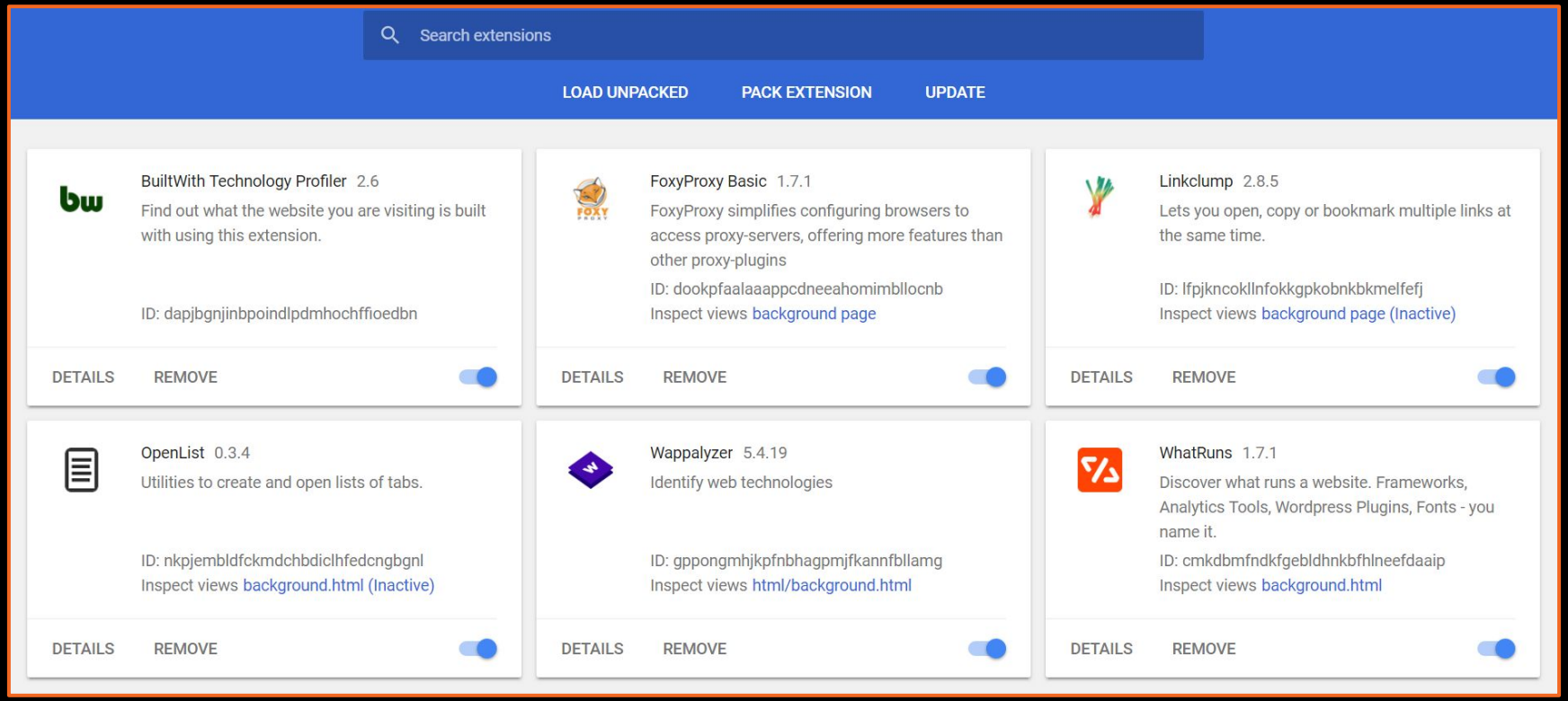
Browser Profiles (don't leak your creds!)

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.



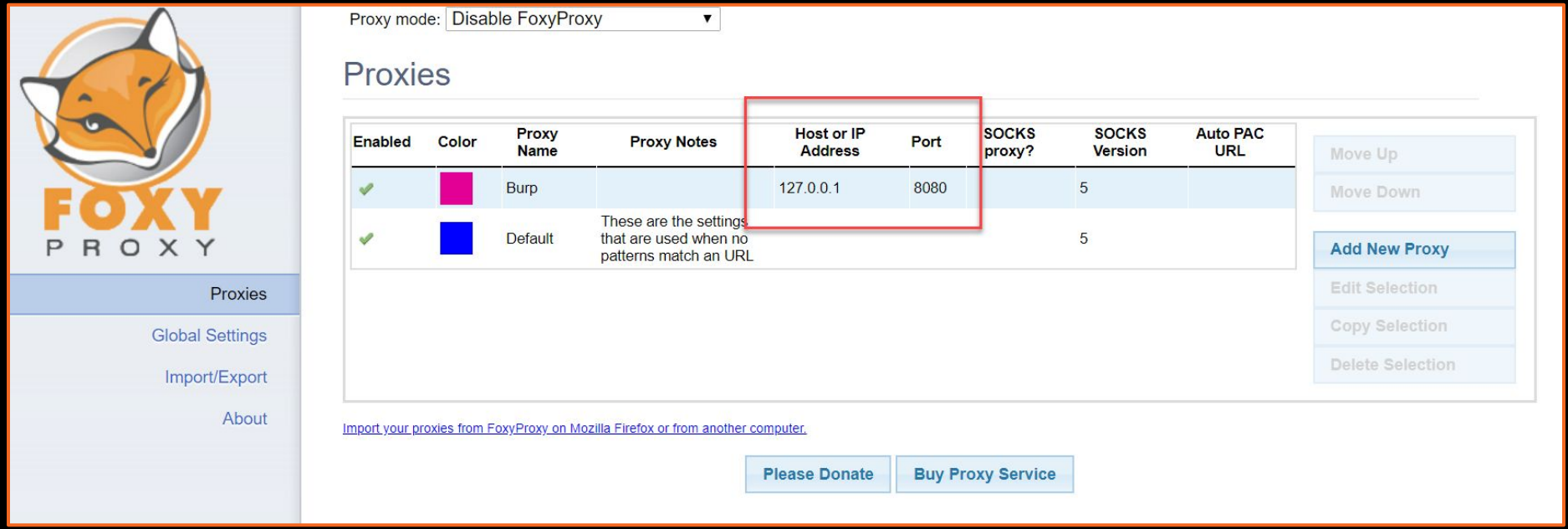
Useful extensions

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.



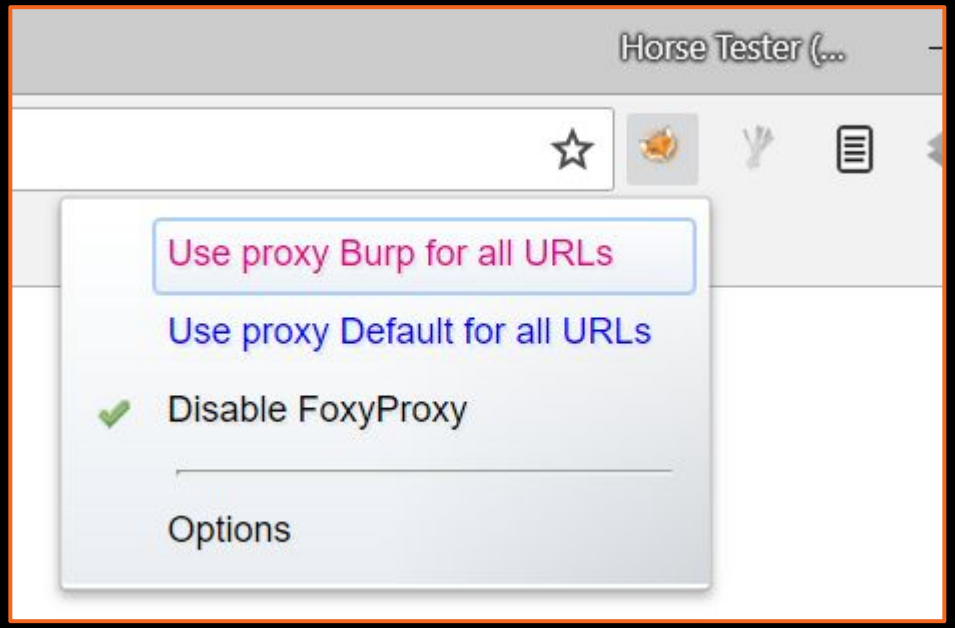
FoxyProxy or Similar

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

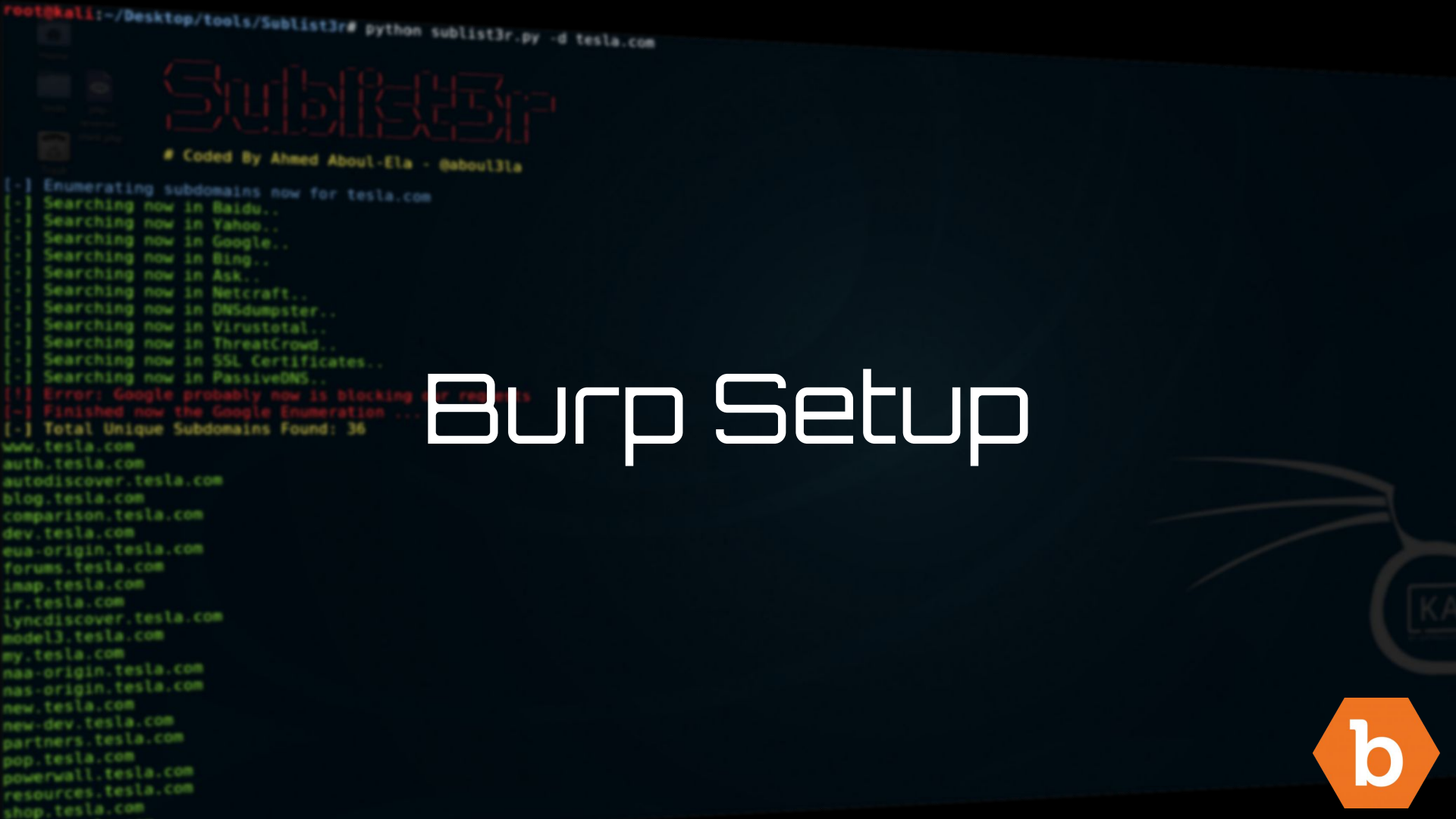


FoxyProxy or Similar

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.

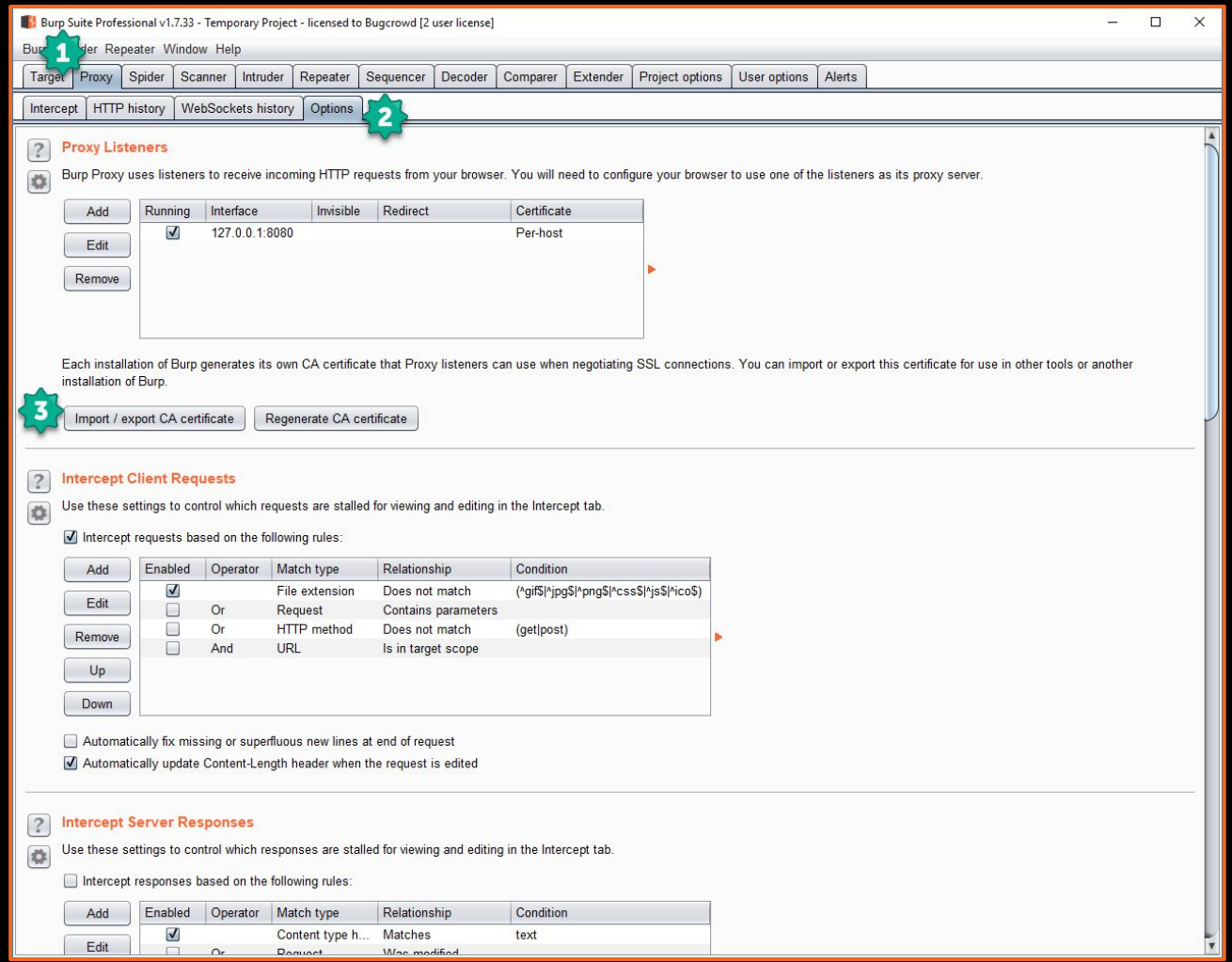


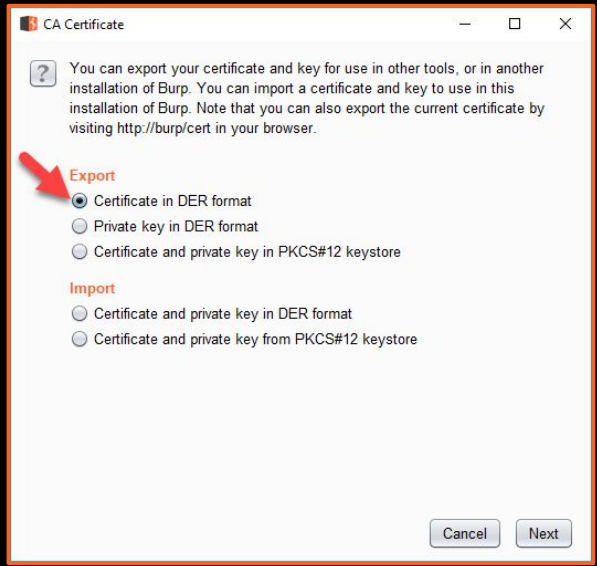
IPVANISH VPN

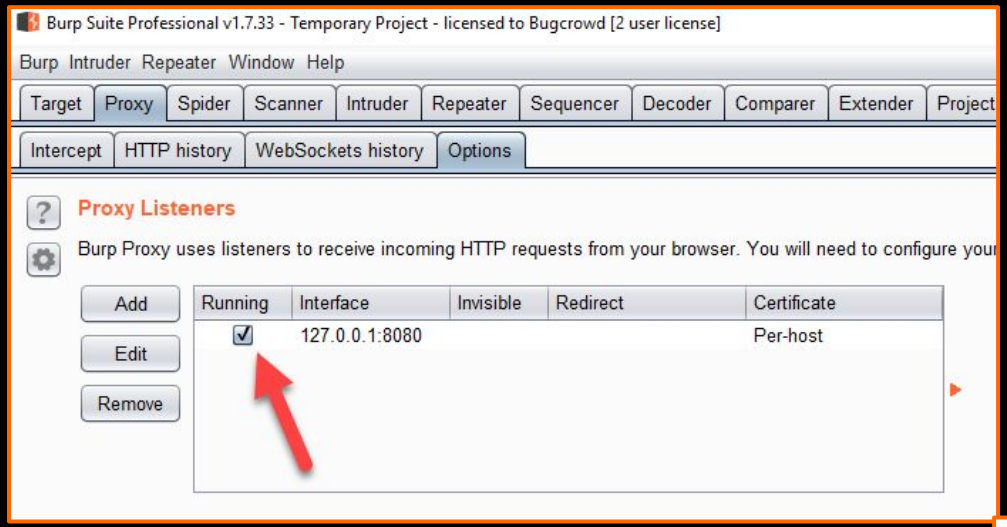

root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching 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 Setup

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.

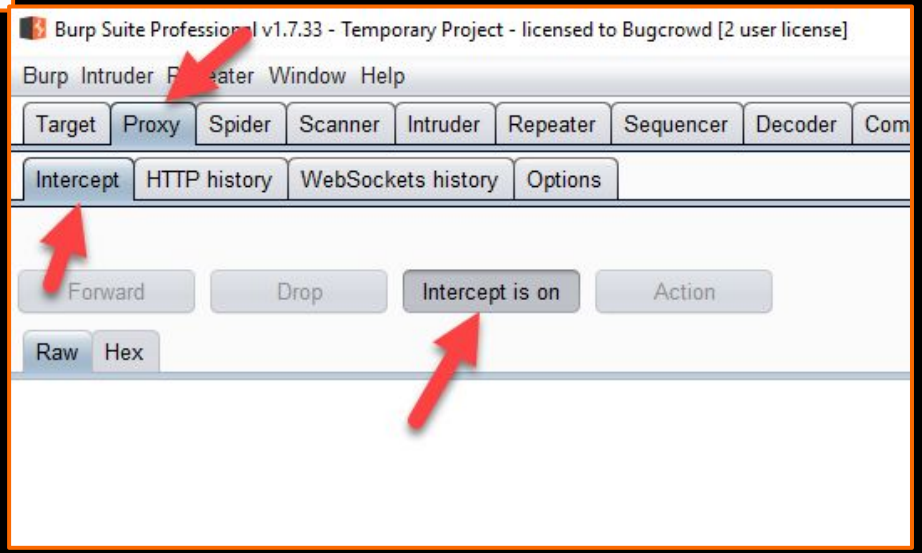






Ensure proxy is up and intercept is off

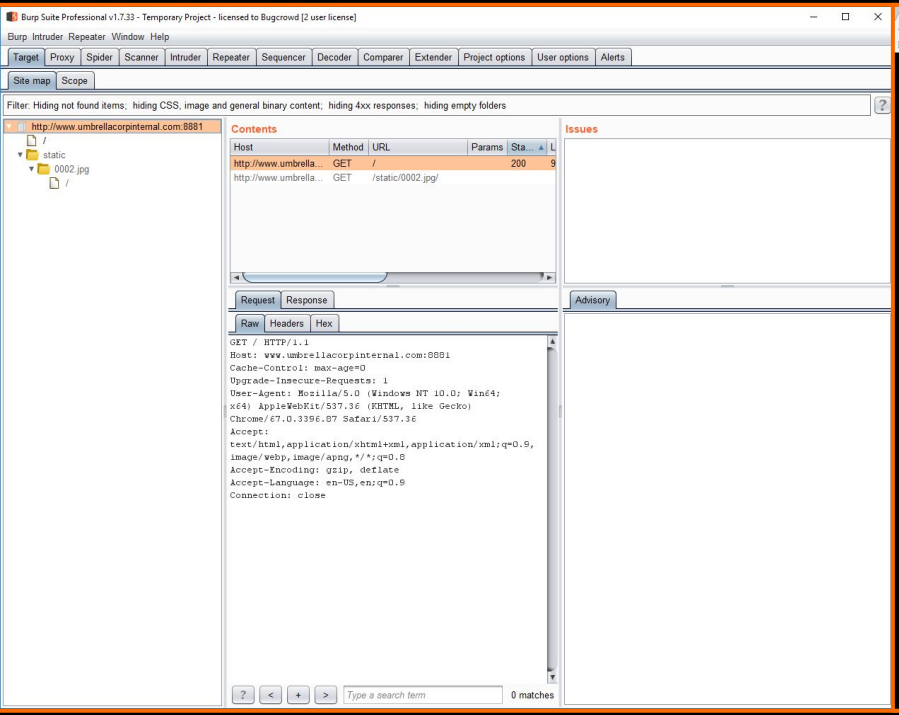
Burp starts up with interception turned on.



Proxying a Target

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

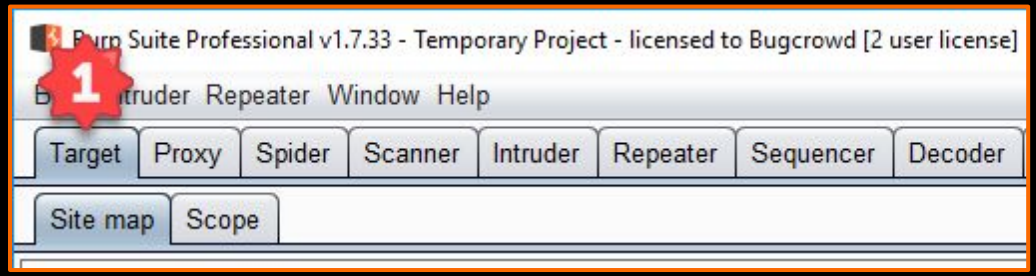
But can you get in?



Burp Core Tools

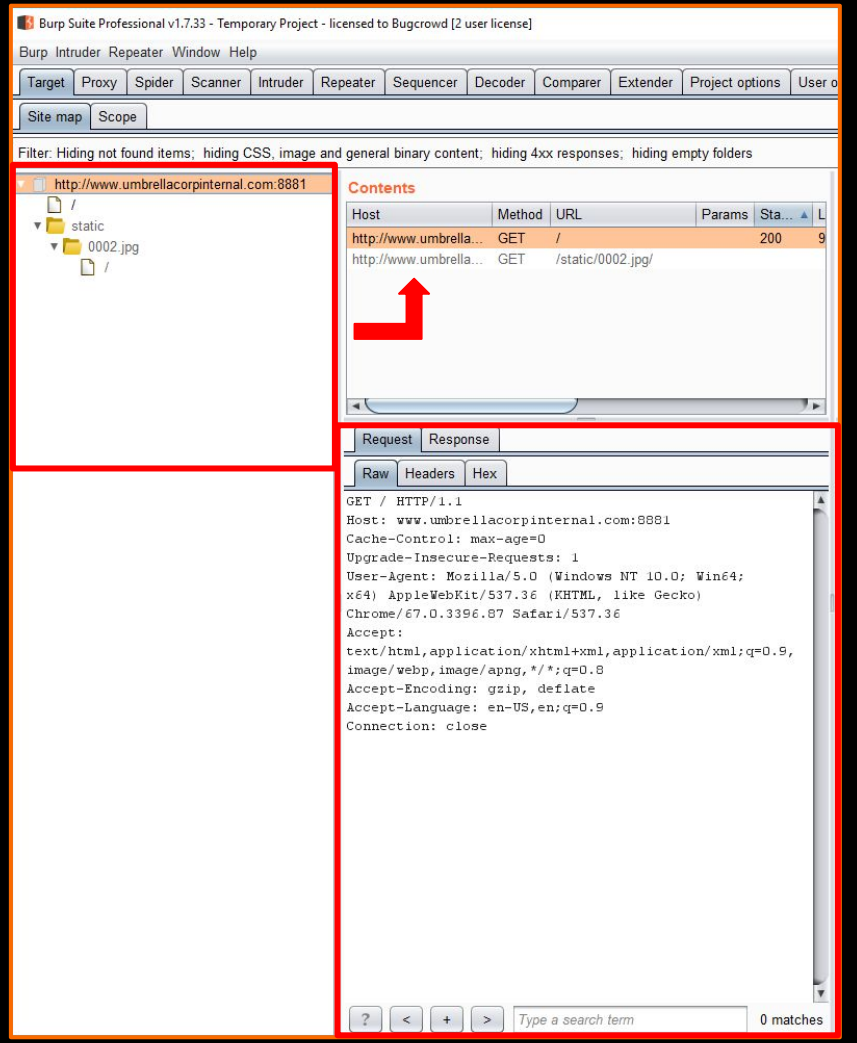

root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching 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: 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

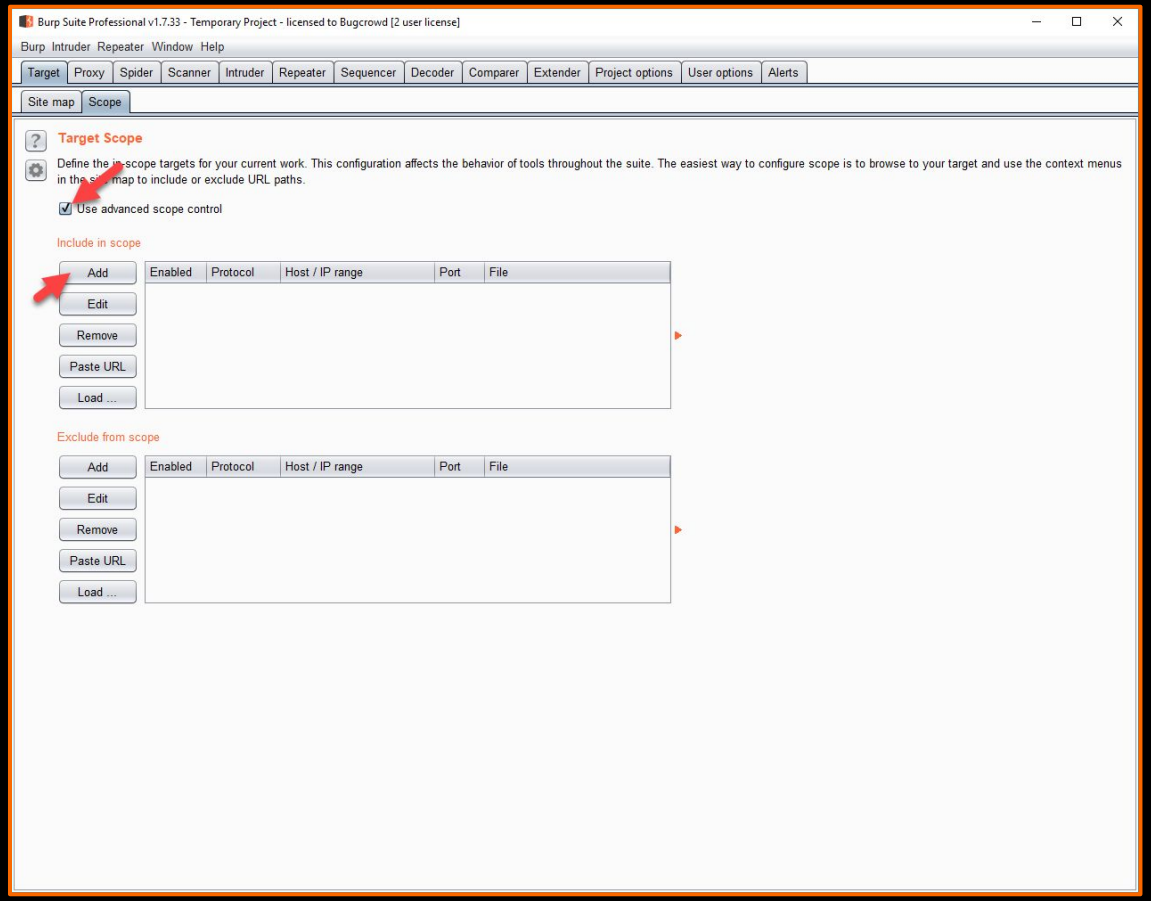


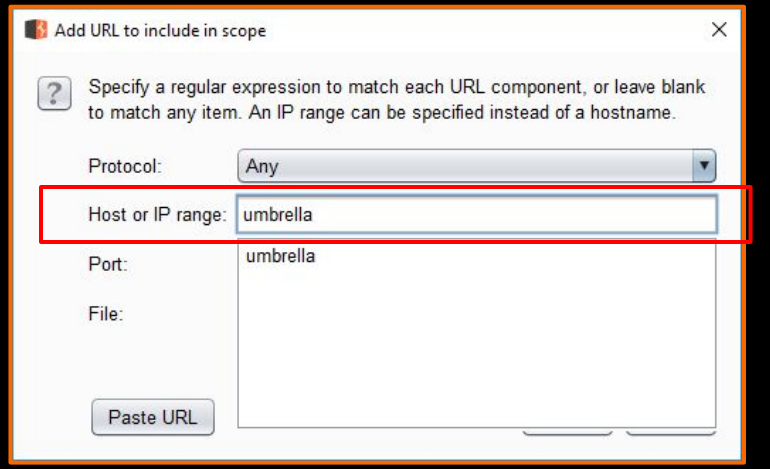
The Target Tab is an overarching tree style view of all websites in scope.

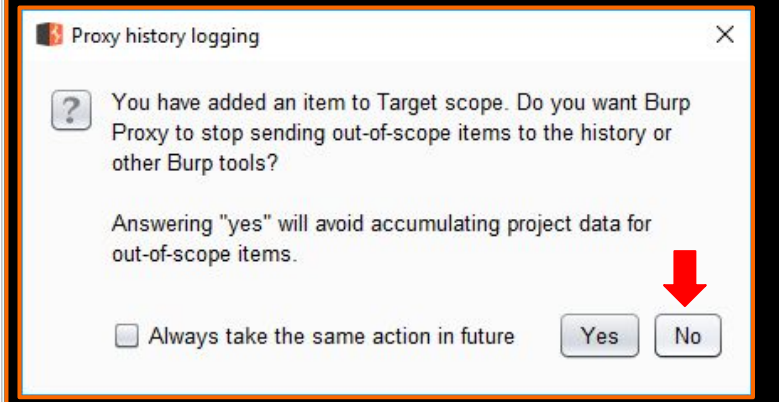
Icons designate what type of content each node is. You can select a single path and see only requests you've made in that area.



Scope - What Do You Want to Focus On?



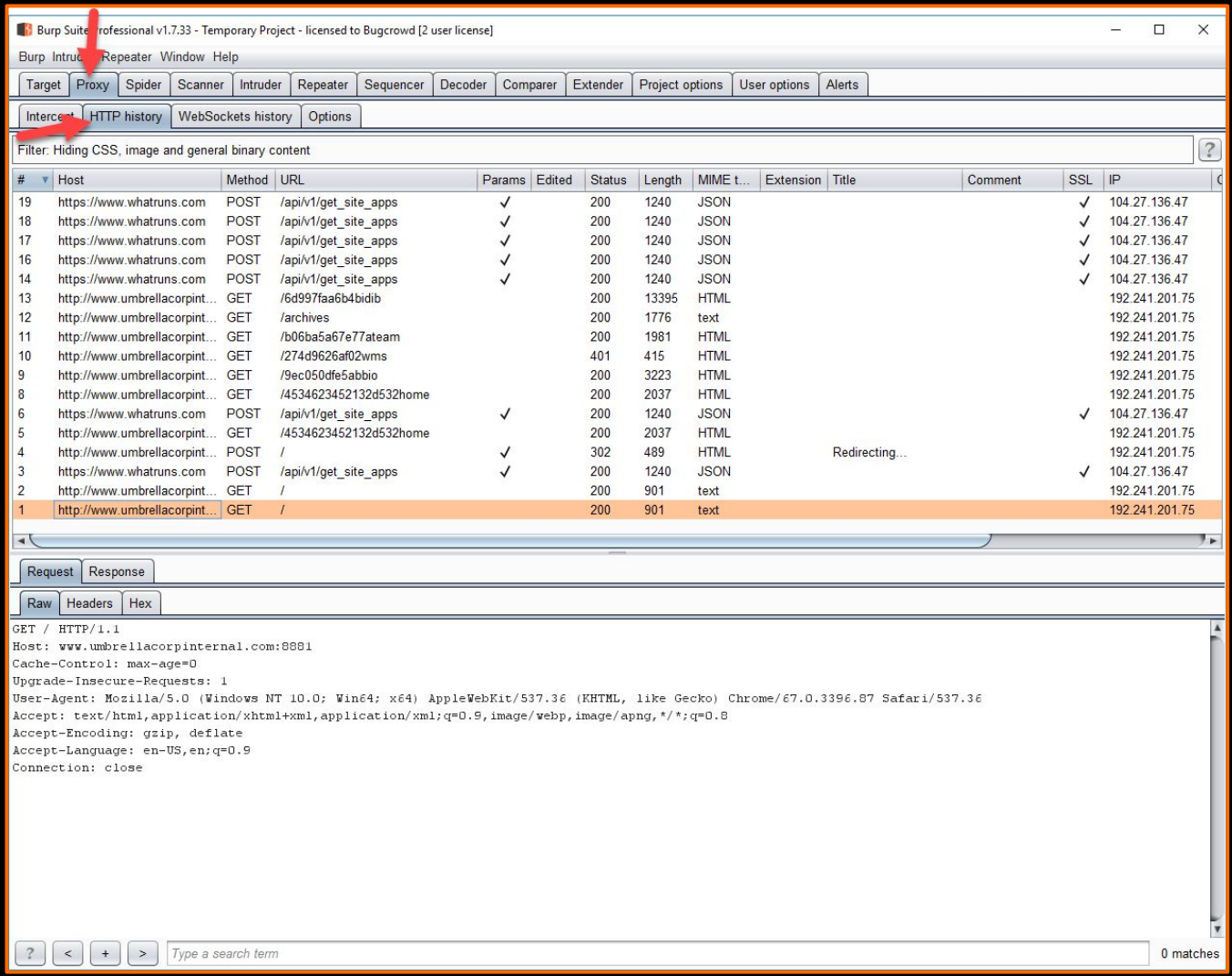




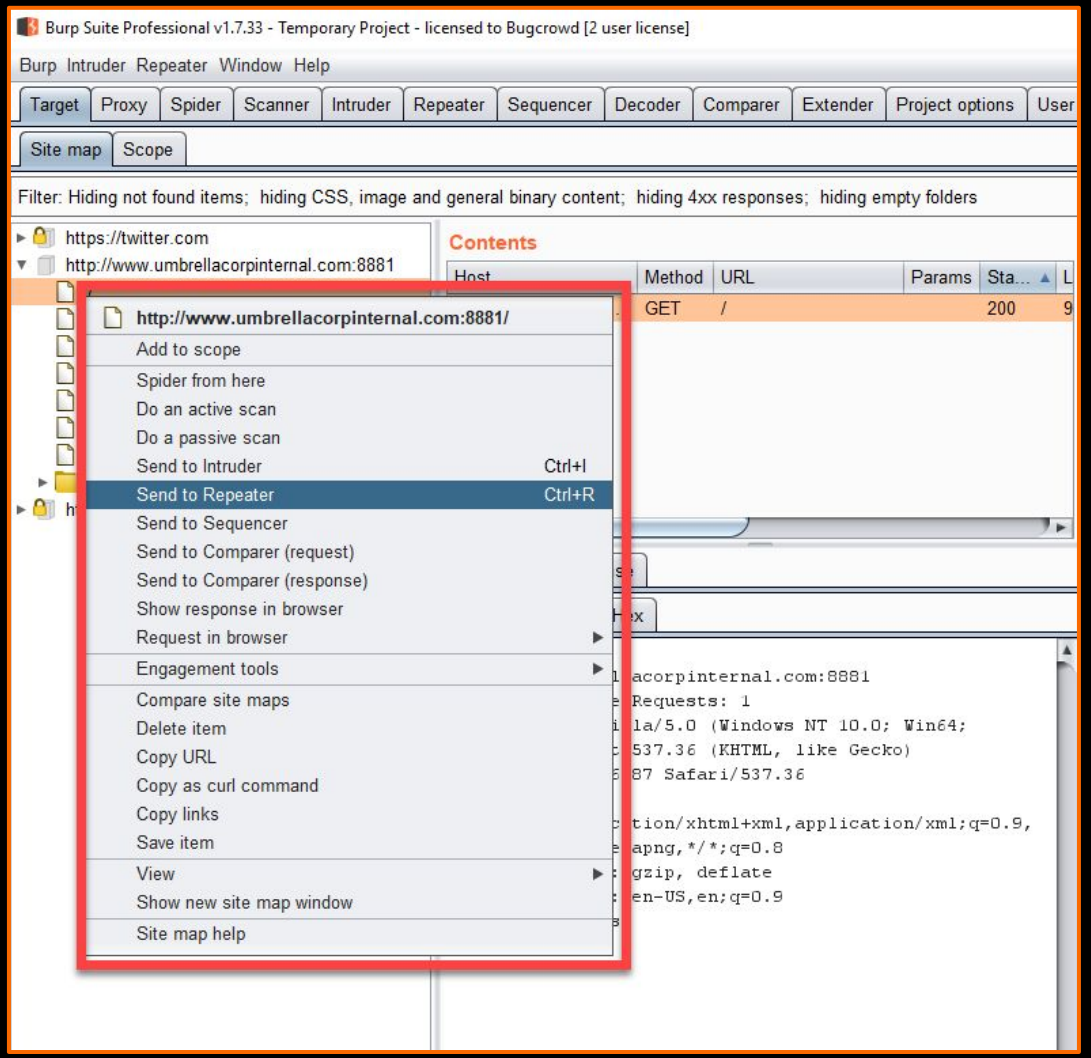

root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] 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

Proxy Tab

Proxy - Listed, ordered view

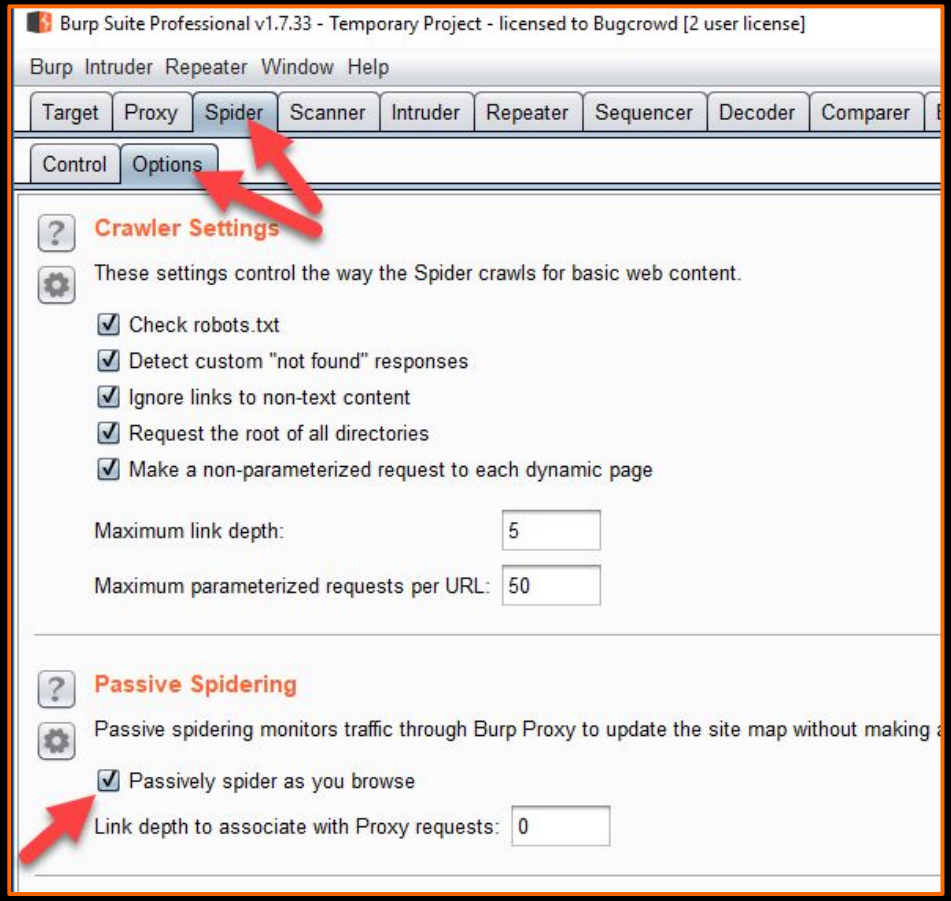


Right Click - Context Menu (all tabs)



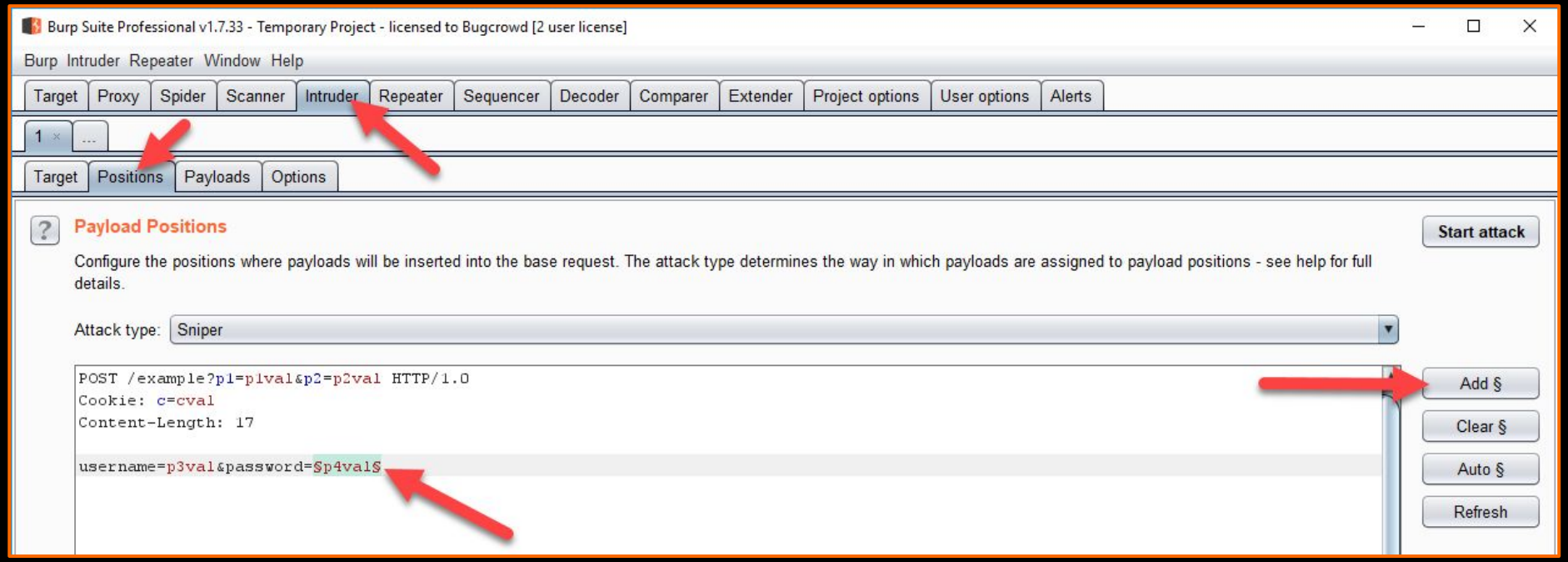

root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] 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
Spider

Spider - spider control & disable passive spider



Burp Intruder

Burp Intruder - The Basics



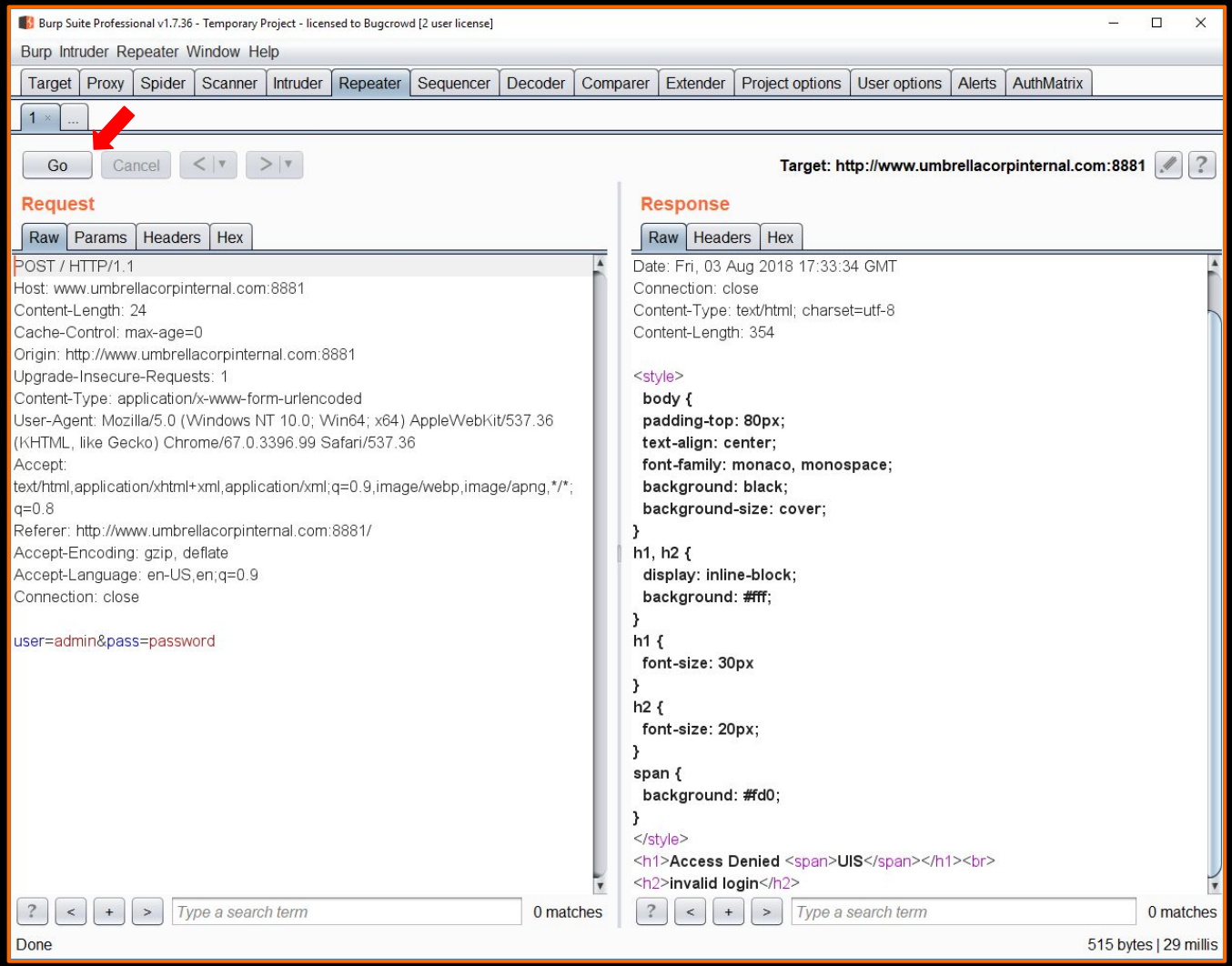
Intruder Lab – Bruteforcing forms


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
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

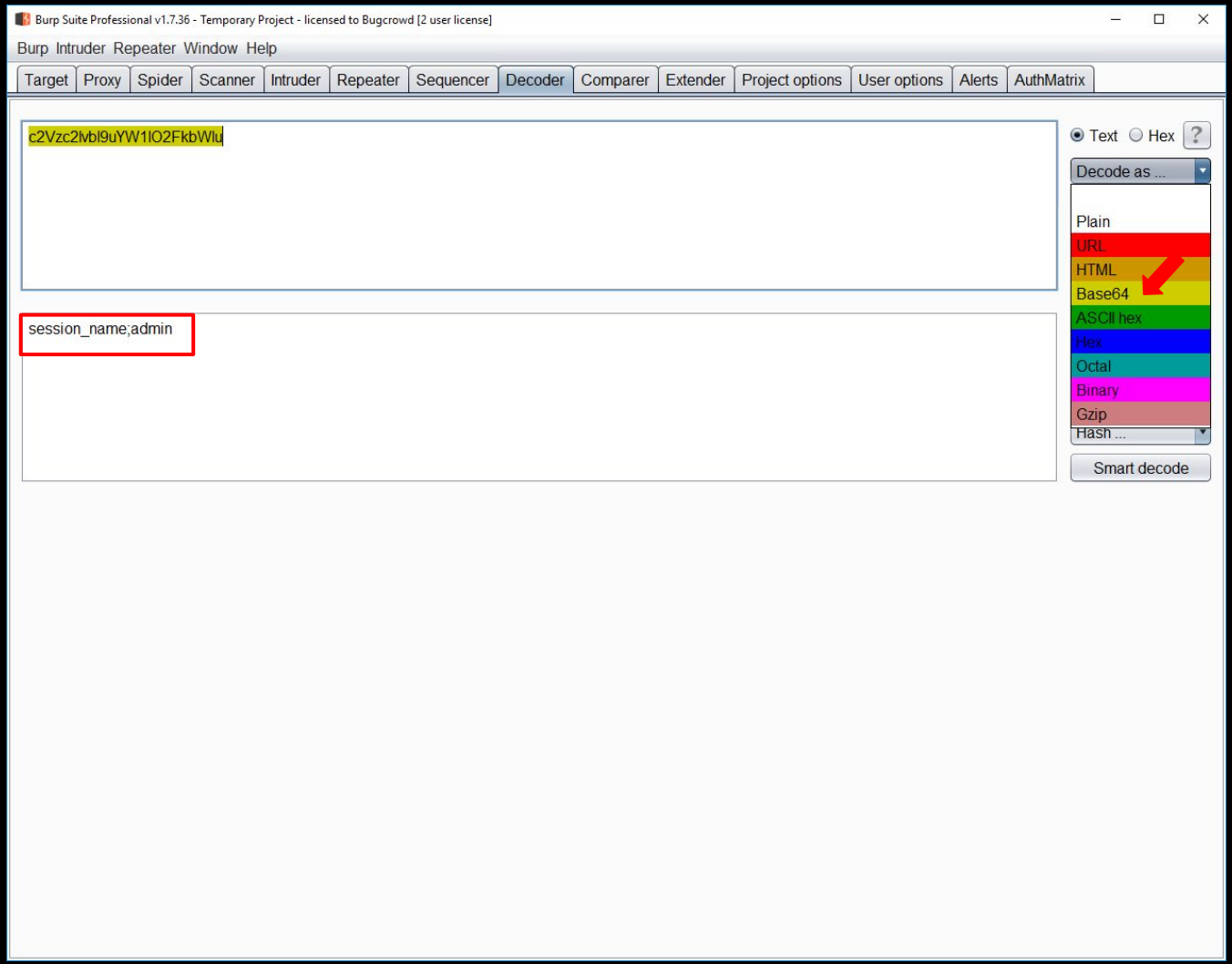
Repeater provides us a powerful tool to replay individual requests and tamper with them. Often called “manual” testing.




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

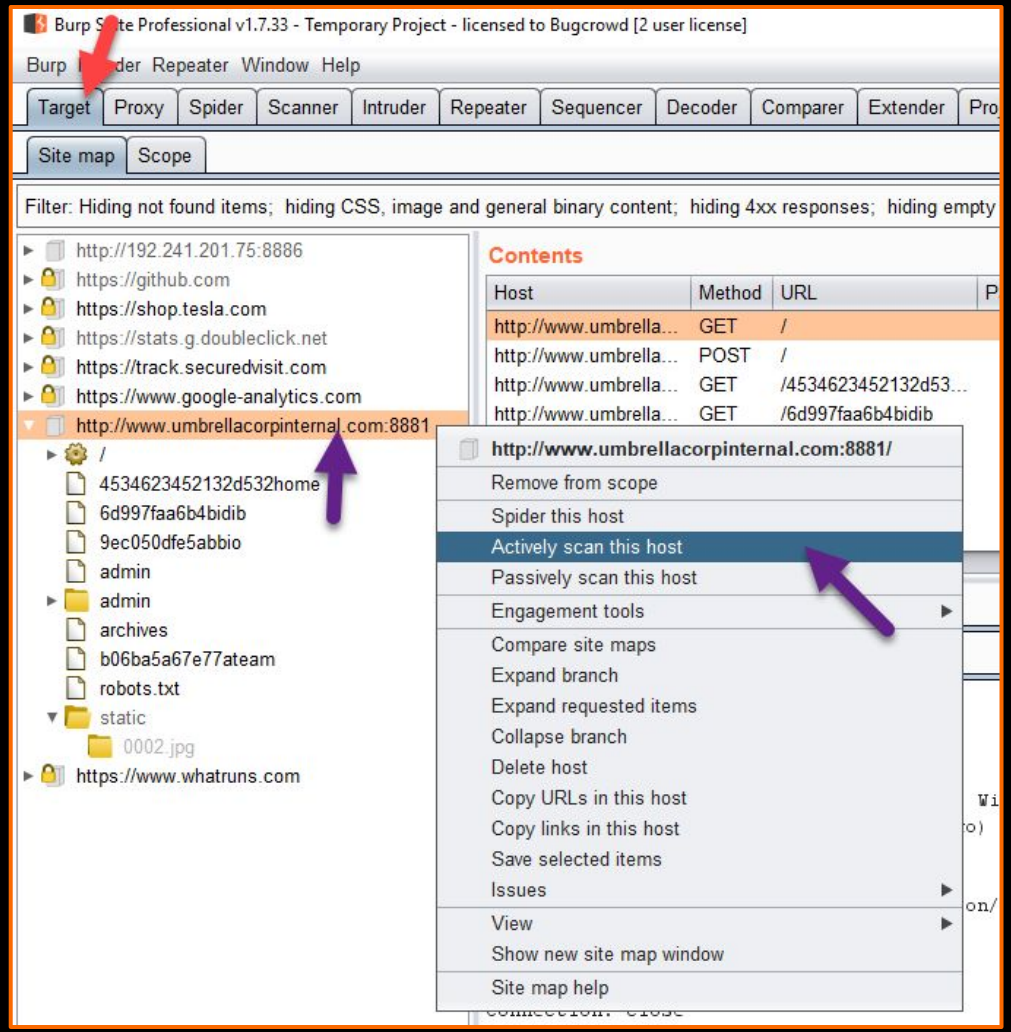
Decoder

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

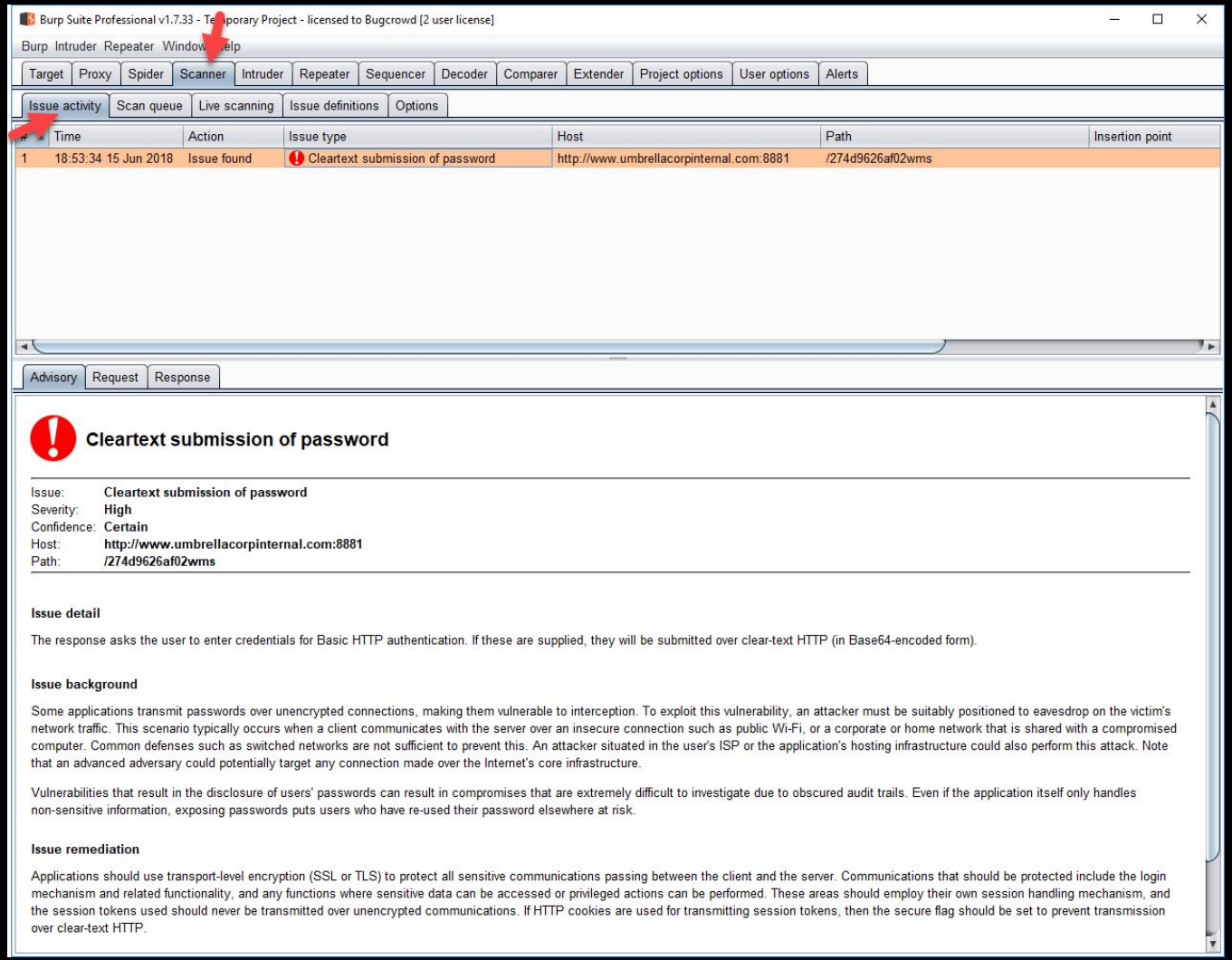



root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] 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



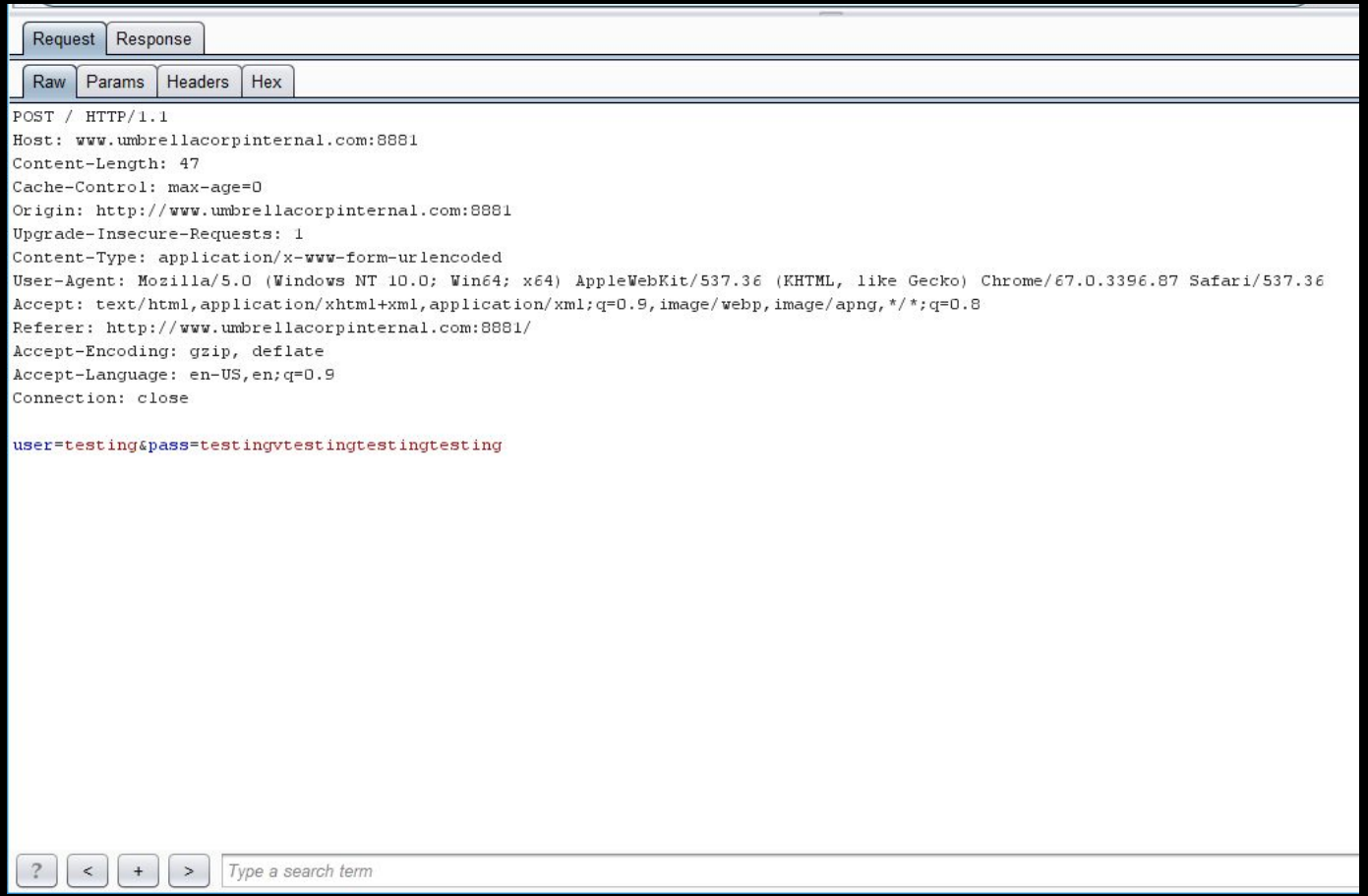
Burp Scanner - Automated Scanning



Burp Scanner - How Does it Work?

Spider finds all input points on a request:

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



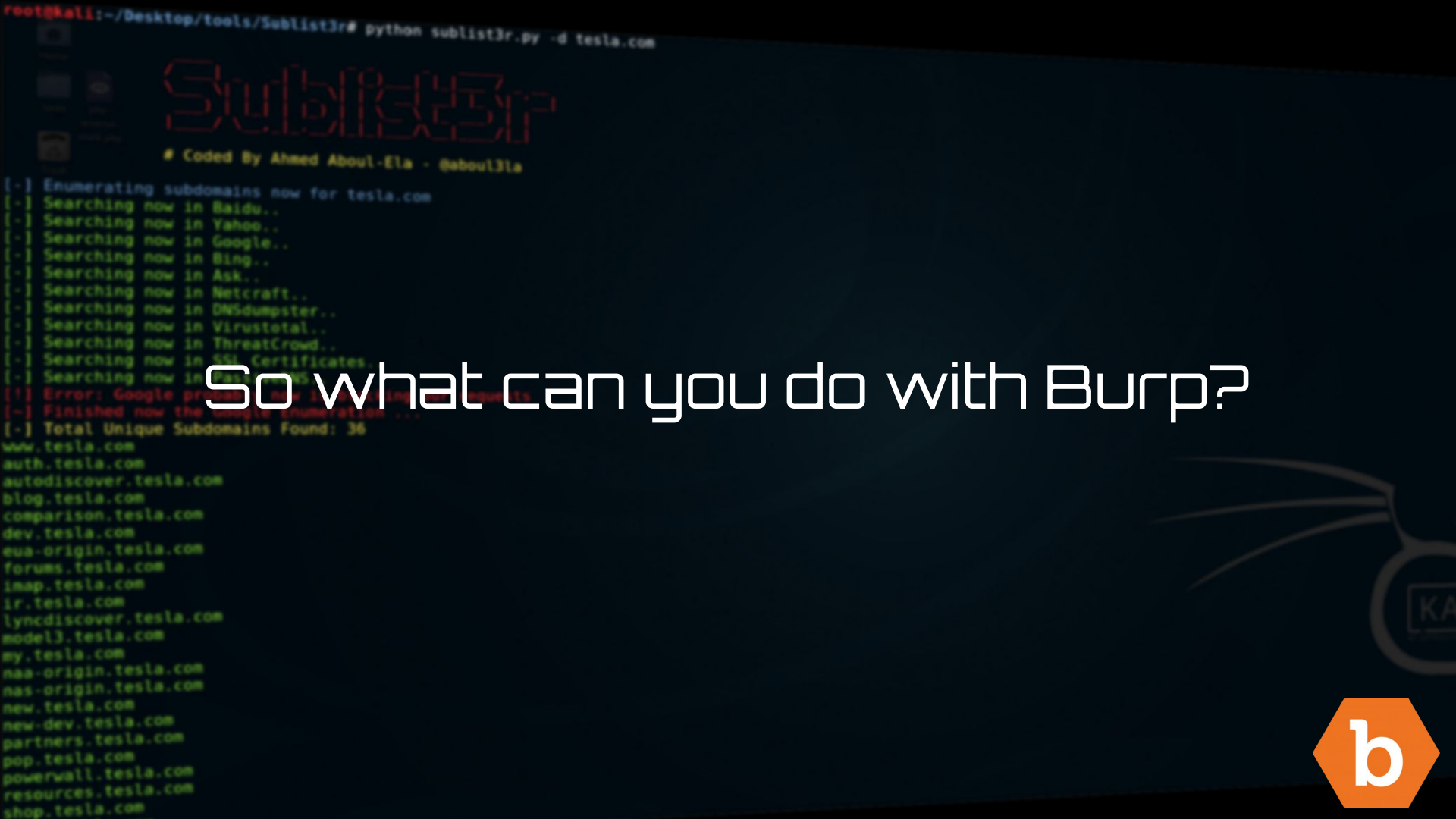
Burp Spider

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
```



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

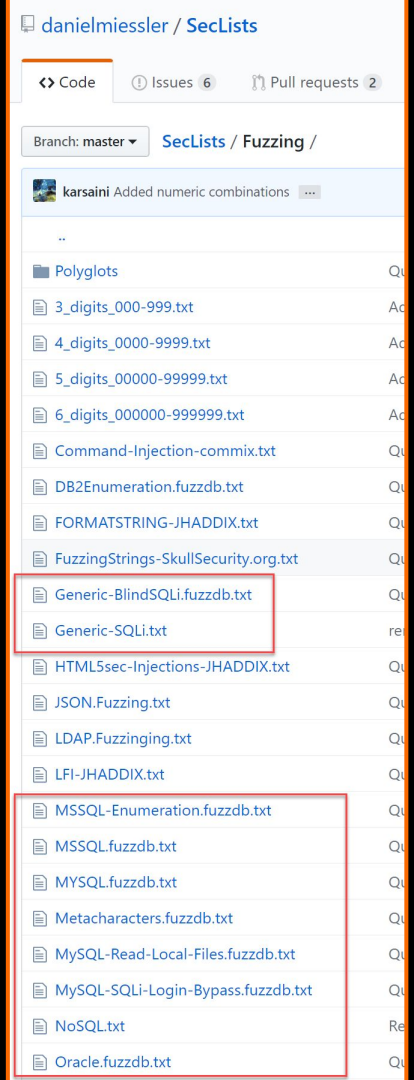
- Set up robust, automated/scripted testing easily.
  - “Fuzz” parameters, paths, etc, etc
  - Bruteforce Passwords
  - Content discovery
  - Iterating ID’s, etc, etc.
  - ++

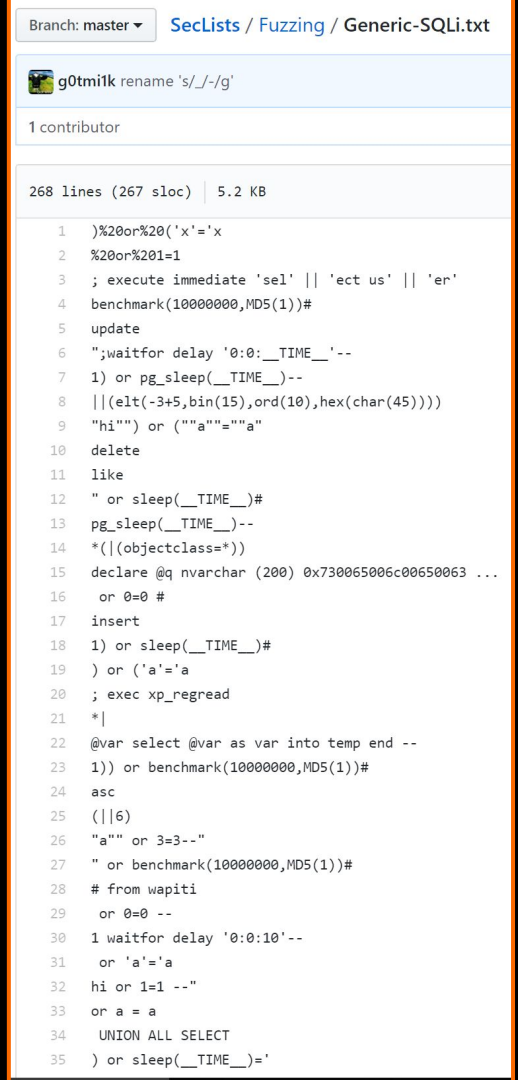
Scanner

- Automatically scan and fuzz all traffic for common vulnerabilities

Manually fuzzing a request

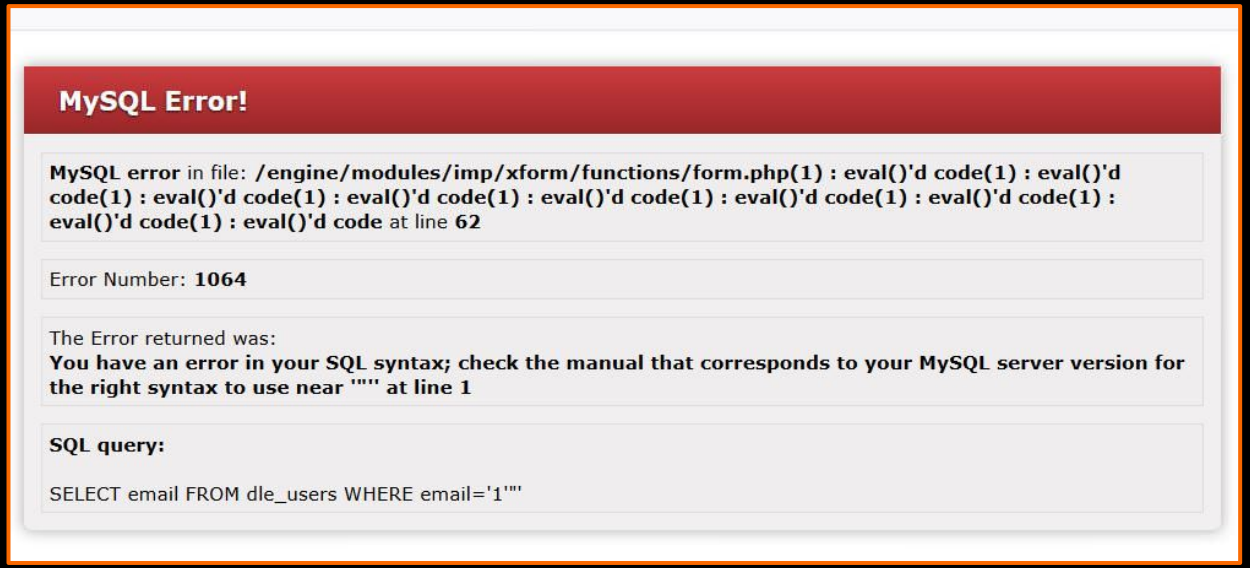
Use Intruder





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



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

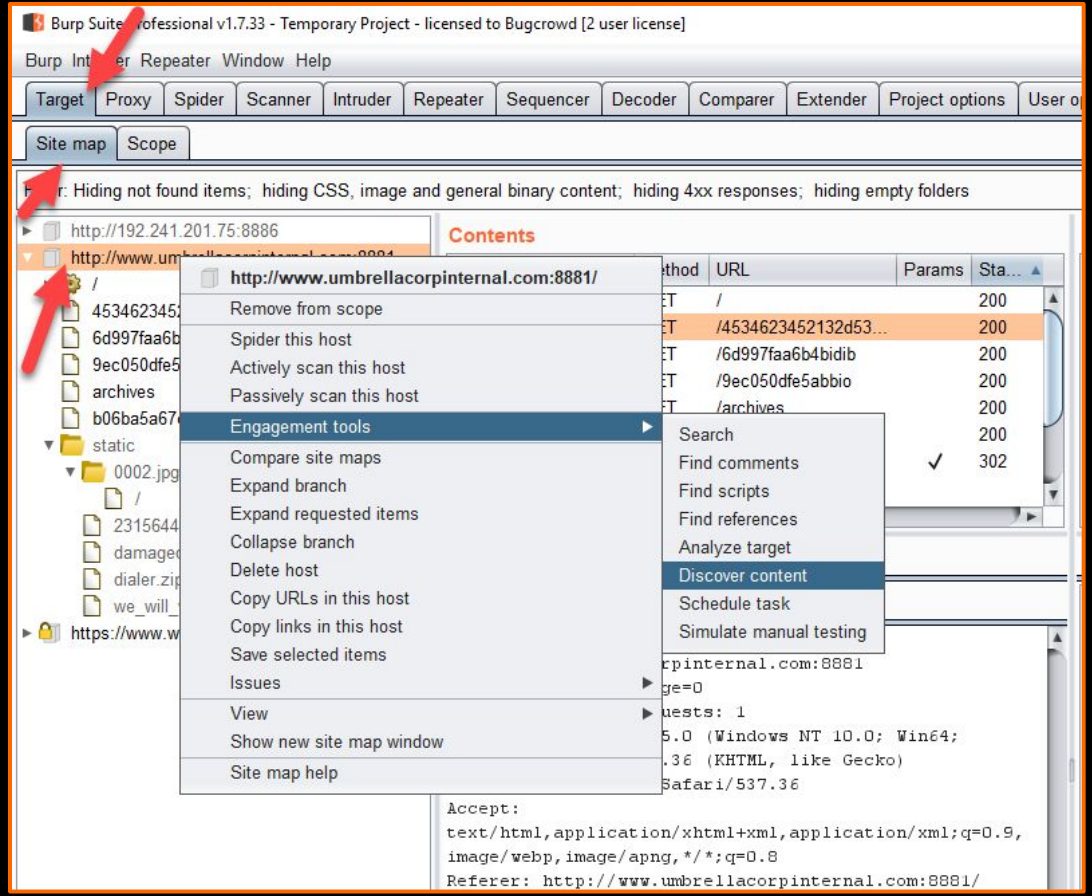
https://www.bugcrowd.com/something.css

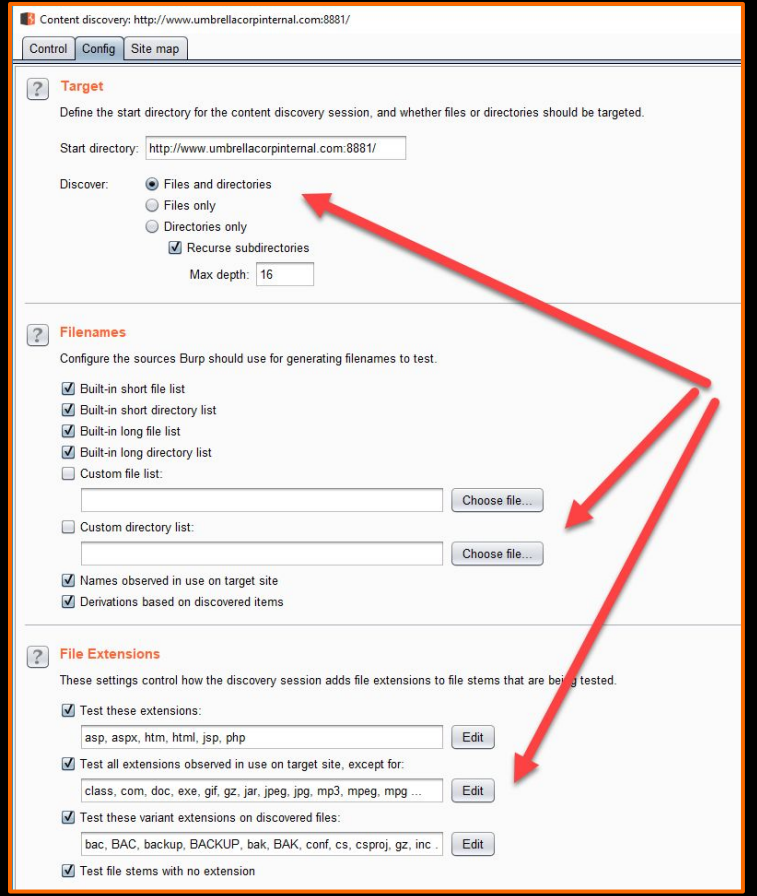
https://www.bugcrowd.com/admin/

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

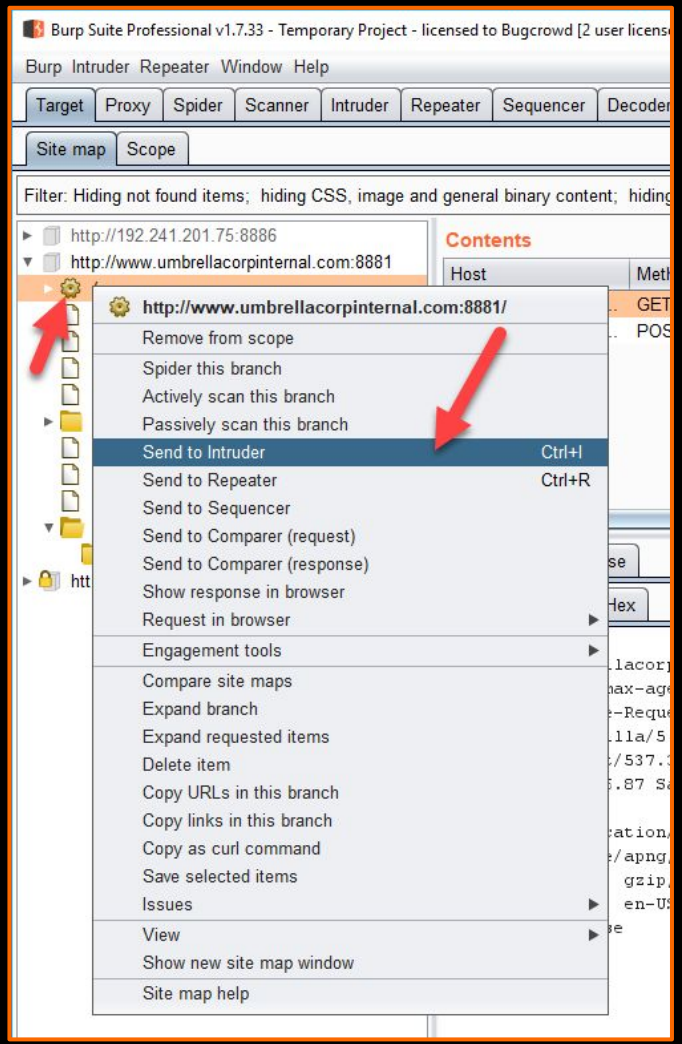
Pro Function - Content Discovery

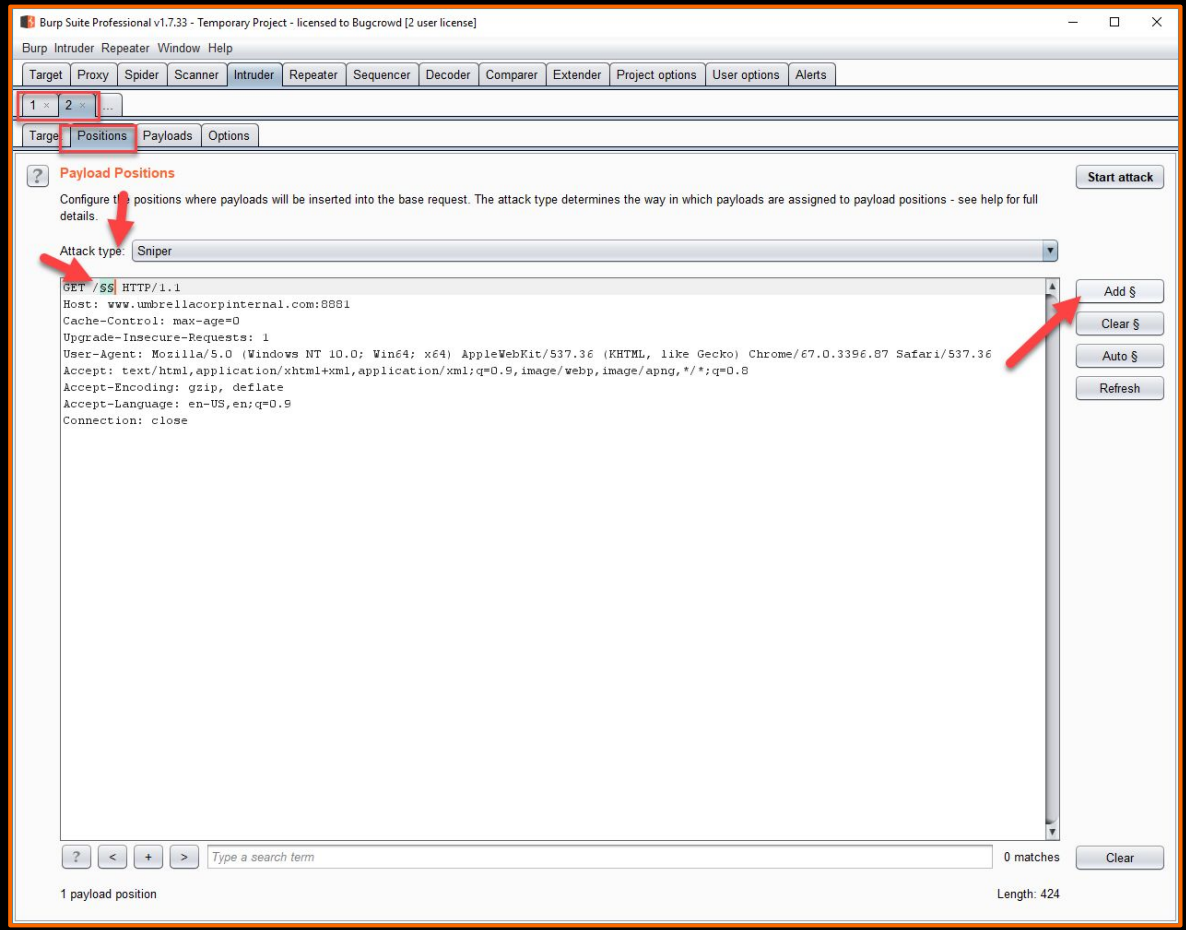
Built in Content Discovery Automation (Pro)





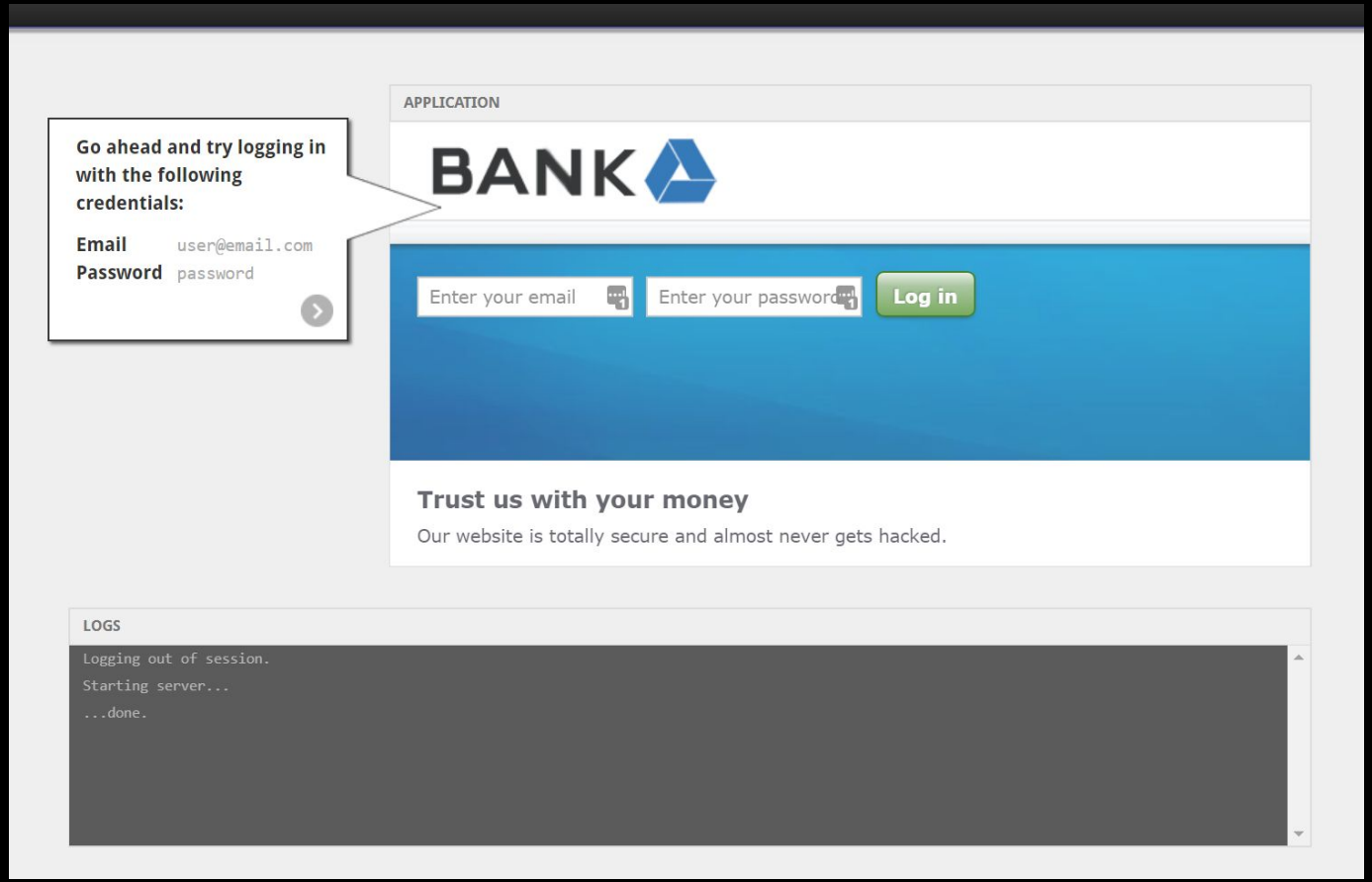
Content Discovery with Intruder





SQL Injection

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



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--
```

Insecure Direct Object Reference and numeric iteration with Burp

IDOR - insecure direct object reference

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

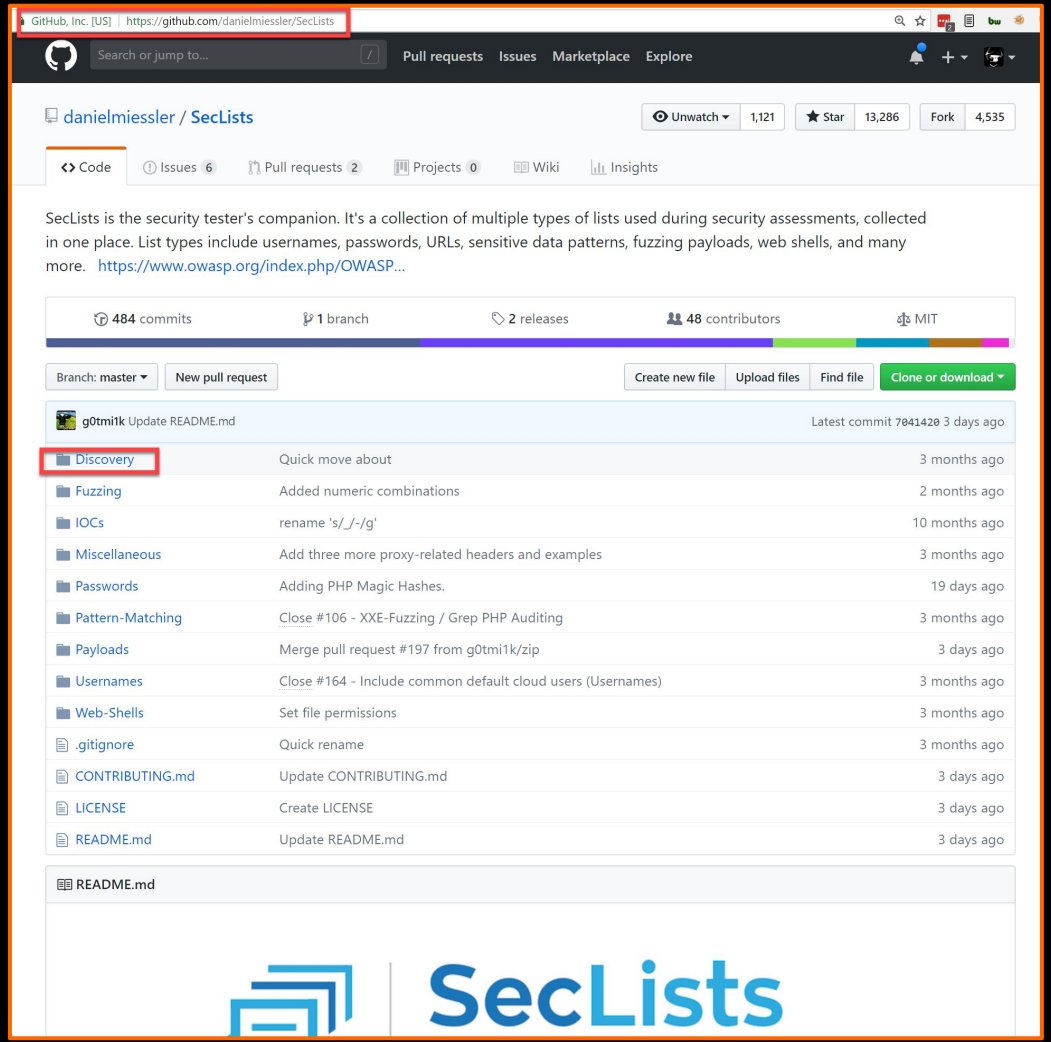
IDOR - insecure direct object reference

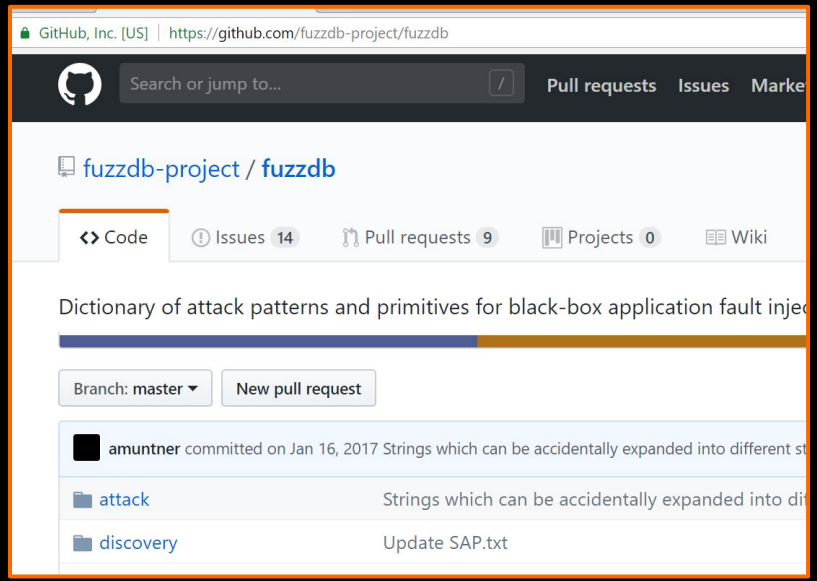
A somewhat real example that happened...

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

Intruder - Cookie lab

SecLists & fuzzdb





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