

# 1. INFORMATION GATHERING GATHERING (RECONNAISSANCE)

Thursday, July 29, 2021 8:31 AM

## 1. PASSIVE RECONNAISSANCE

### a. PHYSICAL/SOCIAL

- LOCATION INFORMATION
  - Satellite Images
  - Drones Recon
    - Building Layout (badge readers, break areas, security, fencing)
- JOB INFORMATION
  - Employees (names, job title, phone numbers, managers, etc.)
  - Pictures (badge photos, desk photos, computer photo, etc.)

### b. WEB/HOST

- Target Validation
  - WHOIS, nslookup, dnsrecon
- Finding Subdomains
  - Google Fu, dig, Nmap, Sublist3r, Bluto, crt.sh, etc.
- Fingerprinting
  - Nmap, Wappalyzer, Whatweb, BuiltWith, Netcat
- Data Breacher
  - HaveIBeenPwned, Breach-Parse, WeLeakInfo

## 2. IDENTIFYING OUR TARGET-

### a. Searching for domain emails and employees-

- <http://hunter.io/search>

### b. Searching username and password in breaches-

- Searching for breaches in google
- Use Breach-Parse

### c. Hunting Subdomains-

#### i. Sublist3r

- 1) apt install sublist3r

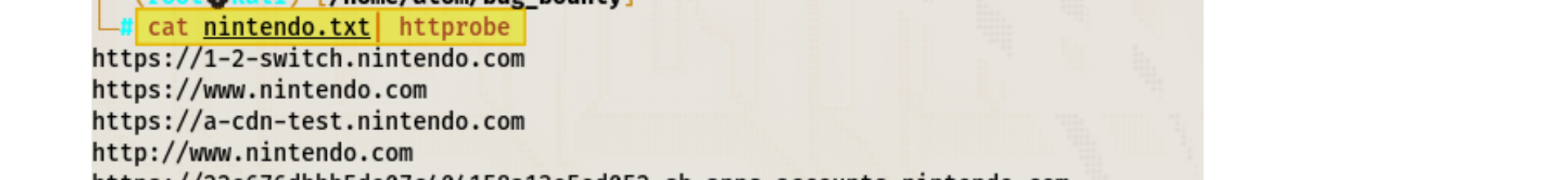
```
root@kali:~/home/atom# apt install sublist3r
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libfontconfig3 libfontconfig1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  sublist3r
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 637 kB of archives.
After this operation, 1,934 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 sublist3r all 1.1-0kali1
all 1 [637 kB]
Fetched 637 kB in 12s (52.5 kB/s)
Selecting previously unselected package sublist3r.
(Reading database ... 48835 files and directories currently installed.)
Preparing to unpack .../sublist3r_1.1-0kali1_all.deb ...
Unpacking sublist3r (1.1-0kali1) ...
Setting up sublist3r (1.1-0kali1) ...
Processing triggers for kali-menu (2021.2.3) ...
```

- 2) sublist3r -d nintendo.com

```
root@kali:~/home/atom# sublist3r -d nintendo.com
[+] Enumerating subdomains now for nintendo.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 Vinted...
[+] Searching now in Threatcrowd...
[+] Searching now in SSL Certificates...
[+] Searching now in Passiv8...
[+] Error: VirusTotal probably now is blocking our requests
[+] Total Unique Subdomains Found: 920
www.nintendo.com
1-2-switch.nintendo.com
a-cdn-test.nintendo.com
www.a-cdn-test.nintendo.com
accounts.nintendo.com
22676dbb0bde87c44158a135ed052-sb-apps.accounts.nintendo.com
91d86947b64726c82e231a6df49793a-sb-apps.accounts.nintendo.com
api.accounts.nintendo.com
apps.accounts.nintendo.com
```

#### ii. crt.sh

- 1) <https://crt.sh>
- 2) <https://crt.sh>

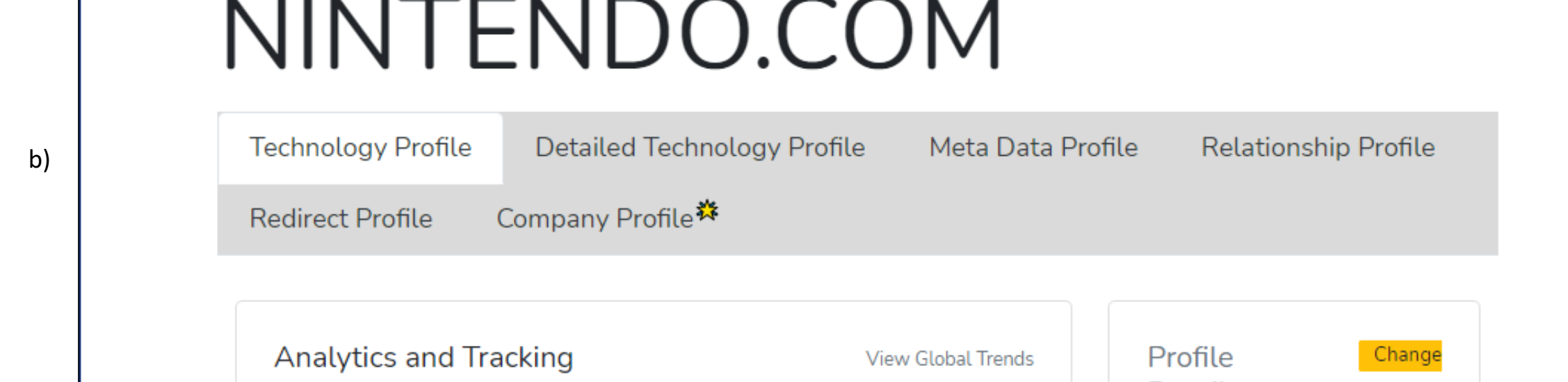


#### iii. Httpprobe-

```
root@kali:~/home/atom/bug_bounty# httpprobe https://1-2-switch.nintendo.com
https://www.nintendo.com
https://a-cdn-test.nintendo.com
https://www.nintendo.com
https://22676dbb0bde87c44158a135ed052-sb-apps.accounts.nintendo.com
https://media.accounts.nintendo.com
http://a-cdn-test.nintendo.com
https://apps.accounts.nintendo.com
http://1-2-switch.nintendo.com
http://media.accounts.nintendo.com
https://91d86947b64726c82e231a6df49793a-sb-apps.accounts.nintendo.com
http://22676dbb0bde87c44158a135ed052-sb-apps.accounts.nintendo.com
```

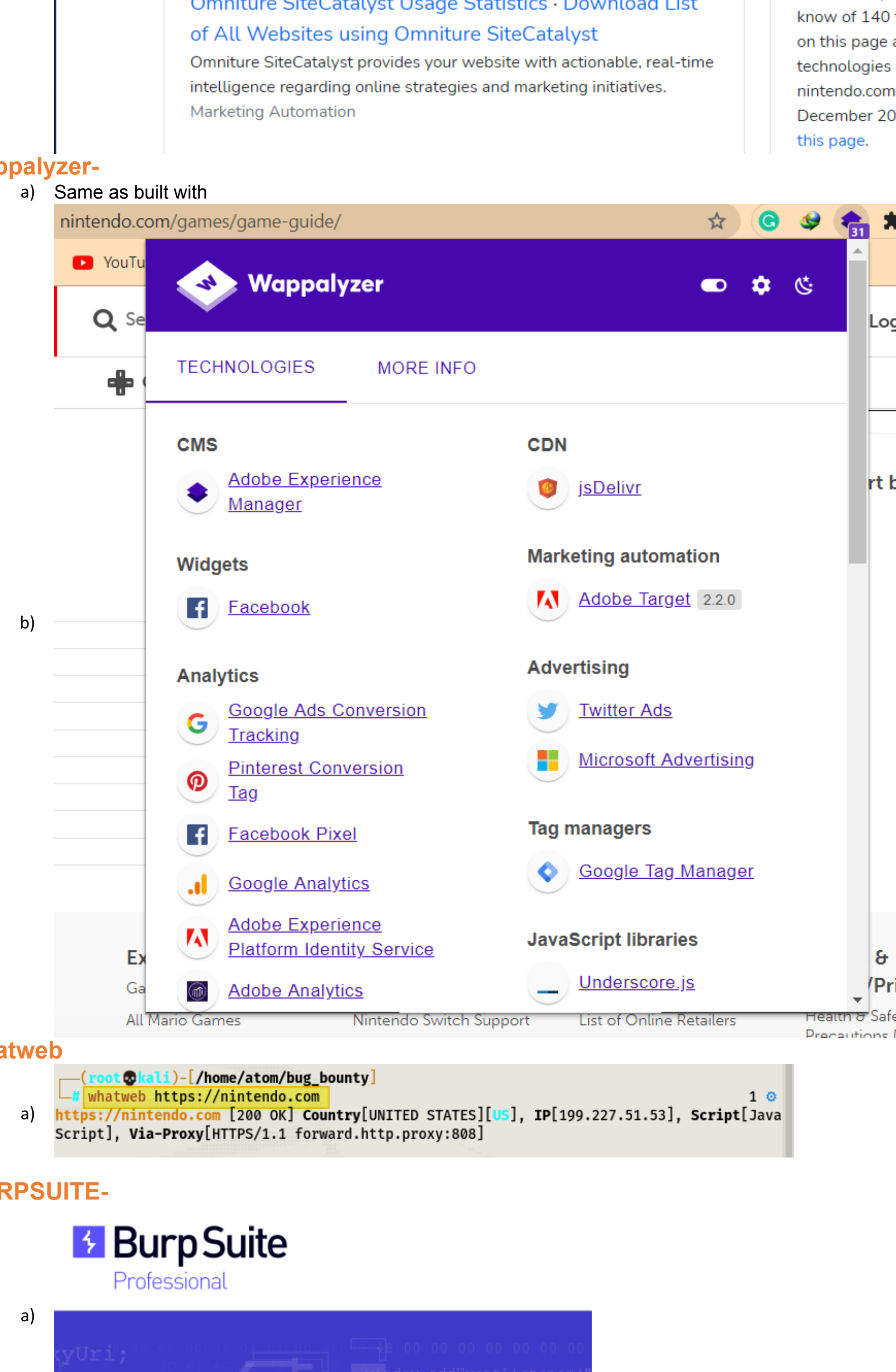
### iv. (IDENTIFYING WEBSITE TECHNOLOGY) built with

#### a) <https://builtwith.com>



#### v. wappalyzer-

##### a) Same as built with

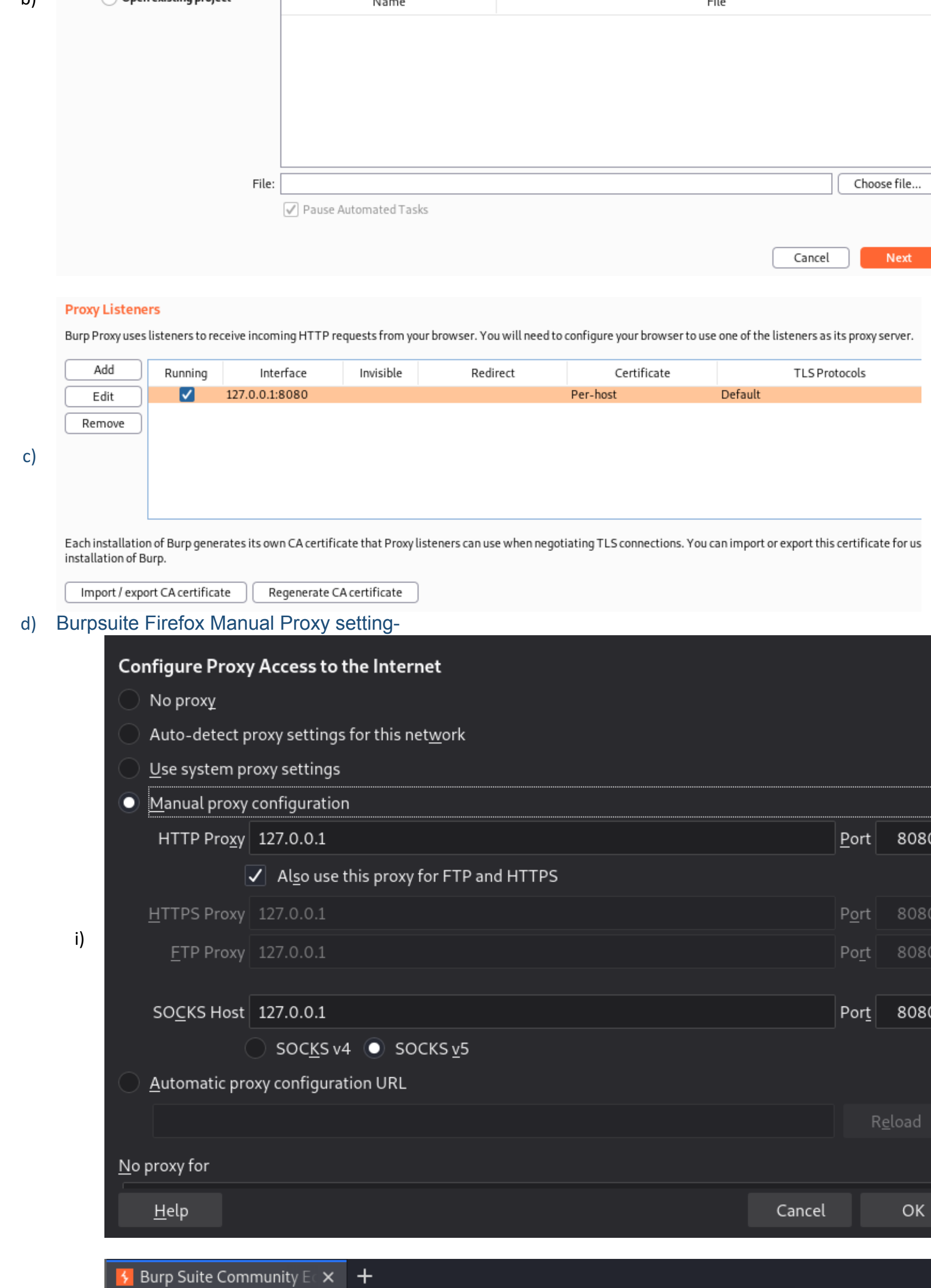


#### vi. whatweb

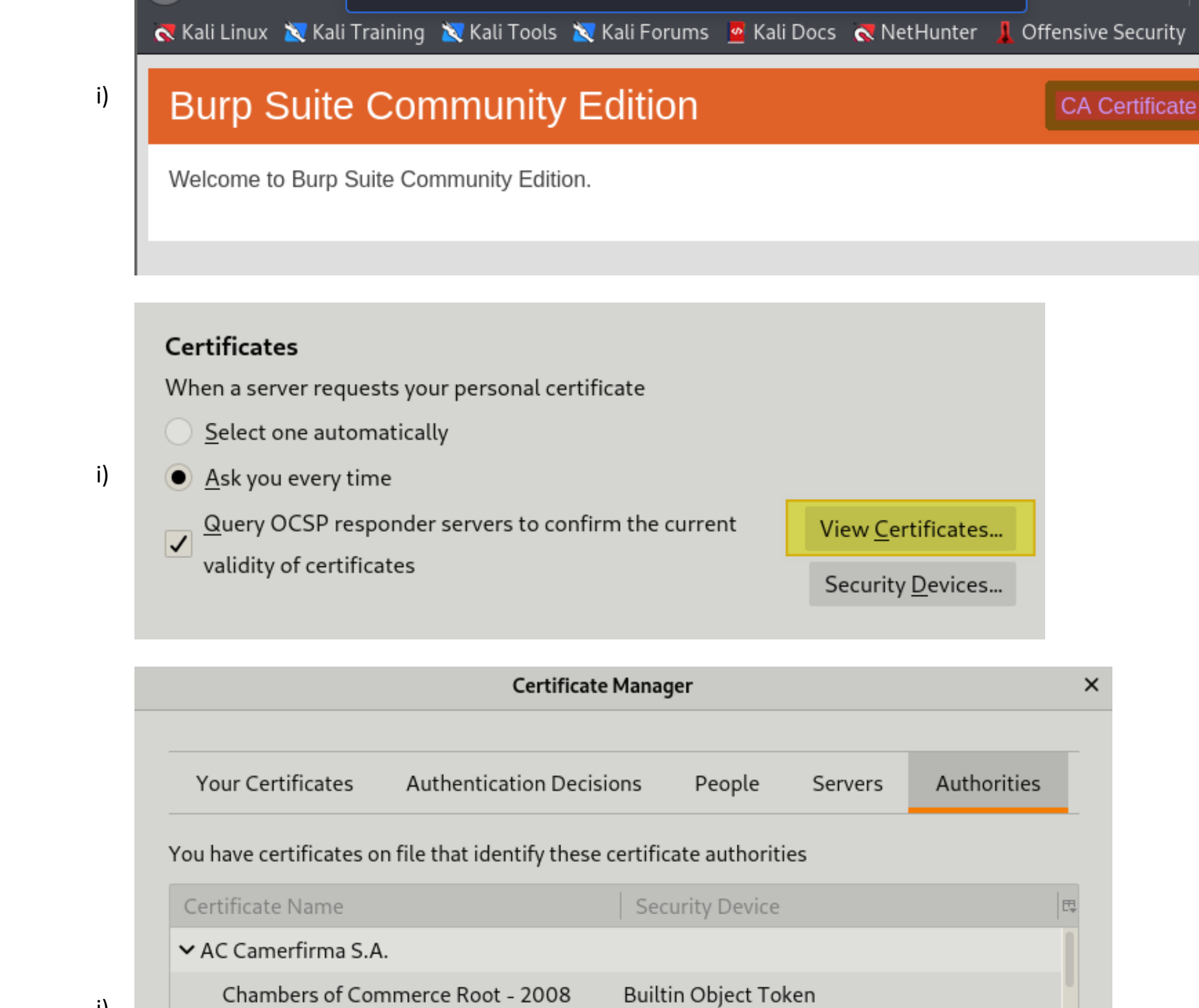
```
root@kali:~/home/atom/bug_bounty# whatweb https://nintendo.com
https://nintendo.com [280 OK] Country[UNITED STATES][en], IP[199.227.51.53], Script[JavaScript], Via-Proxy[HTTPS/1.1 forward.http.proxy:888]
```

#### vii. BURPSUITE-

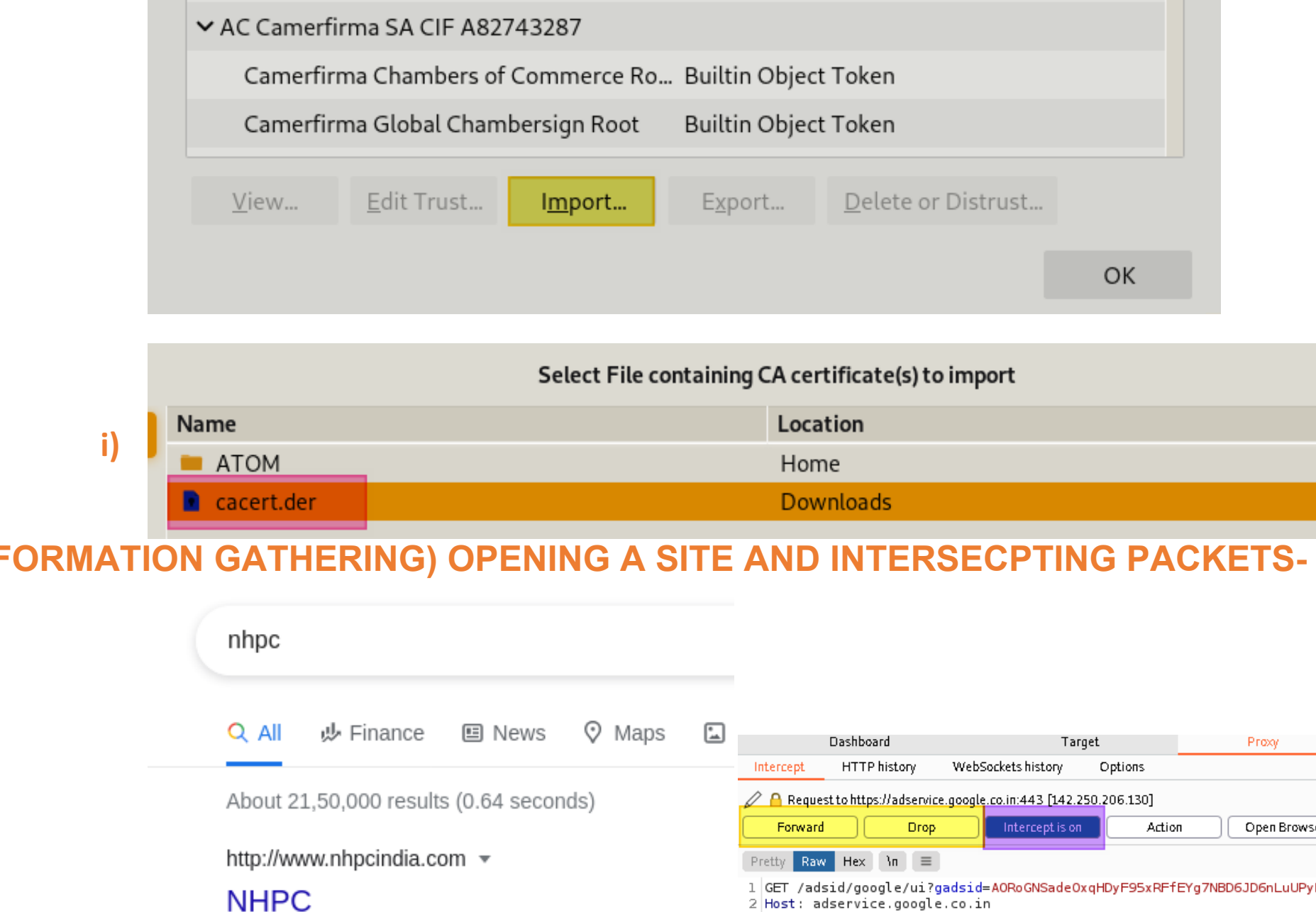
##### a) <https://portswigger.net/burpsuite>



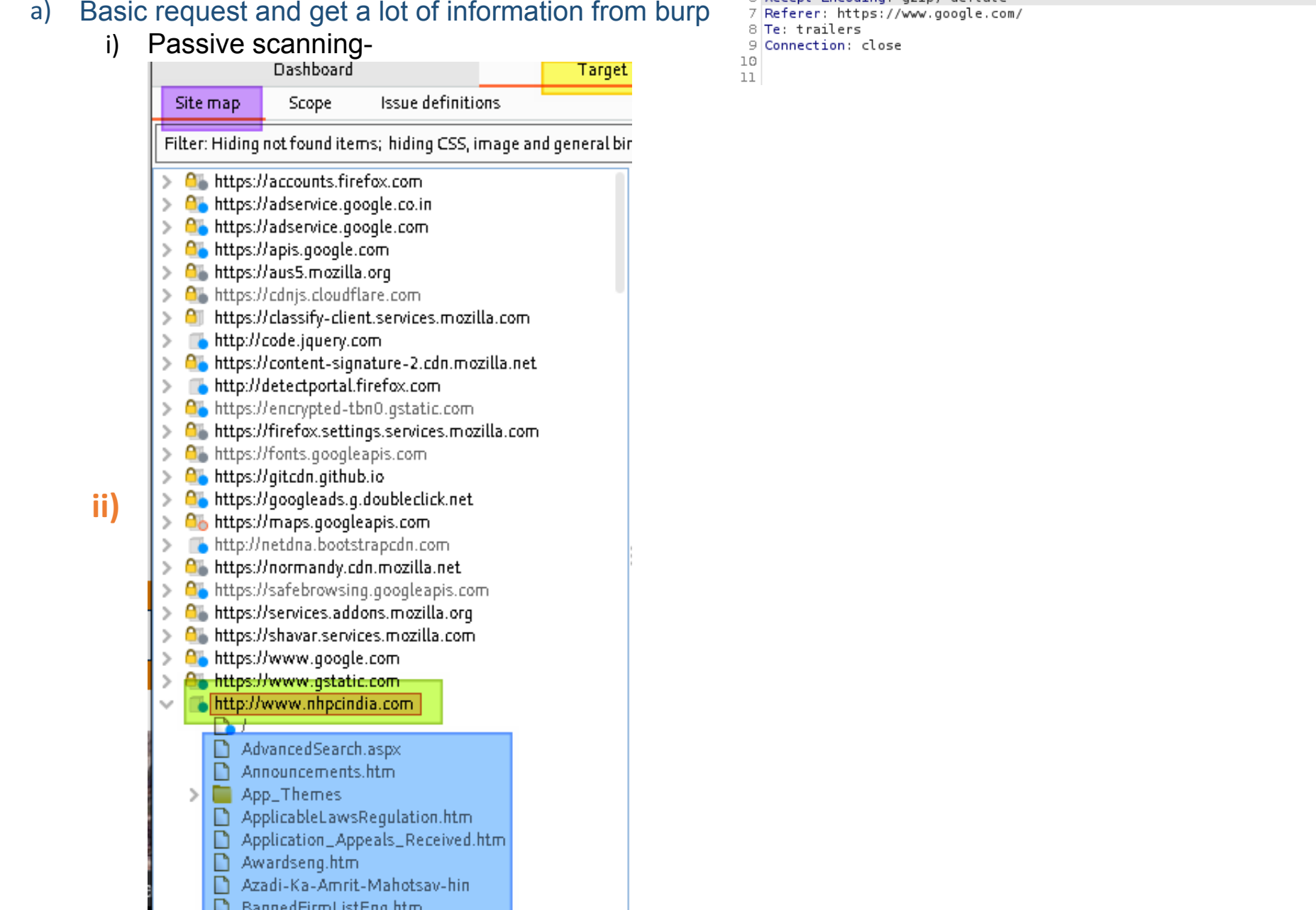
##### b) <https://portswigger.net/burpsuite>



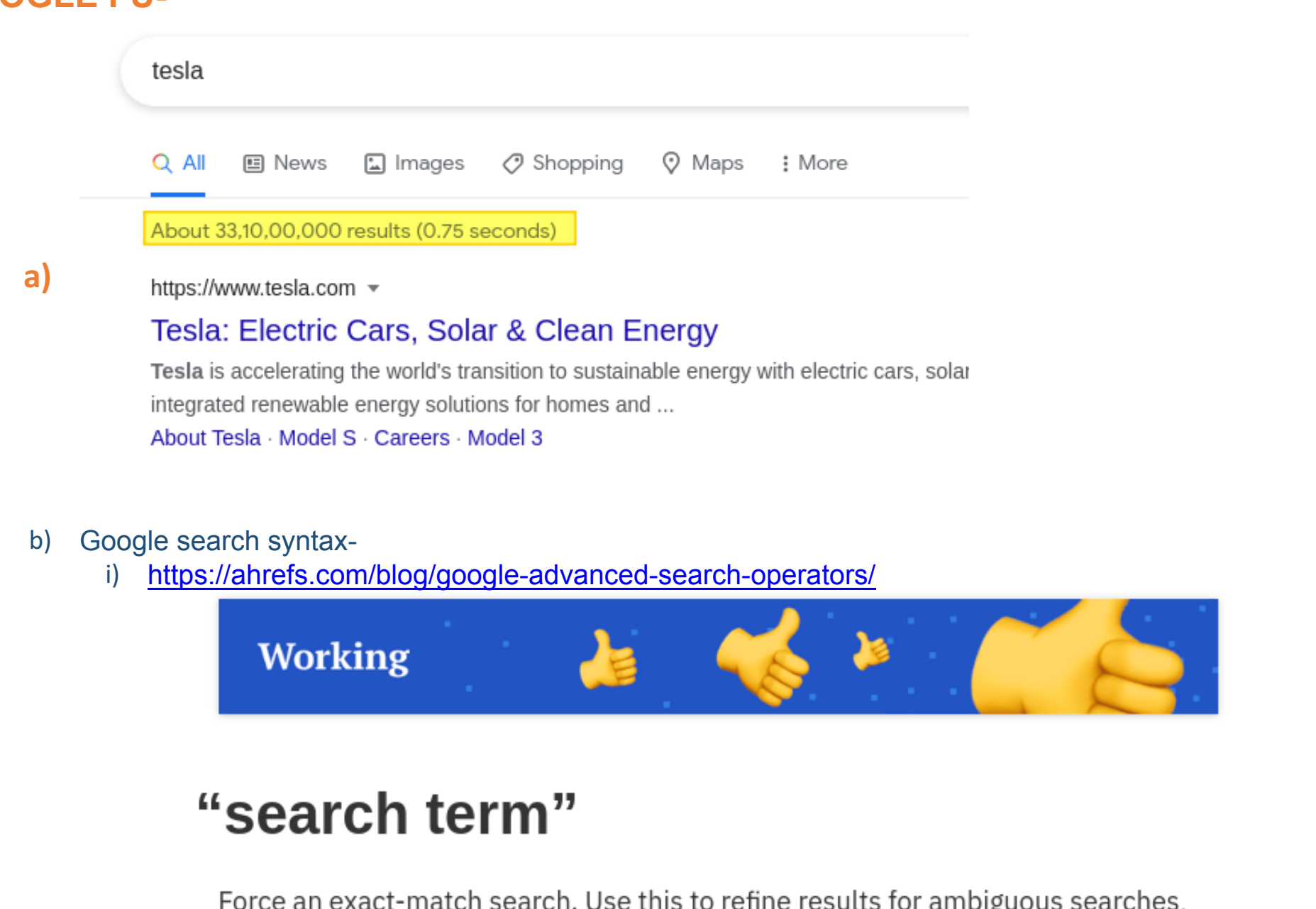
##### c) <https://portswigger.net/burpsuite>



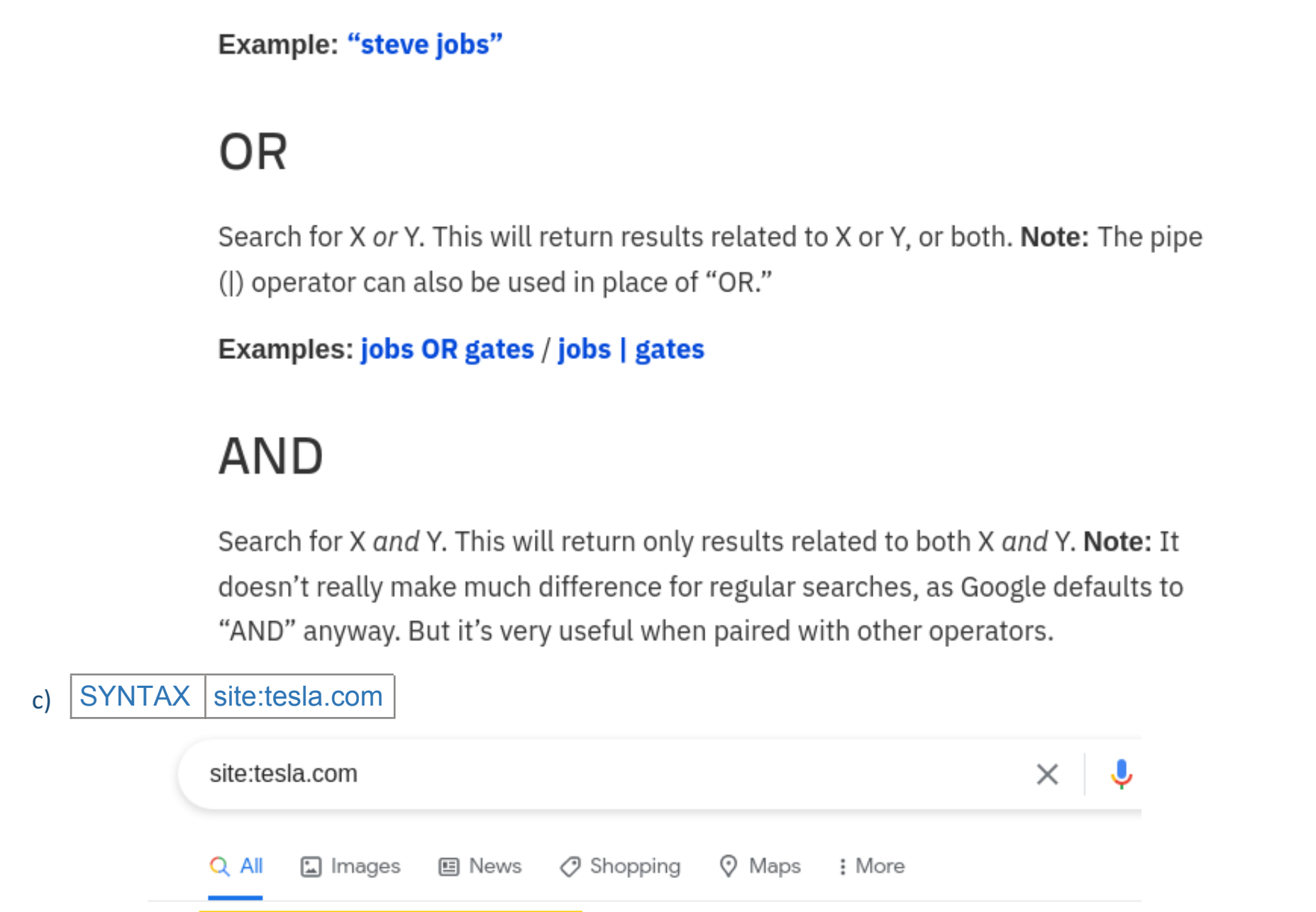
##### d) <https://portswigger.net/burpsuite>



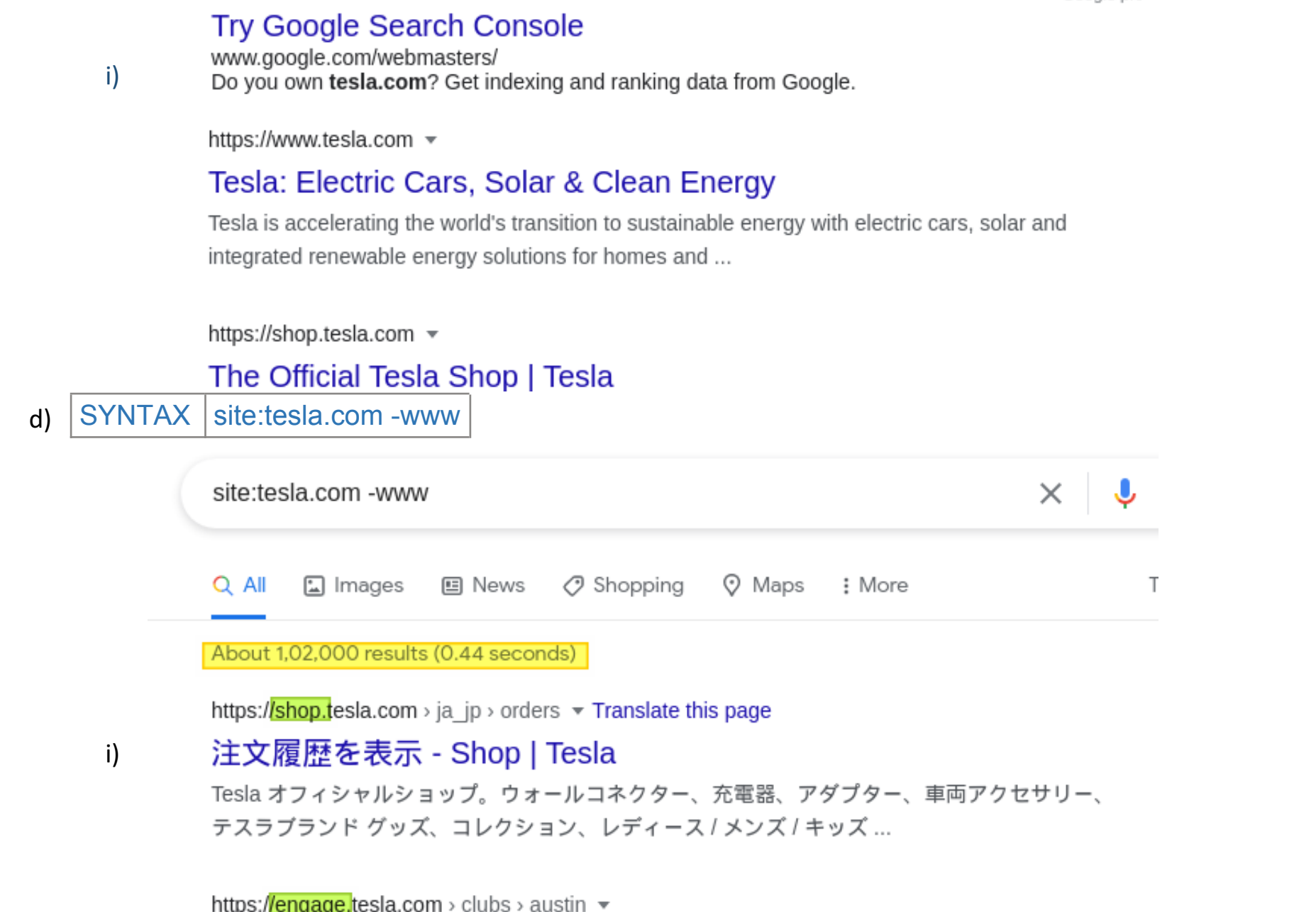
##### e) <https://portswigger.net/burpsuite>



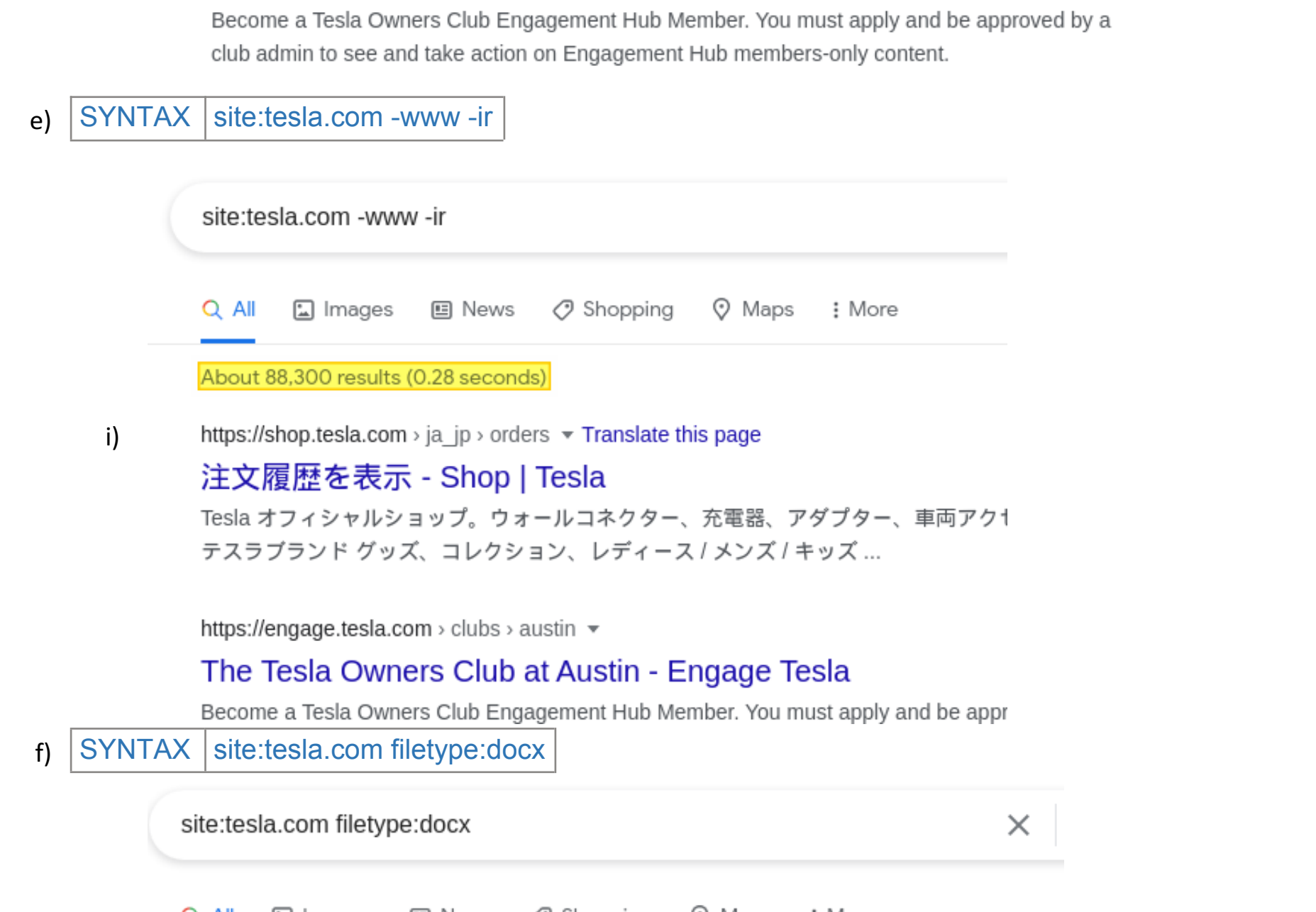
##### f) <https://portswigger.net/burpsuite>



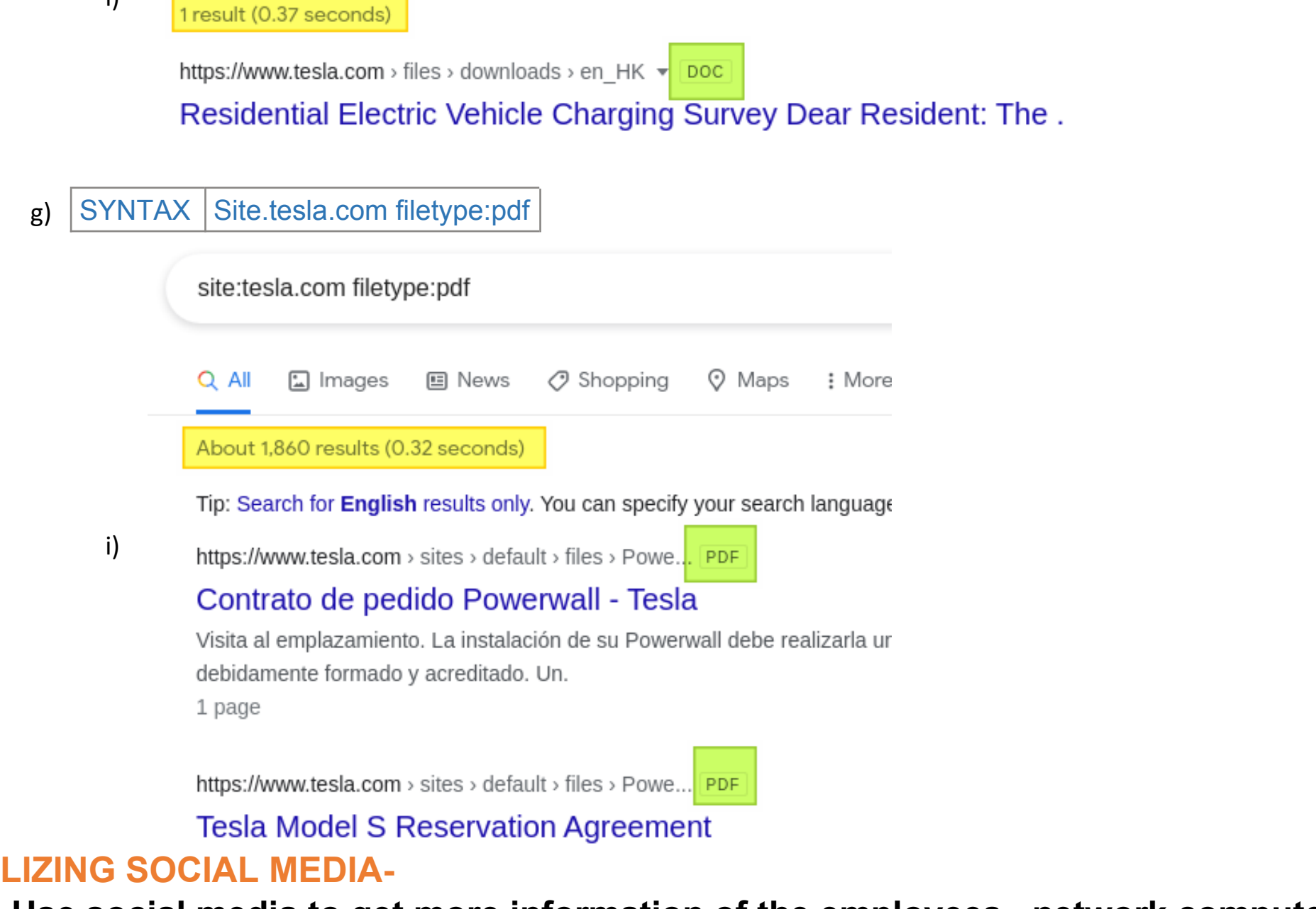
##### g) <https://portswigger.net/burpsuite>



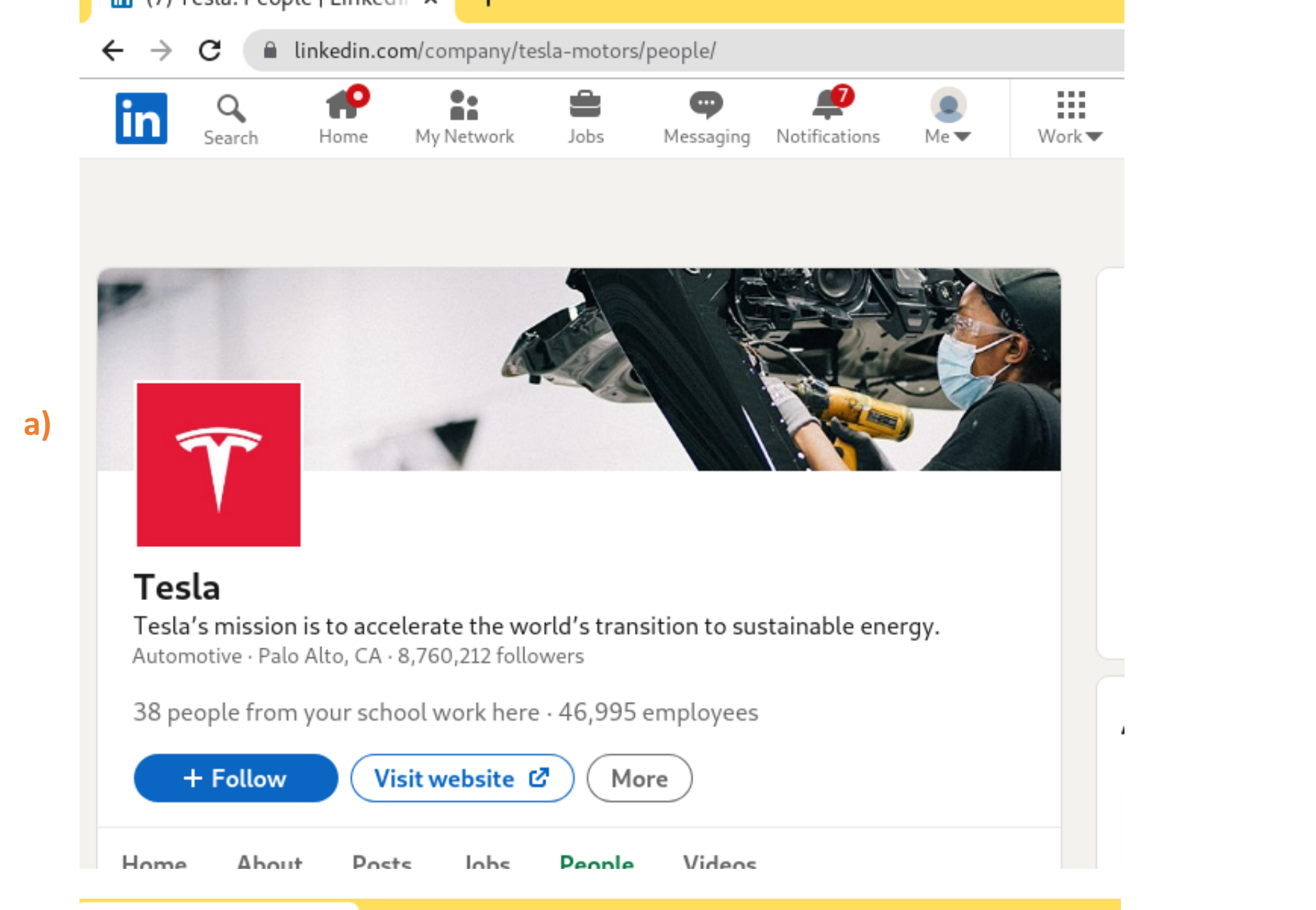
##### h) <https://portswigger.net/burpsuite>



##### i) <https://portswigger.net/burpsuite>



##### j) <https://portswigger.net/burpsuite>



##### k) <https://portswigger.net/burpsuite>



##### l) <https://portswigger.net/burpsuite>



##### m) <https://portswigger.net/burpsuite>



##### n) <https://portswigger.net/burpsuite>



##### o) <https://portswigger.net/burpsuite>



##### p) <https://portswigger.net/burpsuite>



##### q) <https://portswigger.net/burpsuite>



##### r) <https://portswigger.net/burpsuite>



##### s) <https://portswigger.net/burpsuite>



##### t) <https://portswigger.net/burpsuite>



##### u) <https://portswigger.net/burpsuite>



##### v) <https://portswigger.net/burpsuite>



##### w) <https://portswigger.net/burpsuite>



##### x) <https://portswigger.net/burpsuite>



##### y) <https://portswigger.net/burpsuite>



##### z) <https://portswigger.net/burpsuite>



##### aa) <https://portswigger.net/burpsuite>



##### ab) <https://portswigger.net/burpsuite>



##### ac) <https://portswigger.net/burpsuite>



##### ad) <https://portswigger.net/burpsuite>



##### ae) <https://portswigger.net/burpsuite>



##### af) <https://portswigger.net/burpsuite>



##### ag) <https://portswigger.net/burpsuite>



##### ah) <https://portswigger.net/burpsuite>



##### ai) <https://portswigger.net/burpsuite>



##### aj) <https://portswigger.net/burpsuite>



##### ak) <https://portswigger.net/burpsuite>



##### al) <https://portswigger.net/burpsuite>



##### am) <https://portswigger.net/burpsuite>



##### an) <https://portswigger.net/burpsuite>



##### ao) <https://portswigger.net/burpsuite>



##### ap) <https://portswigger.net/burpsuite>



##### aq) <https://portswigger.net/burpsuite>



##### ar) <https://portswigger.net/burpsuite>



##### as) <https://portswigger.net/burpsuite>



##### at) <https://portswigger.net/burpsuite>



##### au) <https://portswigger.net/burpsuite>



##### av) <https://portswigger.net/burpsuite>



##### aw) <https://portswigger.net/burpsuite>



##### ax) <https://portswigger.net/burpsuite>



##### ay) <https://portswigger.net/burpsuite>



##### az) <https://portswigger.net/burpsuite>



##### ba) <https://portswigger.net/burpsuite>



##### bb) <https://portswigger.net/burpsuite>



##### bc) <https://portswigger.net/burpsuite>



##### bd) <https://portswigger.net/burpsuite>



##### be) <https://portswigger.net/burpsuite>



##### bf) <https://portswigger.net/burpsuite>



##### bg) <https://portswigger.net/burpsuite>



##### bh) <https://portswigger.net/burpsuite>



##### bi) <https://portswigger.net/burpsuite>



##### bj) <https://portswigger.net/burpsuite>



##### bk) <https://portswigger.net/burpsuite>



##### bl) <https://portswigger.net/burpsuite>



##### bm) <https://portswigger.net/burpsuite>



##### bn) <https://portswigger.net/burpsuite>



##### bo) <https://portswigger.net/burpsuite>



##### bp) <https://portswigger.net/burpsuite>



##### bq) <https://portswigger.net/burpsuite>



##### br) <https://portswigger.net/burpsuite>



##### bs) <https://portswigger.net/burpsuite>



##### bt) <https://portswigger.net/burpsuite>



##### bu) <https://portswigger.net/burpsuite>

