

[medium.com](https://medium.com/@mrdaraihan/recon-methodology-for-bug-bounty-hunting-11a2a2f3a2)

# Recon Methodology For Bug Bounty Hunting

*Md. Raihan*

9-11 minutes



6 min read

Oct 17, 2025

Press enter or click to view image in full size



## What is Reconnaissance:

The recon phase is all about gathering information. The more data you have on your target, the higher your

chances of finding vulnerabilities. This stage sets the foundation for everything that follows.

## Subdomain Enumeration

Subdomains often hide forgotten features, admin panels, or unpatched vulnerabilities. Use multiple tools for better coverage.

### Passive Subdomain Enumeration

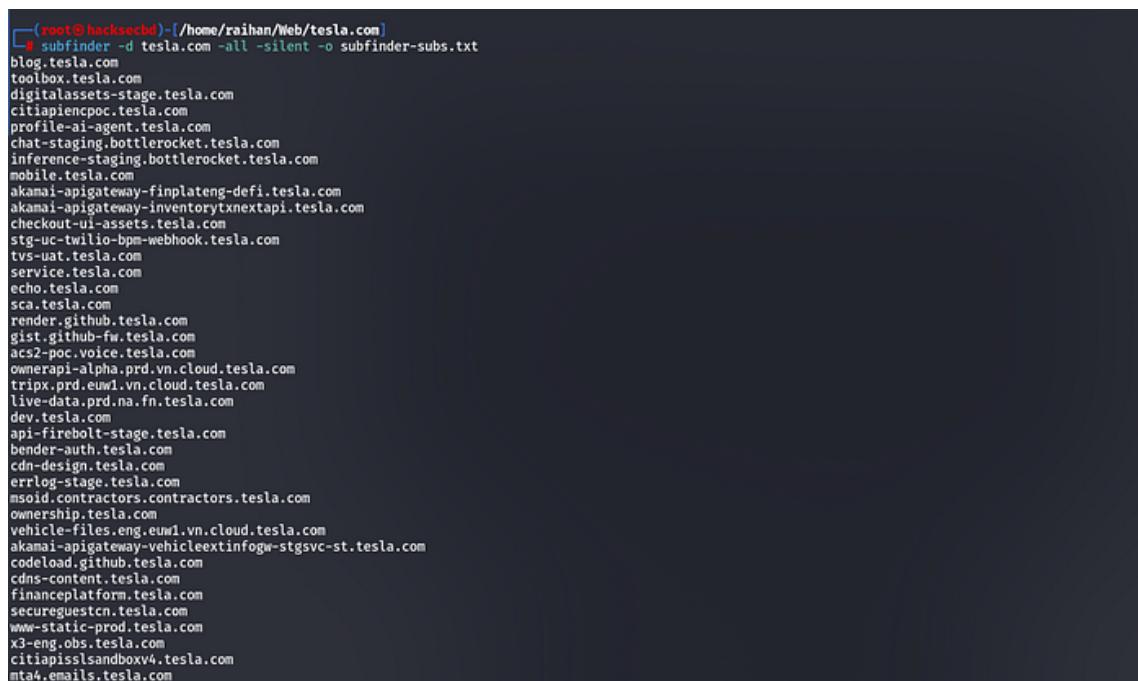
Passive enumeration relies on third-party sources and APIs, such as certificate transparency logs, search engines, and public DNS databases.

- **Tools:** Subfinder, Assetfinder, Amass, Sublist3r, Findomain

#### Subfinder Example Command :

```
subfinder -d target.com -all -silent -o  
subfinder-subs.txt
```

Press enter or click to view image in full size



```
(root@hacksecbd)-[~/home/raihan/Web/tesla.com]  
# subfinder -d tesla.com -all -silent -o subfinder-subs.txt  
blog.tesla.com  
toolbox.tesla.com  
digitalassets-stage.tesla.com  
citiapienpoc.tesla.com  
profile-ai-agent.tesla.com  
chat-staging.bottlerocket.tesla.com  
inference-staging.bottlerocket.tesla.com  
mobile.tesla.com  
akamai-apigateway-finplateng-defi.tesla.com  
akamai-apigateway-inventorytxnextapi.tesla.com  
checkout-ui-assets.tesla.com  
stg-uc-twilio-bpm-webhook.tesla.com  
tvs-uat.tesla.com  
service.tesla.com  
echo.tesla.com  
sca.tesla.com  
render.github.tesla.com  
gist.github-fw.tesla.com  
acs2-poc.voice.tesla.com  
ownerapi-alpha.prd.vn.cloud.tesla.com  
tripx.prd.euw1.vn.cloud.tesla.com  
live-data.prd.na.fn.tesla.com  
dev.tesla.com  
api-firebolt-stage.tesla.com  
bender-auth.tesla.com  
cdn-design.tesla.com  
errlog-stage.tesla.com  
msoid.contractors.contractors.tesla.com  
ownership.tesla.com  
vehicle-files.eng.euw1.vn.cloud.tesla.com  
akamai-apigateway-vehicleextinfogw-stgsvc-st.tesla.com  
codeLoad.github.tesla.com  
cdns-content.tesla.com  
financeplatform.tesla.com  
securequestcn.tesla.com  
www-static-prod.tesla.com  
x3-eng.obs.tesla.com  
citiapisslsandboxv4.tesla.com  
mta4.emails.tesla.com
```

## Assetfinder Example Command :

```
assetfinder -subs-only target.com | tee
assetfinder_subs.txt
```

Press enter or click to view image in full size

```
(root@haksechd)-[~/home/raihan/Web/tesla.com]
# assetfinder -subs-only tesla.com | tee assetfinder_subs.txt
tesla.com
www.tesla.com
digitalassets.tesla.com
suppliers.tesla.com
link.tesla.com
ams13-gpgw1.tesla.com
dali1-gpgw1.tesla.com
mta.email.tesla.com
mta2.email.tesla.com
emails.tesla.com
click.emails.tesla.com
mta.emails.tesla.com
mta2.emails.tesla.com
mta3.emails.tesla.com
mta4.emails.tesla.com
mta5.emails.tesla.com
view.emails.tesla.com
events.tesla.com
hnd13-gpgw1.tesla.com
iad05-gpgw1.tesla.com
itanswers.tesla.com
lax32-gpgw1.tesla.com
marketing.tesla.com
model3.tesla.com
ptr1.tesla.com
o3.ptr1444.tesla.com
ptr2.tesla.com
o2.ptr556.tesla.com
o7.ptr6980.tesla.com
o5.ptr8460.tesla.com
o6.ptr9437.tesla.com
sin05-gpgw1.tesla.com
acs2-poc.voice.tesla.com
vpn1.tesla.com
xmail.tesla.com
digitalassets-shop.tesla.com
digitalassets-accounts.tesla.com
digitalassets-energy.tesla.com
digitalassets-accounts.tesla.com
digitalassets-contents.tesla.com
dex.ops.na.vn.cloud.tesla.com
incontrol.tesla.com
```

## Findomain Example Command:

```
findomain --quiet -t target.com | tee
findomain-subs.txt
```

Press enter or click to view image in full size

```
(root@haksechd)-[~/home/raihan/Web/tesla.com]
# findomain --quiet -t tesla.com | tee findomain-subs.txt
vehicle-files.eng.euw1.vn.cloud.tesla.com
ciscoguest.tesla.com
bottlerocket.tesla.com
vmanage-alerts.tesla.com
tsapi-stg.tesla.com
api-firebolt.tesla.com
envoy-partnertasks.tesla.com
tv-api.tesla.com
myapps.tesla.com
live-data.prd.ma.fn.tesla.com
akamai-apigateway-warpdashboardapi.tesla.com
origin-ranger-api.tesla.com
solarbonds.tesla.com
akamai-apigateway-stg-fta.tesla.com
server.tesla.com
mta.email.tesla.com
akamai-apigateway-vendorpartsapi.tesla.com
citiapiencpocv3.tesla.com
url4857.tesla.com
live-data.prd.euw1.fn.tesla.com
www5.tesla.com
citiapiencpocv2.tesla.com
aurora-ordering-ext.tesla.com
url5347.tesla.com
rubygems.github-fw.tesla.com
csp-dev-teleport-proxy.tesla.com
inference-eu-staging.bottlerocket.tesla.com
tokens-staging.bottlerocket.tesla.com
trt.tesla.com
hub.tesla.com
na-1-sso.tesla.com
consul.bottlerocket.tesla.com
citiapiisslpocv1.tesla.com
codeload.extgithub.tesla.com
diner-api-stage.tesla.com
fleetview.prd.europe.fn.tesla.com
darkfield.tesla.com
citiapiisslsandboxv4.tesla.com
incontrol.tesla.com
origin-finplat-prd.tesla.com
```

## Sublist3r Example Command:

```
sublist3r -d target.com -t 50 -o sublist3r.txt
```

Press enter or click to view image in full size

```
# sublist3r -d tesla.com -t 50 -o sublist3r.txt
[+] Coded By Ahmed Aboul-Ela - @AboulEla
[+] Generating subdomains now for tesla.com
[+] Searching now in Baidu...
[+] Searching now in Yahoo...
[+] Searching now in Google...
[+] Searching now in Bing...
[+] Searching now in DuckDuckGo...
[+] Searching now in Netcraft...
[+] Searching now in DNSdumpster...
[+] Searching now in VirusTotal...
[+] Searching now in Shodan...
[+] Searching now in SSL Certificates...
[+] Searching now in PassiveDNS...
Process DDoS Computer-IP: [REDACTED]
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    self.run()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrftoken(resp)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
  File "/usr/lib/python3/dist-packages/csrf.py", line 10, in findall
    raise IndexError('IndexError: list index out of range')
IndexError: list index out of range
[!] Error: DNSLIB is blocking our requests
[+] Saving results to file: sublist3r.txt
[+] Total Unique Subdomains Found: 34
www.tesla.com
tesla.com
amst1-pg01.tesla.com
auth.tesla.com
billing.tesla.com
developer.tesla.com
digitalassets.tesla.com
digitalassets-shop.tesla.com
energy.tesla.com
powerhub.energy.tesla.com
energylibrary.tesla.com
engage.tesla.com
inside.tesla.com
feedback.tesla.com
fleetview.prd.europe.fn.tesla.com
inside.tesla.com
```

## Amass Example Command:

```
amass enum -passive -d target.com -o
amass_passive.txt
amass enum -active -d example.com -o
amass_active.txt
amass enum -active -brute -d example.com -
config config.ini -o amass_brute.txt
```

## Active Subdomain Enumeration

Active enumeration involves brute-forcing subdomains using wordlists and DNS queries.

**Tools:** Subbrute, MassDNS, Shuffledns, DNSX

Using a wordlist for brute force :

**Example Command :Subdomain Brute-Forcing**

```
python3 subbrute.py target.com -w wordlist.txt
-o brute_subs.txt
./Tools/massdns/scripts/subbrute.py target.com
```

```
/usr/share/wordlists/2m-subdomains.txt |  
massdns -r /usr/share/wordlists/resolvers.txt -  
t A -o S -w target.com.txt  
echo target.com | shuffledns -w wordlist.txt -r  
resolvers.txt -mode bruteforce | tee  
shuffledns.txt
```

# **Subdomain Brute-Forcing**

Brute-forcing is useful when passive methods miss some hidden subdomains.

- **Tools:** SubBrute, FFUF, dnsx, MassDNS

## **FFUF Example Command:**

```
ffuf -u http://FUZZ.target.com -c -w wordlists  
-t 100 -fc 403 | tee ffuf_subs_output.txt
```

Press enter or click to view image in full size

```
[root@backtrack ~]# /home/raihan/Web/tesla.com
[ffuf] -w http://FUZZ.tesla.com -c -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 100 -fc 403 | tee ffuf_subs_output.txt


```

v2.1.0-dev

```
:: Method : GET
:: URL   : http://FUZZ.tesla.com
:: Wordlist : FUZZ: /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 100
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
:: Filter  : Response status: 403
```

---

```
autodiscover      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 100ms]
oil               [Status: 302, Size: 420, Words: 10, Lines: 23, Duration: 320ms]
hub               [Status: 302, Size: 428, Words: 10, Lines: 23, Duration: 350ms]
warehouse        [Status: 302, Size: 427, Words: 10, Lines: 23, Duration: 366ms]
factory           [Status: 302, Size: 428, Words: 10, Lines: 23, Duration: 558ms]
engage            [Status: 301, Size: 107, Words: 5, Lines: 8, Duration: 199ms]
wire              [Status: 302, Size: 427, Words: 10, Lines: 23, Duration: 420ms]
autodiscover.c    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 0ms]
autodiscover.t    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 0ms]
autodiscover.service [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 73ms]
```

---

```
:: Progress: [11442/11442] :: Job [1/1] :: 113 req/sec :: Duration: [0:05:46] :: Errors: 114379 ::
```

use this command to filter out the ffufoutput:

```
for subs in $(cat ffuf_subs_output.txt | awk  
'{print $1}'); do  
    echo "${subs}.target.com" >> ffuf-subs-  
final.txt ;  
done
```

Then remove the ffuf\_subs\_output.txt ,file:

Press enter or click to view image in full size

```
[root@hacksecbd]~[/home/raihan/Web/tesla.com]
└─# for subs in $(cat ffuf_subs_output.txt | awk '{print $1}'); do
      echo "${subs}.tesla.com" >> ffuf-subs-final.txt ;
done

[root@hacksecbd]~[/home/raihan/Web/tesla.com]
└─# cat ffuf-subs-final.txt
autodiscover.tesla.com
bi.tesla.com
hub.tesla.com
warehouse.tesla.com
factory.tesla.com
engage.tesla.com
wire.tesla.com
autodiscover.c.tesla.com
autodiscover.t.tesla.com
autodiscover.service.tesla.com

[root@hacksecbd]~[/home/raihan/Web/tesla.com]
└─# rm ffuf_subs_output.txt

[root@hacksecbd]~[/home/raihan/Web/tesla.com]
└─#
```

**Combine all results into one file using anew:**

cat \*.txt | anew all\_subdomains.txt

Press enter or click to view image in full size

```
[root@hacksecbd]~[/home/raihan/Web/tesla.com]
└─# ls
assetfinder_subs.txt ffuf-subs-final.txt findomain-subs.txt subfinder-subs.txt sublist3r.txt

[root@hacksecbd]~[/home/raihan/Web/tesla.com]
└─# cat *.txt | anew all_subdomains.txt
tesla.com
www.tesla.com
digitalassets.tesla.com
suppliers.tesla.com
link.tesla.com
ans13-gpgw1.tesla.com
dall1-gpgw1.tesla.com
mta_email.tesla.com
mta2_email.tesla.com
emails.tesla.com
click_emails.tesla.com
mta_emails.tesla.com
mta2_emails.tesla.com
mta3_emails.tesla.com
mta4_emails.tesla.com
mta5_emails.tesla.com
view_emails.tesla.com
events.tesla.com
hd13-gpgw1.tesla.com
iad05-gpgw1.tesla.com
itanswrs.tesla.com
lax32-gpgw1.tesla.com
marketing.tesla.com
model3.tesla.com
ptr1.tesla.com
o3.ptr1444.tesla.com
ptr2.tesla.com
o2.ptr556.tesla.com
o7.ptr6980.tesla.com
o5.ptr8466.tesla.com
o6.ptr9437.tesla.com
sim05-gpgw1.tesla.com
acs2-poc.voice.tesla.com
vpnl.tesla.com
xmail.tesla.com
digitalassets-shop.tesla.com
```

Then remove the assetfinder\_subs.txt ,  
ffuf\_subs\_final.txt ,findomain-subs.txt ,  
subfinder\_subs.txt , sublist3r.txtfile:

rm assetfinder\_subs.txt ffuf-subs-final.txt  
findomain-subs.txt subfinder-subs.txt  
sublist3r.txt

## Finding live domains

Not every resolved subdomain will be hosting a web service. HTTP probing helps you identify which subdomains are serving websites.

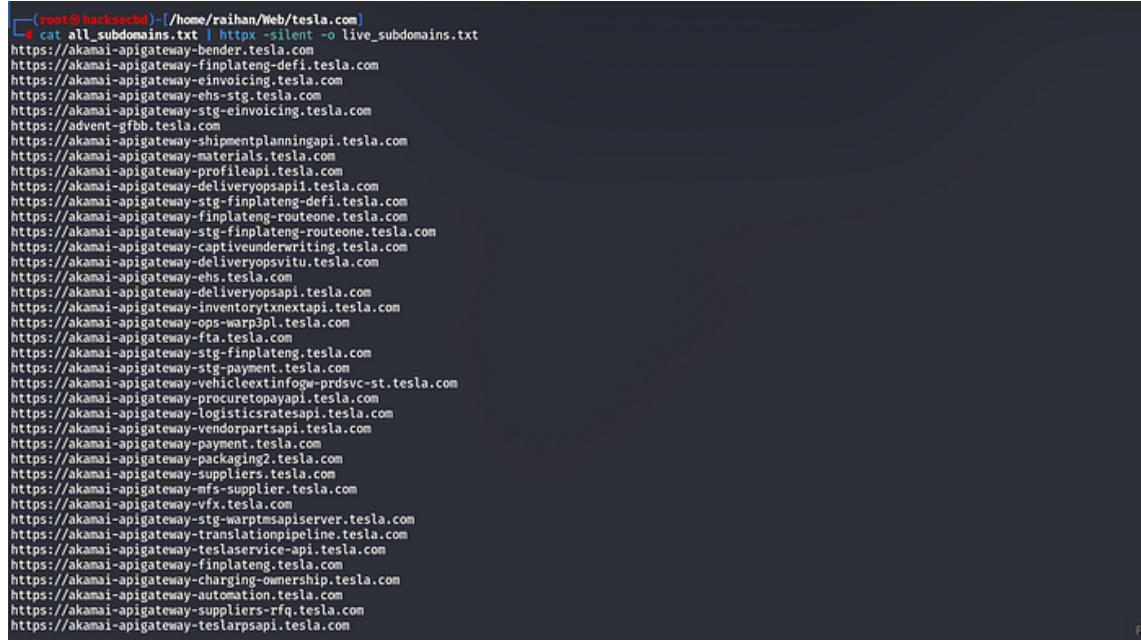
## Finding live domains

- **Tools:** httpx, httprobe

### httpx Example Command:

```
cat all_subdomains.txt | httpx -silent -o  
live_subdomains.txt
```

Press enter or click to view image in full size



```
[root@hackerbd]~[/home/raihan/Web/tesla.com]  
# cat all_subdomains.txt | httpx -silent -o live_subdomains.txt  
https://akamai-apigateway-header.tesla.com  
https://akamai-apigateway-fiplateng-defi.tesla.com  
https://akamai-apigateway-einvoicing.tesla.com  
https://akamai-apigateway-ehs-stg.tesla.com  
https://akamai-apigateway-stg-einvoicing.tesla.com  
https://advent-gfbb.tesla.com  
https://akamai-apigateway-shipmentplanningapi.tesla.com  
https://akamai-apigateway-materials.tesla.com  
https://akamai-apigateway-profileapi.tesla.com  
https://akamai-apigateway-deliveryopsapi1.tesla.com  
https://akamai-apigateway-stg-fiplateng-defi.tesla.com  
https://akamai-apigateway-fiplateng-routeone.tesla.com  
https://akamai-apigateway-stg-fiplateng-routeone.tesla.com  
https://akamai-apigateway-captiveunderwriting.tesla.com  
https://akamai-apigateway-deliveryopsvitu.tesla.com  
https://akamai-apigateway-ehs.tesla.com  
https://akamai-apigateway-deliveryopsapi.tesla.com  
https://akamai-apigateway-inventorytxnextapi.tesla.com  
https://akamai-apigateway-ops-warp3pl.tesla.com  
https://akamai-apigateway-fta.tesla.com  
https://akamai-apigateway-stg-fiplateng.tesla.com  
https://akamai-apigateway-stg-payment.tesla.com  
https://akamai-apigateway-vehicleextinfog-prdsvc-st.tesla.com  
https://akamai-apigateway-procuretopayapi.tesla.com  
https://akamai-apigateway-logisticsratesapi.tesla.com  
https://akamai-apigateway-vendorpartsapi.tesla.com  
https://akamai-apigateway-payment.tesla.com  
https://akamai-apigateway-packaging2.tesla.com  
https://akamai-apigateway-suppliers.tesla.com  
https://akamai-apigateway-mfs-supplier.tesla.com  
https://akamai-apigateway-fx.tesla.com  
https://akamai-apigateway-stg-warptmsapiserver.tesla.com  
https://akamai-apigateway-translationpipeline.tesla.com  
https://akamai-apigateway-teslaservice-api.tesla.com  
https://akamai-apigateway-fiplateng.tesla.com  
https://akamai-apigateway-charging-ownership.tesla.com  
https://akamai-apigateway-automation.tesla.com  
https://akamai-apigateway-suppliers-rfq.tesla.com  
https://akamai-apigateway-teslarpsapi.tesla.com
```

### httprobe Example Command:

```
cat all_subdomains.txt | httprobe | tee -a  
alive_subdomains.txt
```

## Collecting IP Addresses

Once the subdomains are resolved, it's often useful to collect their associated IP addresses for future port

scanning and fingerprinting.

- **Tools:** dnsx, shodanx

# **dnsx with IP Output:**

```
dnsx -l live_subdomains.txt -a -resp-only -o  
live_ips.txt
```

Press enter or click to view image in full size

## shodanx Example:

```
shodanx domain --domain "tesla.com"
```

Press enter or click to view image in full size

```
(raihan@hacksecbd) - [~/Web/tesla.com]
$ shodanx domain --domain "tesla.com" | tee shodanx_ips.txt
tee: shodanx_ips.txt: Permission denied

Shodan Domains
- RevoltSecuritys

[version]:shodanx current version v1.1.1 (latest)

91.239.232.36
37.60.251.247
91.239.232.42
190.224.163.184
14.199.63.164
23.158.136.139
38.47.117.120
44.227.162.90
47.83.127.168
47.243.226.27
52.36.185.222
52.38.42.230
69.165.65.45
69.165.65.102
85.120.81.163
85.120.81.189
85.120.81.208
89.34.227.50
89.213.104.12
89.213.104.105
91.208.184.202
92.112.125.30
103.102.4.10
103.102.5.236
103.196.20.193
104.129.54.56
104.194.68.216
107.172.252.158
```

```
148.135.51.2
154.219.96.164
159.253.120.113
160.30.4.51
163.61.102.106
```

## Identifying, Web Services, technology

- **Tools:** httpx, wappalyzer

### Httpx Example Command:

```
httpx -list live_subdomains.txt -silent -status-code -tech-detect -title -sc -location -td -cl -probe -o httpx_output.txt
```

Press enter or click to view image in full size

```
(root@haksecd0):~/home/raihan/Web/tesla.com
# httpx -list live_subdomains.txt -silent -status-code -tech-detect -title -sc -location -td -cl -probe -o httpx_output.txt
https://akamai-apigateway-e-invoicing.tesla.com [SUCCESS] [201] [https://www.tesla.com/] [0]
https://akamai-apigateway-ehs-stg.tesla.com [SUCCESS] [403] [] [403] [Access Denied] [HSTS]
https://akamai-apigateway-bender.tesla.com [SUCCESS] [301] [https://www.tesla.com/] [0]
https://akamai-apigateway-sgt-e-invoicing.tesla.com [SUCCESS] [403] [] [372] [Access Denied] [HSTS]
https://akamai-apigateway-sgt-e-invoicing.tesla.com [SUCCESS] [301] [https://www.tesla.com/] [0]
https://akamai-apigateway-sgt-fleetmanagement.tesla.com [SUCCESS] [403] [] [403] [Access Denied] [HSTS]
https://akamai-apigateway-sgt-finlateng-routetone.tesla.com [SUCCESS] [403] [] [403] [Access Denied] [HSTS]
https://akamai-apigateway-sgt-finlateng-defi.tesla.com [SUCCESS] [403] [] [407] [Access Denied] [HSTS]
https://akamai-apigateway-sgt-payment.tesla.com [SUCCESS] [503] [] [372] [Service Unavailable] [HSTS]
https://akamai-apigateway-deliveryopsapi.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-inventorytxnextapi.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-profileapi.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-charging-ownership.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-vehicleinfow-prdsvr-st.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-packaging2.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-ops-warpapl.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-ops-warpgpl.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-sgt-inventorytxnextapi.tesla.com [SUCCESS] [503] [] [383] [Internal Server Error] [HSTS]
https://akamai-apigateway-deliveryopsapi.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-mfs-supplier-tesla.com [SUCCESS] [503] [] [380] [Internal Server Error] [HSTS]
http://autodiscover.tesla.com [SUCCESS] [301] [https://outlook.office365.com/mail/?realm=tesla.com\wvd\autodiscover] [0] [HTTP/3,IIS:10.0,Microsoft ASP.NET,Windows Server]
https://advent-gfb.tesla.com [SUCCESS] [403] [] [373] [Service Unavailable]
https://advent-gfb.tesla.com [SUCCESS] [403] [] [373] [Service Unavailable]
https://akamai-apigateway-equipmentplanningapi.tesla.com [SUCCESS] [403] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-ehs.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-captivesunderwriting.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-procuretopayapi.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-logisticsratesapi.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-deliveryopsvit.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-sgt-finlateng.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-dev-warpapiserver.tesla.com [SUCCESS] [503] [] [385] [Internal Server Error] [HSTS]
https://akamai-apigateway-vehicleinfow-prdsvr-st.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-vehicleinfow-prdsvr-st.tesla.com [SUCCESS] [403] [] [383] [Access Denied] [HSTS]
https://akamai-apigateway-sgt-profileapi.tesla.com [SUCCESS] [503] [] [380] [Internal Server Error] [HSTS]
https://akamai-apigateway-sgt-profileapi.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-suppliers-rfq.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-dev-captivesunderwriting.tesla.com [SUCCESS] [503] [] [380] [Internal Server Error] [HSTS]
https://akamai-apigateway-sgt-warpapiserver.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-dev-warpapiserver-upgrade.tesla.com [SUCCESS] [503] [] [387] [Internal Server Error] [HSTS]
https://akamai-apigateway-testlasapi.tesla.com [SUCCESS] [403] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-sgt-warpapiserver.tesla.com [SUCCESS] [403] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-sgt-deliveryopsapi.tesla.com [SUCCESS] [403] [] [383] [Internal Server Error] [HSTS]
https://akamai-apigateway-sgt-captivesunderwriting.tesla.com [SUCCESS] [503] [] [383] [Internal Server Error] [HSTS]
https://akamai-apigateway-sgt-captiveunderwriting.tesla.com [SUCCESS] [503] [] [385] [Internal Server Error] [HSTS]
```

## Finding WAF (Web Application Firewall)

```
cat httpx_output.txt | grep 403
```

Press enter or click to view image in full size

```
(root@haksecd0):~/home/raihan/Web/tesla.com
# cat httpx_output.txt | grep 403
https://akamai-apigateway-ehs-stg.tesla.com [SUCCESS] [403] [] [403] [Access Denied] [HSTS]
https://akamai-apigateway-finlateng-defi.tesla.com [SUCCESS] [403] [] [373] [Access Denied] [HSTS]
https://akamai-apigateway-sgt-finlateng-routetone.tesla.com [SUCCESS] [403] [] [412] [Access Denied] [HSTS]
https://akamai-apigateway-finlateng-defi.tesla.com [SUCCESS] [403] [] [421] [Access Denied] [HSTS]
https://akamai-apigateway-finlateng-routetone.tesla.com [SUCCESS] [403] [] [412] [Access Denied] [HSTS]
https://akamai-apigateway-finlateng-defi.tesla.com [SUCCESS] [403] [] [407] [Access Denied] [HSTS]
https://akamai-apigateway-vehicleinfow-prdsvr-st.tesla.com [SUCCESS] [403] [] [421] [Access Denied] [HSTS]
https://akamai-apigateway-zip3-suppliersequence.tesla.com [SUCCESS] [403] [] [415] [Access Denied] [HSTS]
https://api-firebolt.tesla.com [SUCCESS] [403] [] [380] [Access Denied] [HSTS]
https://api-firebolt-dev.tesla.com [SUCCESS] [403] [] [380] [Access Denied] [HSTS]
https://api-firebolt-stage.tesla.com [SUCCESS] [403] [] [380] [Access Denied] [HSTS]
https://analytics-relay.tesla.com [SUCCESS] [403] [] [381] [Access Denied] [HSTS]
https://auth-global.tesla.com [SUCCESS] [403] [] [378] [Access Denied]
https://apiGateway-userinsights.tesla.com [SUCCESS] [403] [] [391] [Access Denied] [HSTS]
https://auth-global-stage.tesla.com [SUCCESS] [403] [] [389] [Access Denied]
https://autobidder.powerhub.energy.tesla.com [SUCCESS] [403] [] [398] [Access Denied] [HSTS]
https://apps.tesla.com [SUCCESS] [403] [] [366] [Access Denied]
https://cua-hp-me-choose-ui.tesla.com [SUCCESS] [403] [] [401] [Access Denied] [HSTS]
https://billing.tesla.com [SUCCESS] [403] [] [371] [Access Denied] [HSTS]
https://auth.tesla.com [SUCCESS] [403] [] [366] [Access Denied]
https://apiGateway-track-sedgwick-integration-api.tesla.com [SUCCESS] [403] [] [410] [Access Denied] [HSTS]
https://charging-guest-ownership.tesla.com [SUCCESS] [403] [] [398] [Access Denied] [HSTS]
https://eld-ec.tesla.com [SUCCESS] [403] [] [374] [Access Denied] [HSTS]
https://energy-chargecontrol.tesla.com [SUCCESS] [403] [] [409] [Access Denied] [HSTS]
https://autobidder-powerhub.energy.tesla.com [SUCCESS] [403] [] [397] [Access Denied] [HSTS]
https://cybersecurity.tesla.com [SUCCESS] [403] [] [371] [Access Denied] [HSTS]
https://courses.tesla.com [SUCCESS] [403] [] [381] [Access Denied] [HSTS]
https://auth-stage.tesla.com [SUCCESS] [403] [] [376] [Access Denied]
https://bettertime.tesla.com [SUCCESS] [403] [] [374] [Access Denied] [HSTS]
https://cdn-design.tesla.com [SUCCESS] [403] [] [376] [Access Denied] [HSTS]
https://business-ui-ownership.tesla.com [SUCCESS] [403] [] [391] [Access Denied] [HSTS]
https://cx-api-apac.tesla.com [SUCCESS] [403] [] [388] [Access Denied] [HSTS]
```

```
https://bettertime-stage.tesla.com [SUCCESS] [403] [] [382] [Access Denied] [HSTS]
https://cx-apac.tesla.com [SUCCESS] [403] [] [379] [Access Denied] [HSTS]
https://checkout-ui-assets.tesla.com [SUCCESS] [403] [] [388] [Access Denied] [HSTS]
https://cdns-content.tesla.com [SUCCESS] [403] [] [280] [Error] [HSTS]
https://cicerone.tesla.com [SUCCESS] [403] [] [378] [Access Denied] [HSTS]
https://developer.tesla.com [SUCCESS] [403] [] [372] [Access Denied] [HSTS]
https://diner-stg-finplateng.tesla.com [SUCCESS] [403] [] [376] [Access Denied] [HSTS]
https://cus-help-drive-ui.tesla.com [SUCCESS] [403] [] [381] [Access Denied] [HSTS]
https://diner-webapp.tesla.com [SUCCESS] [403] [] [380] [Access Denied] [HSTS]
https://diner-webapp-stage.tesla.com [SUCCESS] [403] [] [388] [Access Denied] [HSTS]
https://digitalcontent.tesla.com [SUCCESS] [403] [] [378] [Access Denied] [HTTP/3]
```

## Find Subdomain Without WAF

```
cat httpx_output.txt | grep -v -i -E
'Cloudfront|imperva|cloudflare' >
non_waf_subs.txt
```

Press enter or click to view image in full size

```
(root@hacksecbd):~/home/raihan/Web/tesla.com
└─# cat httpx_output.txt | grep -v -i -E 'Cloudfront|imperva|cloudflare' > non_waf_subs.txt
└─# cat non_waf_subs.txt
https://akamai-apigateway-einvoicing.tesla.com [SUCCESS] [301] [https://www.tesla.com/] []
https://akamai-apigateway-ehs-stg.tesla.com [SUCCESS] [403] [] [401] [Access Denied] [HSTS]
https://akamai-apigateway-bender.tesla.com [SUCCESS] [301] [https://www.tesla.com/] []
https://accounts.tesla.com [SUCCESS] [403] [] [372] [Access Denied] [HSTS]
https://akamai-apigateway-stg-einvoicing.tesla.com [SUCCESS] [301] [https://www.tesla.com/] []
https://akamai-apigateway-stg-finplateng-defi.tesla.com [SUCCESS] [403] [] [419] [Access Denied] [HSTS]
https://akamai-apigateway-stg-finplateng-routetone.tesla.com [SUCCESS] [403] [] [421] [Access Denied] [HSTS]
https://akamai-apigateway-stg-finplateng-routetone.tesla.com [SUCCESS] [403] [] [421] [Access Denied] [HSTS]
https://akamai-apigateway-stg-finplateng-defi.tesla.com [SUCCESS] [403] [] [421] [Access Denied] [HSTS]
https://akamai-apigateway-stg-payment.tesla.com [SUCCESS] [503] [] [372] [Service Unavailable] [HSTS]
https://akamai-apigateway-deliveryoppapi.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-inventorynexxtapi.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-charging-ownerchip.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-automation.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-packaging2.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-ops-warpapl.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-stg-internalsequence.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-stg-internalsequence.tesla.com [SUCCESS] [503] [] [371] [Internal Server Error] [HSTS]
https://akamai-apigateway-deliveryoppapi.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-mfs-supplier-ut.tesla.com [SUCCESS] [503] [] [485] [Internal Server Error] [HSTS]
http://autodiscover.tesla.com [SUCCESS] [301] [https://outlook.office365.com/mail/realmtesla.com/vwd'autodiscover] []
[HTTP/3,IIS:10.0,Microsoft ASP.NET,Windows Server]
https://advent-gfb.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable]
https://akamai-apigateway-payments.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-shipmentplanningapi.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-ehs.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-captainrewriting.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-vehicleextinfofw-prdsvc-st.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-logisticsapis.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-deliveryoppvtu.tesla.com [SUCCESS] [503] [] [373] [Service Unavailable] [HSTS]
https://akamai-apigateway-stg-finplateng.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-dev-warpimpapiserver.tesla.com [SUCCESS] [503] [] [388] [Internal Server Error] [HSTS]
https://akamai-apigateway-materials.tesla.com [SUCCESS] [503] [] [371] [Service Unavailable] [HSTS]
https://akamai-apigateway-vehicleextinfofw-prdsvc-st.tesla.com [SUCCESS] [403] [] [424] [Access Denied] [HSTS]
https://akamai-apigateway-stg-profileapi.tesla.com [SUCCESS] [503] [] [385] [Internal Server Error] [HSTS]
https://akamai-apigateway-fta.tesla.com [SUCCESS] [503] [] [377] [Service Unavailable] [HSTS]
https://akamai-apigateway-suppliers-rfq.tesla.com [SUCCESS] [503] [] [377] [Service Unavailable] [HSTS]
```

## Visit All Non\_Waf Subdomain Manually

```
cat non_waf_subs.txt | grep 403 | awk '{print $1}'
```

Press enter or click to view image in full size

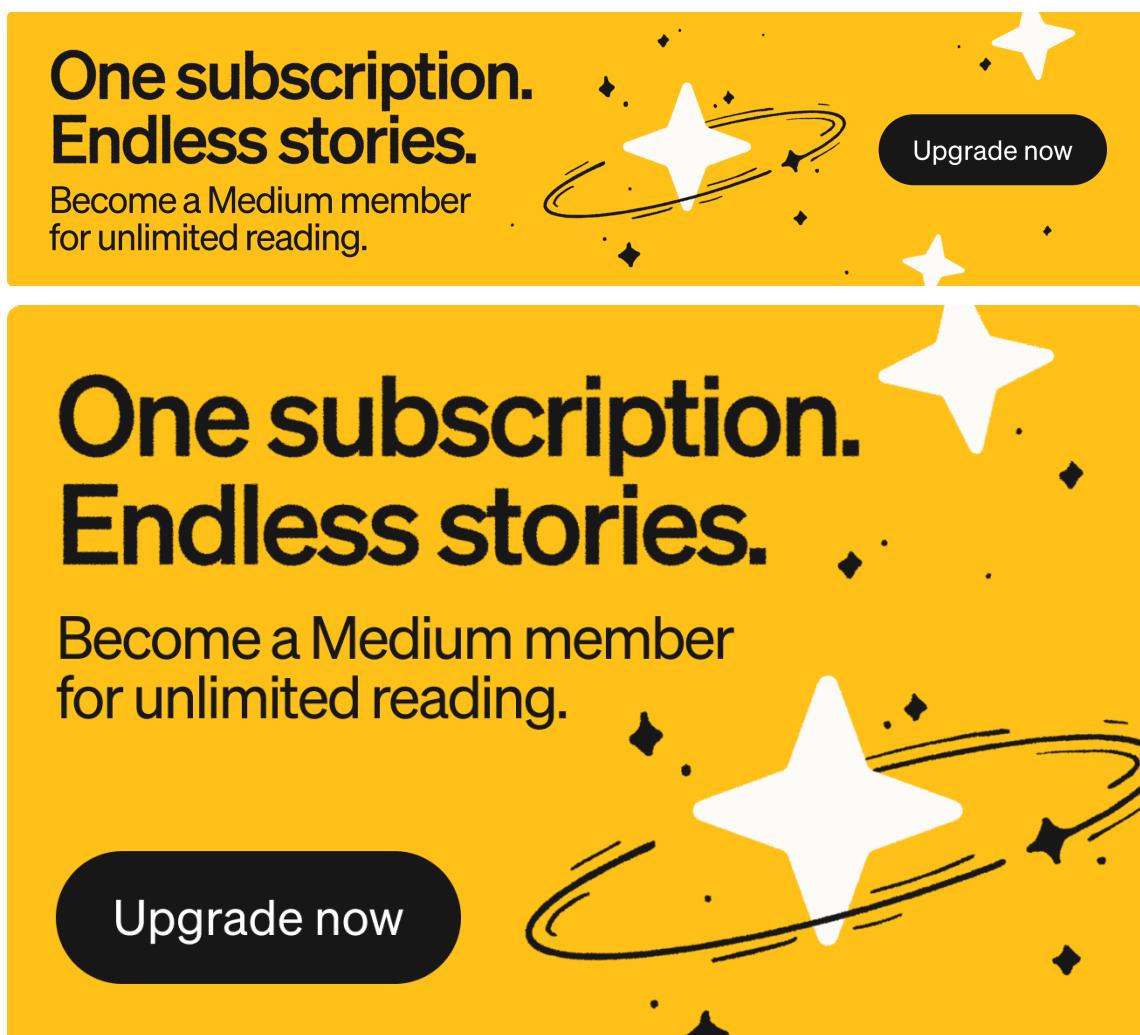
```
(root@hacksecbd):~/home/raihan/Web/tesla.com
└─# cat non_waf_subs.txt | grep 403 | awk '{print $1}' > non_waf_domains.txt
└─# cat non_waf_domains.txt
https://akamai-apigateway-ehs-sig.tesla.com
https://accounts.tesla.com
https://akamai-apigateway-stg-finplateng-defi.tesla.com
https://akamai-apigateway-stg-finplateng-routetone.tesla.com
https://akamai-apigateway-finplateng-routetone.tesla.com
https://akamai-apigateway-finplateng-defi.tesla.com
https://akamai-apigateway-vehicleextinfofw-prdsvc-st.tesla.com
https://akamai-apigateway-zip1-suppliersequence.tesla.com
https://api-firebolt.tesla.com
https://api-firebolt-dev.tesla.com
https://api-firebolt-stage.tesla.com
https://analytics-relay.tesla.com
https://auth-global.tesla.com
https://apigateway-userinsights.tesla.com
https://auth-global-stage.tesla.com
https://autobidder.powerhub.energy.tesla.com
https://apps.tesla.com
https://cua-help-me-choose-ui.tesla.com
https://billing.tesla.com
https://auth.tesla.com
https://apigateway-track-sedgwick-integration-api.tesla.com
https://charging-guest-ownership.tesla.com
https://clld-ec.tesla.com
https://cua-help-me-charge-ui.tesla.com
https://autobidder-preprd.powerhub.energy.tesla.com
https://cyberbeer.tesla.com
https://courses.tesla.com
https://cua-chat-ui.tesla.com
https://auth-stage.tesla.com
https://bettertime.tesla.com
https://design.tesla.com
https://business-ui-ownership.tesla.com
https://cx-api-apac.tesla.com
https://bettertime-stage.tesla.com
https://checkou-ui-assets.tesla.com
https://cdns-content.tesla.com
https://cicerone.tesla.com
https://dro.tesla.com
https://developer.tesla.com
```

<https://cua-test-drive-ui.tesla.com>

## Screenshotting Web Services

When dealing with a large number of subdomains, taking screenshots of each live web server is a great way to visualize them quickly, identify login portals, or other points of interest.

**Tools:** Aquatone, EyeWitness, Gowitness



### Aquatone Example Command:

```
cat live_subdomains.txt | aquatone -out  
screenshots
```

Press enter or click to view image in full size

```
[root@hacksecbd]~/home/raihan/Web/tesla.com]  
# cat all_subdomains.txt | aquatone -out screenshots  
aquatone v1.7.0 started at 2025-10-25T00:38:53+06:00  
  
Targets : 895  
Threads : 12  
Ports   : 80, 443, 8000, 8080, 8443  
Output dir : screenshots  
  
tesla.com: port 80 open
```

```

tesla.com: port 443 open
link.tesla.com: port 80 open
suppliers.tesla.com: port 80 open
www.tesla.com: port 80 open
extgitlab.tesla.com: port 80 open
autobidder-preprd.powerhub.energy.tesla.com: port 80 open
ssl.tesla.com: port 80 open
tf-poc.tesla.com: port 80 open
ss-dev.tesla.com: port 80 open
bettertime.tesla.com: port 80 open
akamai-apigateway-vehicleextinfofw-prdsvc-st.tesla.com: port 80 open
courses.tesla.com: port 80 open
envoy-partnerleadsharing.tesla.com: port 80 open
exp-zcp-cloud-eu-utmfg.tesla.com: port 80 open
akamai-apigateway-stg-captiveunderwriting.tesla.com: port 80 open
cx-api-apac.tesla.com: port 80 open
akamai-apigateway-logisticsratesapi.tesla.com: port 80 open
envoy-partnertasks.tesla.com: port 80 open
teamchat.tesla.com: port 80 open
diner-webapp.tesla.com: port 80 open
myapps.tesla.com: port 80 open
akamai-apigateway-dev-warpmtapiserver.tesla.com: port 80 open
diner-webapp-stage.tesla.com: port 80 open
akamai-apigateway-stg-teslarpsapi.tesla.com: port 80 open
akamai-apigateway-shipmentplanningapi.tesla.com: port 80 open
akamai-apigateway-stg-fta.tesla.com: port 80 open
akamai-apigateway-zip3-suppliersequence.tesla.com: port 80 open
akamai-apigateway-stg-warpassetapi.tesla.com: port 80 open
static-assets-pay.tesla.com: port 80 open
akamai-apigateway-materials.tesla.com: port 80 open
einvoicing.tesla.com: port 80 open
livestreamapi.tesla.com: port 80 open
akamai-apigateway-stg-ops-warpp3l.tesla.com: port 80 open
tcc-graph-stg.tesla.com: port 80 open

```

## Gowitness Example Command:

```
gowitness scan file -f live_subdomains.txt --threads 10 --screenshot-path screenshots
```

Press enter or click to view image in full size

```
[root@backsechd]:/home/raihan/Web/tesla.com
# gowitness scan file -f live_subdomains.txt --threads 10 --screenshot-path screenshots
2025/10/25 00:34:21 WARN no writers have been configured, to persist probe results, add writers using --write-- flags
2025/10/25 00:34:34 INFO result at target=https://akamai-apigateway-finplateng-defi.tesla.com:443 status-code=403 title="Access Denied" have-screenshot=true
2025/10/25 00:34:34 INFO result at target=https://akamai-apigateway-ehs-stg.tesla.com:443 status-code=403 title="Access Denied" have-screenshot=true
2025/10/25 00:34:34 INFO result at target=https://akamai-apigateway-finplateng-defi.tesla.com:443 status-code=200 title="Success" have-screenshot=true
2025/10/25 00:34:34 INFO result at target=https://akamai-apigateway-einvoiceing.tesla.com:443 status-code=200 title="Success" have-screenshot=true
2025/10/25 00:34:37 INFO result at target=https://advent-gfb.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-shipmentplanningapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-materials.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-profileapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-finplateng-defi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-stg-finplateng-defi.tesla.com:443 status-code=403 title="Access Denied" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-stg-finplateng-routeone.tesla.com:443 status-code=403 title="Access Denied" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-stg-finplateng-routeone.tesla.com:443 status-code=403 title="Access Denied" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-deliveryopsvitu.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-deliveryopsvitu.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-inventoryxnextapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-cos-warpp3l.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:34:39 INFO result at target=https://akamai-apigateway-ftesla.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:22 INFO result at target=https://akamai-apigateway-stg-finplateng.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:24 INFO result at target=https://akamai-apigateway-stg-finplateng.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:24 INFO result at target=https://akamai-apigateway-stg-finplateng.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:27 INFO result at target=https://akamai-apigateway-procurementapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:27 INFO result at target=https://akamai-apigateway-procurementapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:27 INFO result at target=https://akamai-apigateway-logisticsratesapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:31 INFO result at target=https://akamai-apigateway-vendorpartsapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:34 INFO result at target=https://akamai-apigateway-packaging2.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:39 INFO result at target=https://akamai-apigateway-suppliers.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:39 INFO result at target=https://akamai-apigateway-suppliers.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:40 INFO result at target=https://akamai-apigateway-vfx.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:40 INFO result at target=https://akamai-apigateway-vfx.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:45 INFO result at target=https://akamai-apigateway-stg-reqtmssapiserver.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:52 INFO result at target=https://akamai-apigateway-translationpipeline.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:59 INFO result at target=https://akamai-apigateway-testservice-api.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:35:59 INFO result at target=https://akamai-apigateway-finplateng.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:36:00 INFO result at target=https://akamai-apigateway-chargepoint.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:36:07 INFO result at target=https://akamai-apigateway-xmltms.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:36:11 INFO result at target=https://akamai-apigateway-suppliers-rfq.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
2025/10/25 00:36:13 INFO result at target=https://analytics-relay.tesla.com:443 status-code=200 title="Electric Cars, Solar & Clean Energy | Tesla" have-screenshot=true
2025/10/25 00:36:16 INFO result at target=https://akamai-apigateway-zip3-suppliersequence.tesla.com:443 status-code=403 title="Access Denied" have-screenshot=true
2025/10/25 00:36:20 INFO result at target=https://akamai-apigateway-warpassetapi.tesla.com:443 status-code=503 title="Service Unavailable" have-screenshot=true
```

## Eyewitness Example Command:

```
eyewitness -f ips.txt --web --directory /path/to/output
```

## Port scanning

Port scanning is the process of probing a network host to identify open, closed, or filtered network ports, which reveals which services are running and potential points of entry.

**Tools:** nmap, naabu

### **Naabu Example Command:**

```
naabu -list live_subs.txt -o naabu_scans.txt
```

## **Content Discovery (Directory and File Bruteforcing)**

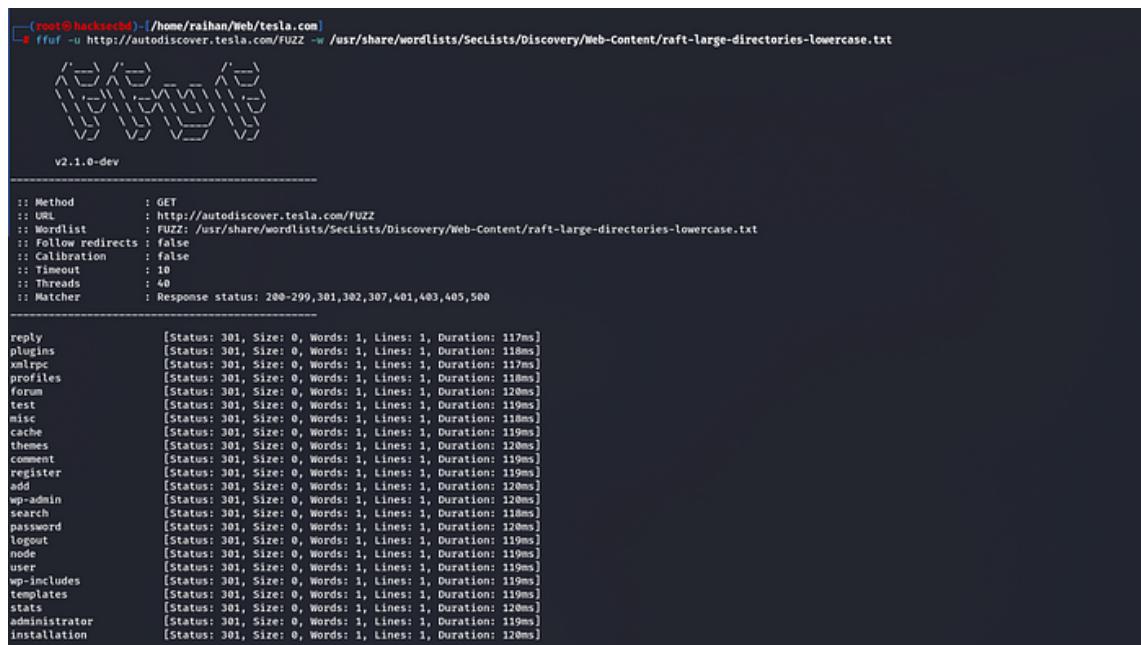
Directory bursting (also known as directory brute forcing) is a web application technology used to find and identify possible hidden directories in websites. This is done with the aim of finding forgotten or unsecured web directories to see if they are vulnerable to exploitation.

**Tools:** FFuf, Gobuster,Dirsearch

### **FFUF Example Command:**

```
ffuf -u https://example.com/FUZZ -w //path/to/wordlist.txt
```

Press enter or click to view image in full size



```
(root@hacksec0d)-[~/home/raihan/Web/tesla.com]
# ffuf -u http://autodiscover.tesla.com/FUZZ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-directories-lowercase.txt
V2.1.0-dev

:: Method      : GET
:: URL        : http://autodiscover.tesla.com/FUZZ
:: Wordlist   : FUZZ: /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-directories-lowercase.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500

reply          [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 117ms]
plugins        [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 118ms]
xmlrpc         [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 117ms]
profiles       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 118ms]
forum          [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
test           [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
misc            [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 118ms]
cache           [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
themes          [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
comment         [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
register        [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
add             [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
admin           [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
search          [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 118ms]
password        [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
logout          [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
node            [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
user             [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
wp-includes      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
templates       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
stats            [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
administrator   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 119ms]
installation    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 120ms]
```

### **Gobuster Example Command:**

```
gobuster dir --url https://example.com --
```

```
wordlist /path/to/wordlist.txt
```

### **Dirsearch Examples Command:**

```
dirsearch -u https://target.com/ -w /usr/share/wordlists/custom.txt --full-url --random-agent -x 404,400 -e php,html,js,json,ini
```

## **Extract URLs**

Sometimes, older versions of the website might expose endpoints or parameters that are not available on the live site. You can use archived data from the Wayback Machine to discover such URLs.

**Tools:** waybackurls,GAU,waymore

Acctive Tool: katana

### **Waybackurls Examples Command:**

```
cat live_subs.txt | waybackurls | anew wayback_urls.txt
```

### **Gau Examples Command:**

```
cat live_subs.txt | gau | anew gau_urls.txt
```

### **Waymore Examples Command:**

```
cat live_subs.txt | waymore | anew wayback_urls.txt
```

## **Acctive scanns**

### **Katana Examples Command:**

```
katana -list live_subdomain.txt -f qurl | anew katana_urls.txt
```

Press enter or click to view image in full size

```
[root@hacksec0d ~]# /home/raihan/Web/tesla.com
```

```
[INFO] Current katana version v1.2.2 (latest)
[INFO] Started standard crawling for >> https://mfs-supplier-uat.tesla.com
[INFO] Started standard crawling for >> https://sjc36-gppwl.tesla.com
[INFO] Started standard crawling for >> https://hermes-stream-api.prd.eu.vn.cloud.tesla.com
[INFO] Started standard crawling for >> https://mobile-links.prd.vn.cloud.tesla.com
[INFO] Started standard crawling for >> https://digitalcontent.tesla.com
[INFO] Started standard crawling for >> https://link.qa.tesla.com
[INFO] Started standard crawling for >> https://tcc-graph.tesla.com
[INFO] Started standard crawling for >> https://mfs-supplier-gfb.tesla.com
[INFO] Started standard crawling for >> https://kronos.tesla.com
[INFO] Started standard crawling for >> https://fleetview.prd.europe.fn.tesla.com
https://link.qa.tesla.com
https://mfs-supplier-uat.tesla.com
https://digitalcontent.tesla.com
https://kronos.tesla.com
https://mfs-supplier-gfb.tesla.com
https://hermes-stream-api.prd.eu.vn.cloud.tesla.com
https://tcc-graph.tesla.com
https://sjc36-gppwl.tesla.com
https://sjc36-gppwl.tesla.com/global-protect/login.esp
https://mobile-links.prd.vn.cloud.tesla.com
[INFO] Started standard crawling for >> https://hermes-stream-api.prd.vn.cloud.tesla.com
[INFO] Started standard crawling for >> https://akamai-apigateway-stg-warpedi.tesla.com
[INFO] Started standard crawling for >> https://vehicle-files.prd.euvn.vn.cloud.tesla.com
[INFO] Started standard crawling for >> https://cyberbeer.tesla.com
[INFO] Started standard crawling for >> https://digitalassets-learning.tesla.com
[INFO] Started standard crawling for >> https://gigalife.tesla.com
[INFO] Started standard crawling for >> https://stg-uc-twilio-bpm-webhook.tesla.com
[INFO] Started standard crawling for >> https://cdn-design.tesla.com
https://cdn-design.tesla.com
https://cyberbeer.tesla.com
https://gigalife.tesla.com
https://stg-uc-twilio-bpm-webhook.tesla.com
https://hermes-stream-api.prd.vn.cloud.tesla.com
https://digitalassets-learning.tesla.com
[INFO] Started standard crawling for >> http://bolt.tesla.com
https://fleetview.prd.europe.fn.tesla.com
```

# Combine all URIs into one file

```
cat katana_urls.txt wayback_urls.txt  
gau_urls.txt wayback_urls.txt | anew  
all_urls.txt
```

## Crawling and Spidering

You can automate crawling of the target website to discover deeper endpoints, hidden forms, or parameters for attacks like XSS or SSRF.

Louis. Katalina, ,Gospidet

# Katana Example Command.

```
katana -list All_uris.txt -silent -d 0 -it 20 -  
f qurl -ef js,css, -o katana_Crawl.txt
```

Press Enter or click to view image in full size

# Gospider Example Command:

```
gospider -s https://target.com -d 1 -o  
gospider_crawl.txt
```

# Parameter Discovery

Bruteforcing for parameters can help uncover hidden endpoints vulnerable to injections like SQLi or XSS.

**Tools:** Arjuh, kataha, FFUF

## Katana Example Command:

```
katana -list live_subdomains.txt -silent -d 6 --  
rl 20 -f qurl -ef js,css, | anew  
katana_params.txt
```

## Arjun Example Command:

arjun -u "https://target.com"

Press enter or click to view image in full size

```
$ arjun -u https://accounts.tesla.com
[!] JUN v2.2.7

[*] Scanning 0/1: https://accounts.tesla.com
[*] Probing the target for stability
[*] Analysing HTTP response for anomalies
[*] Extracting parameters from the response for testing: buildId, languageCode, page, zh2811, locale, ou, currentPath, teslaHost, localeCode, cnDomain, regionName, languageName, callback_url_path, redirect_url_path, adminName, countryCode, defaultLocale, localeUrlPrefix, countryNameLocalized, countryName
[*] LogicForcing the URL endpoint
[*] Webpage is returning different content on each request. Skipping.
[*] No parameters were discovered.
```

# Filtering Interesting URLs

To focus on potentially vulnerable URLs, you can use GF (Grep patterns for fuzzing).

## Tools: GF

## **GF Example Command:**

```
cat all_urls.txt | gf xss | anew  
xss_candidates.txt  
cat all_urls.txt | gf sqli | anew  
sqli_candidates.txt  
cat all_urls.txt | gf ssti| anew  
ssti_candidates.txt  
cat all_urls.txt | gf xxe| anew  
xxe_candidates.txt
```

## Fingerprinting Web Technologies

Understanding the technologies in use can help you tailor your attacks. For instance, knowing the CMS or the web server can lead you to specific vulnerabilities or exploits.

**Tools:** Wappalyzer, WhatWeb

**Wappalyzer (Browser Extension):** Simply browse the target site to see technologies in use.

**WhatWeb Example Command:**

```
whatweb target.com
```

Press enter or click to view image in full size

```
[root@backtrack] :/home/railhan/Web/tesla.com  
# whatweb accounts.tesla.com  
accounts.tesla.com [403 Forbidden] Akamai-Global-Host, Country[UNITED STATES][US], HTTPServer[AkamaiGHHost], IP[23.204.252.56], Title[Access Denied], UncommonHeaders[x-reference-error,  
akamai-request-bc,permissions-policy]  
https://accounts.tesla.com [403 Forbidden] Akamai-Global-Host, Country[UNITED STATES][US], HTTPServer[AkamaiGHHost], IP[23.204.252.56], Strict-Transport-Security[max-age=15768000], Title[Access Denied], UncommonHeaders[x-reference-error,akamai-request-bc,permissions-policy]
```

## Mapping the Attack Surface: Identifying Entry Points

Now that you've collected subdomains, URLs, and ports, it's time to map out the target's attack surface. This includes testing for vulnerable technologies and hidden paths.

# JS File Analysis

JavaScript files can leak sensitive information like API keys, hardcoded secrets, or even useful endpoints.

**Tools:** katana, LinkFinder, JSFinder, subjs

```
cat All_urls.txt | grep "\.js" | anew  
katana_js.txt
```

## Katana Example Command:

```
cat all_urls.txt | grep "\.js" | anew  
katana_js.txt
```

Press enter or click to view image in full size

# **LinkFinder Example Command:**

```
python3 linkfinder.py -i https://target.com/app.js -o cli
```

## Subjs Example Command:

```
subjs -i https://target.com | anew  
js_endpoints.txt
```

# **Others File Analysis**

```
cat All_urls.txt | grep -E "\.txt|\.\log|
```

\.cache|\.secret|\.db|\.backup|\.yml|\.json|  
\.gz|\.rar|\.zip|\.config"

## **Now Start Vulnerability Testing...**