Information Gathering (Reconnaissance)

Passive Recon There are two types

Physical site or **social site**

PHYSICAL SITE: Include Satellite Images, Drone Recon

Building Layout (Badge Reader, Break areas, Security, Fencing)

Example: **JOB INFORMATION**

Include Employee (name, job title, phone number, manager, etc.)

Pictures (Badge photo, desk photos, computer photo, etc.)

WEB \ HOST

WHOIS, nslookup, dnsrecon

FINDING SUBDOMAINS

Google FU, dig, NMap, Sublist3r, Bluto, crt.sh, etc.

FINGERPRINTING - what running on website and what is running on host & what kind of service out there, (IAS, APACHE) what version it was running it

NMap, Wappalyzer, WhatWeb, BuiltWith, Netcat

DATA BREACHES - is the most common way external assessment into network

HavelBeenPwned, Breach-Parse, WeLeanInfo. (Homedepo, AquaFax, LinkedIn)

Identify our targets

WWW.bugcrowd.com (is a public bug bounty program)

Establish client to attack,

WE are using TESLA Program. (Consider tesla is our target)

E-Mail Address Gathering with Hunter.io

E-Mail Address Gathering with **Hunter.io**

Look out basic items, which are available on internet.

- Users
- Email format
- Breach Credentials

Breach-Parse\GitHub\sh

Gathering Breached Credentials with Breach-Parse

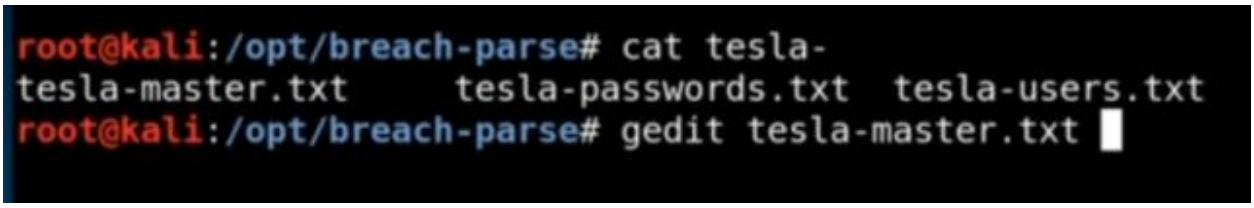
Go to GitHub:

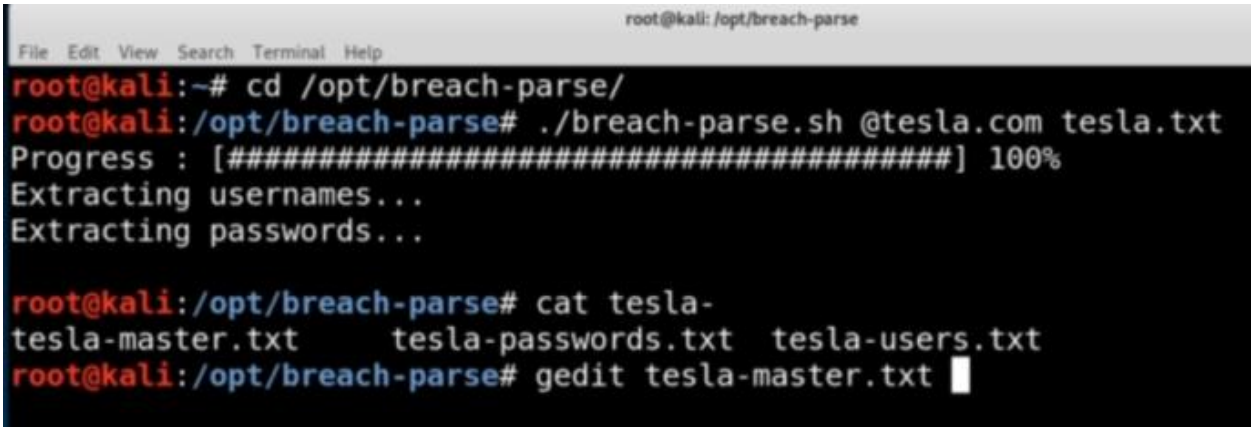
https://github.com/hmaverickadams/

https://github.com/hmaverickadams/breach-parse

click on breachparse.sh

Go to Linux and type below command and do not perform this





After opening the file using pluma, we can see the email id and passwords, which is going to be show first name and passwords.

Gather info breach parse

This website allow you to find all the username and password from just pay two$ and get email phone domains etc.

https://weleakinfo.to/

Utilizing the harvester

>> used to find the usernames and subdomains.

>> Open kali and open terminal

Example:

>> **theHarvester -d tesla.com -l 500 -b google**

```
[*] Target: tesla.com

[*] Searching Google.
        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.

[*] No IPs found.

[*] Emails found: 7
----------------------
cam@tesla.com
ckawai@tesla.com
designer@tesla.com
ir@tesla.com
press@tesla.com
wmcclary@tesla.com
wstockton@tesla.com

[*] Hosts found: 5
---------------------
energysupport.tesla.com:136.143.190.74
forums.tesla.com:23.9.221.3
ir.tesla.com:96.17.150.105, 96.17.150.137
livestream.tesla.com:23.9.221.3
www.tesla.com:23.9.221.3
```

theHarvester -d microsoft.com

\\ **-d** is domain

\\ **-l** is limit number of 500 search

\\ **-f** is print results

```
Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
                        google, google-certificates, googleCSE, googleplus, goog
le-profiles,
                        hunter, linkedin, netcraft, pgp, threatcrowd,
                        twitter, vhost, virustotal, yahoo, all
       -g: use Google dorking instead of normal Google search
       -s: start in result number X (default: 0)
       -v: verify host name via DNS resolution and search for virtual hosts
       -f: save the results into an HTML and XML file (both)
       -n: perform a DNS reverse query on all ranges discovered
       -c: perform a DNS brute force for the domain name
       -t: perform a DNS TLD expansion discovery
       -e: use this DNS server
       -p: port scan the detected hosts and check for Takeovers (80,443,22,21,80
80)
       -l: limit the number of results to work with(Bing goes from 50 to 50 resu
lts,
```

```
Examples:
        theharvester -d microsoft.com -l 500 -b google -f myresults.html
        theharvester -d microsoft.com -b pgp, virustotal
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d microsoft.com -l 200 -g -b google
        theharvester -d apple.com -b googleCSE -l 500 -s 300
        theharvester -d cornell.edu -l 100 -b bing -h
```

Hunting subdomains IMP

hunting subdomains

>> Open kali and terminal

we have to gather information of what subdomains out there

>> *.tesla.com # this * is wild card: means anything or everything open to us except out of scope is in subdomain range'

Subdomains, which are look like

>> dev.tesla.com OR >> testsite.tesla.com

for hunt this down via using **Sublist3r tool**

Open terminal and install sublist3r tool

>> **apt install sublist3r**

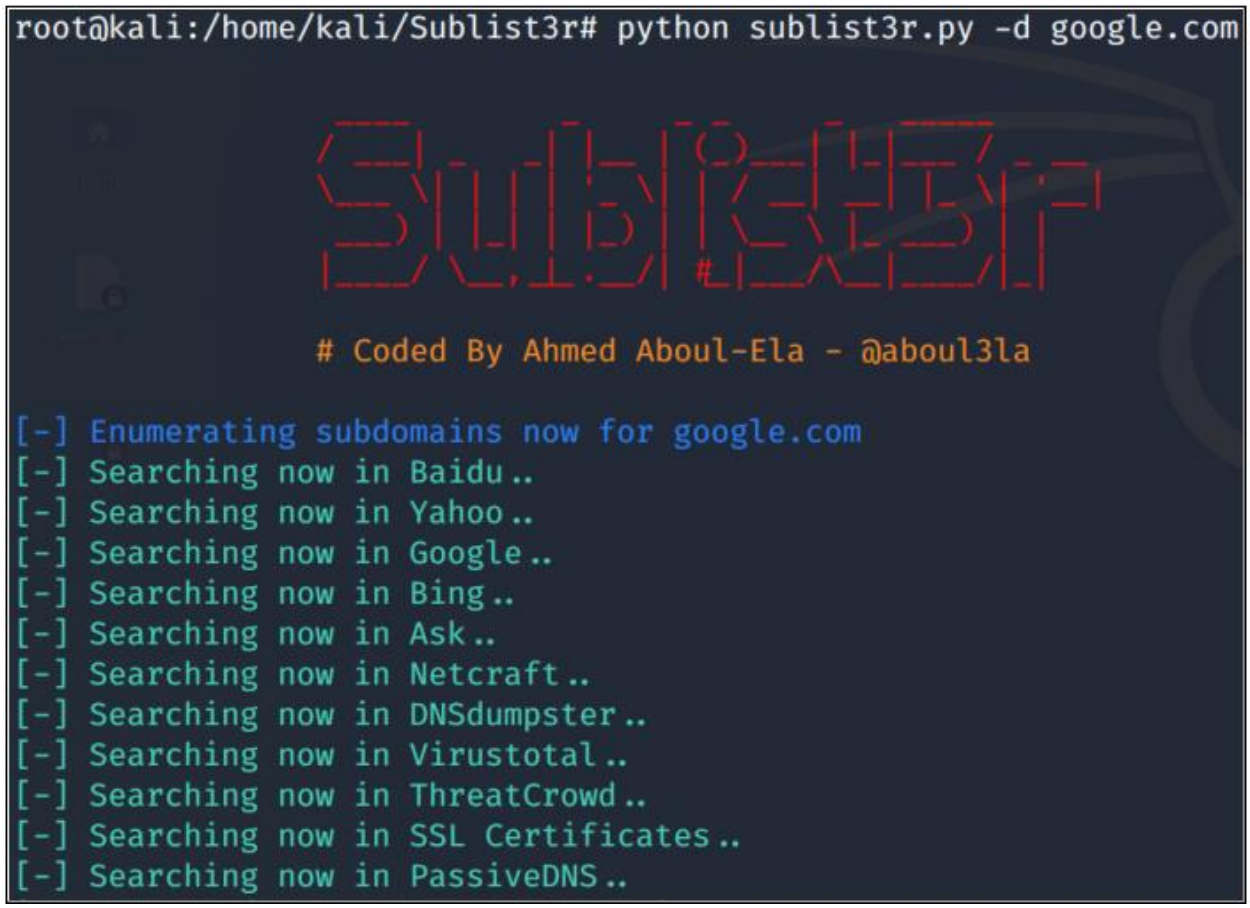
>> **sublist3r -d google.com**

********** (if not working then follow this step) **********

>> **git clone https://github.com/aboul3la/Sublist3r.git**

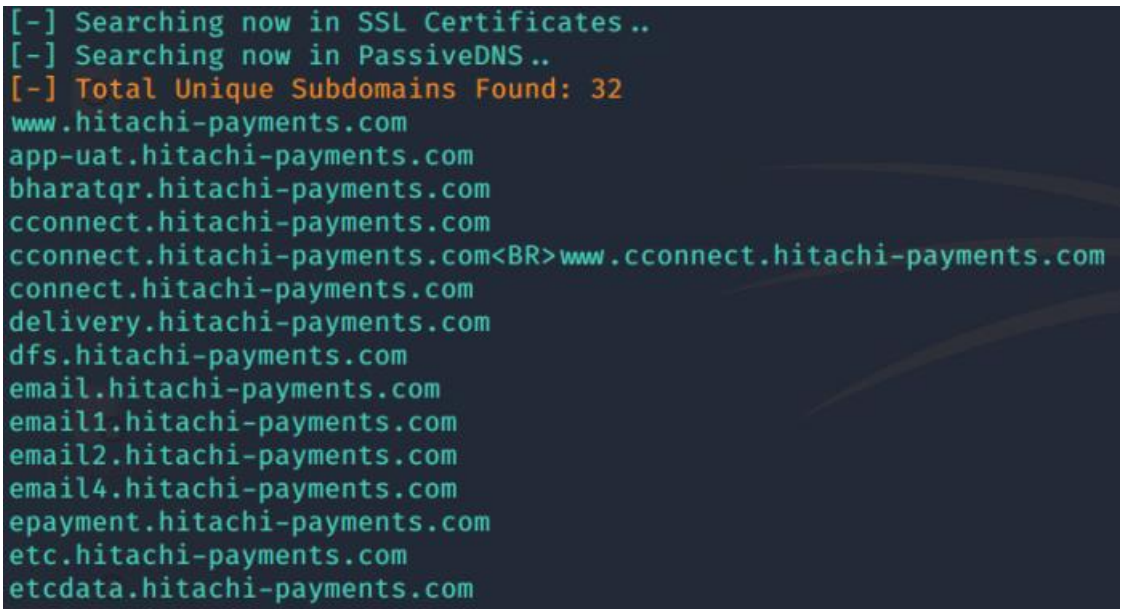
>> **pip install -r requirement.txt**

>> **python sublist3r.py –h**



Example:

>> **sublist3r -d hitachi-payments.com -t 100**



More details you want to find more details information of subdomains just go through

Go to google.com and search

https://github.com/tomnomnom/httprobe

Find out the results.

2nd way to check subdomains

Go to website

>> **crt.sh**

>> Type **domain name** and **extensions**

Like **google.com**, **hitachi-payments.com** or facebook.com

---

3rd way to check subdomain hunting

Go to google.com

>> owasp amass

https://github.com/OWASP/Amass

Follow link, install in kali machine, and check all possibilities

Identify web tech

1st Method

Identify the website technologies

Go to google machine

Search

>>https://builtwith.com/

In addition, get to how company developed website on what platform they used

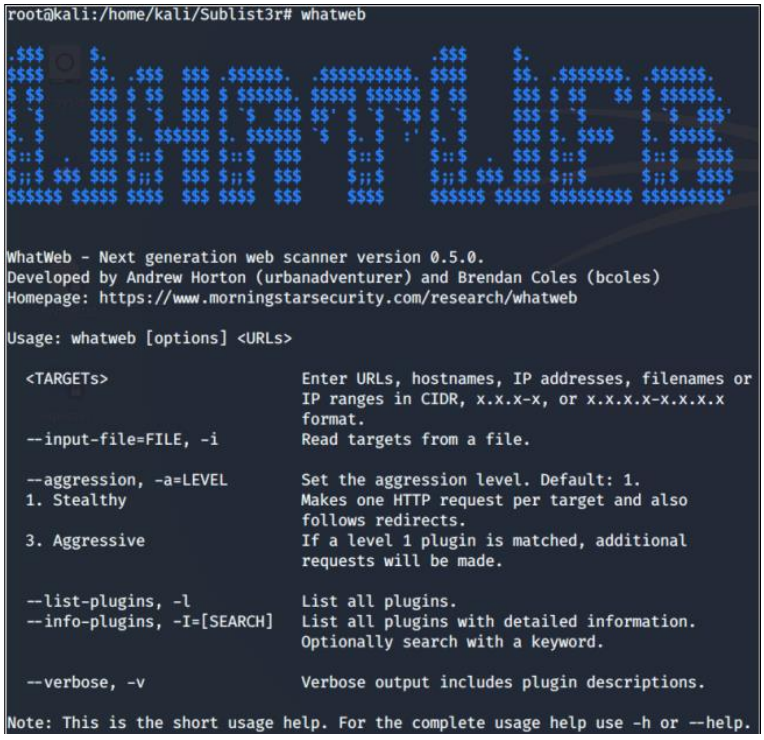
>> https://www.wappalyzer.com/ is web plug-in Extension, which can added in browser

---

2nd method

Open terminal & type WHATWEB is kali Linux inbuilt tool. Which can help to gather information

>> **whatweb**



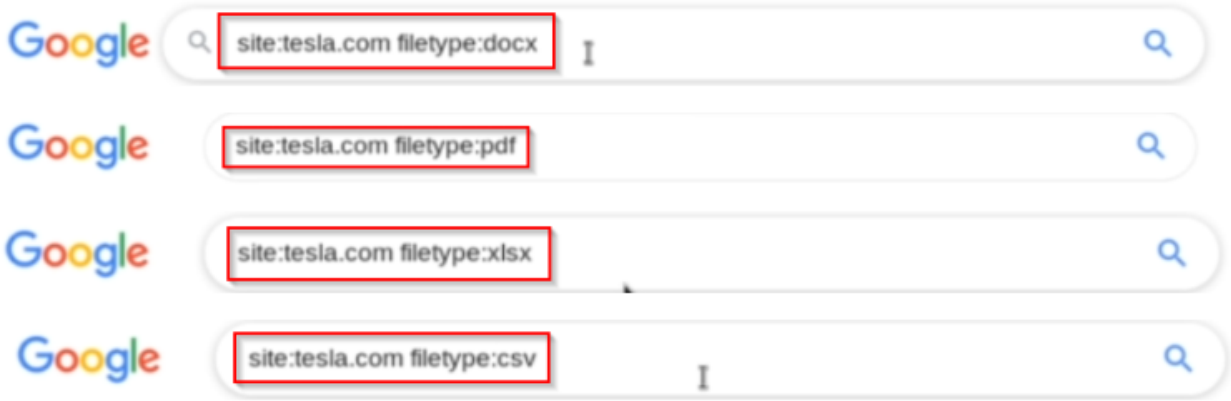
>> whatweb http://www.google.com

>> whatweb http://www.hitachi-payments.com

Google Fu

We can also find sensitive information if we search like this way.

Lot of information is sometimes available out there without even security. Simply we can find with google.



Burp Suite

Information gathering tool built in available in kali Linux

Burp suite also name Web Proxy: means it has capability to intercepting web traffic for us

>> Select the temp project

>> Select the start burp

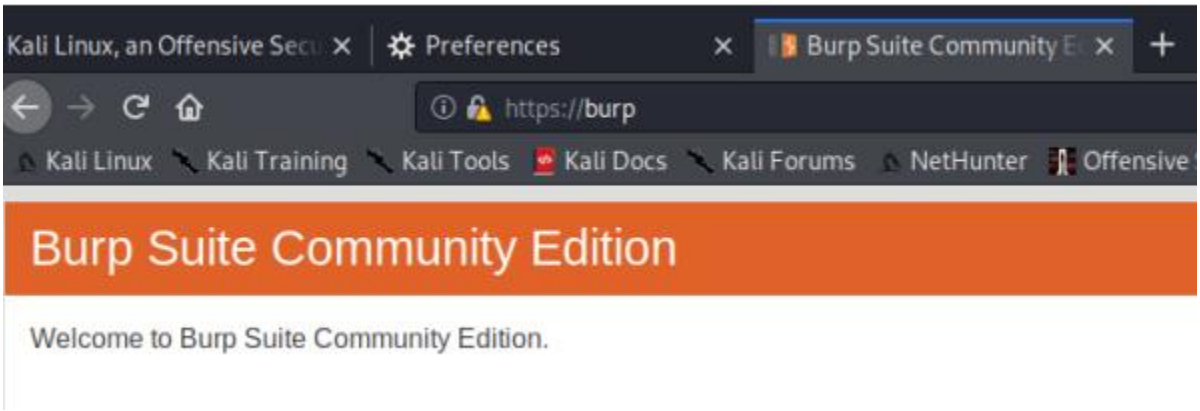
>> Open Firefox and go to preference and select setting at bottom.

>> Network Proxy and settings

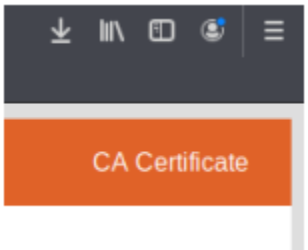
>> Select manual proxy configuration ip is 127.0.0.1 8080.

>> Select the checkbox "Use this proxy server for all protocols (install **foxy proxy** for immediate switch)

>> open the new tab and paste this **https://burp** search bar.



>> Download the CA Certificates and save the **cacert.der** file.

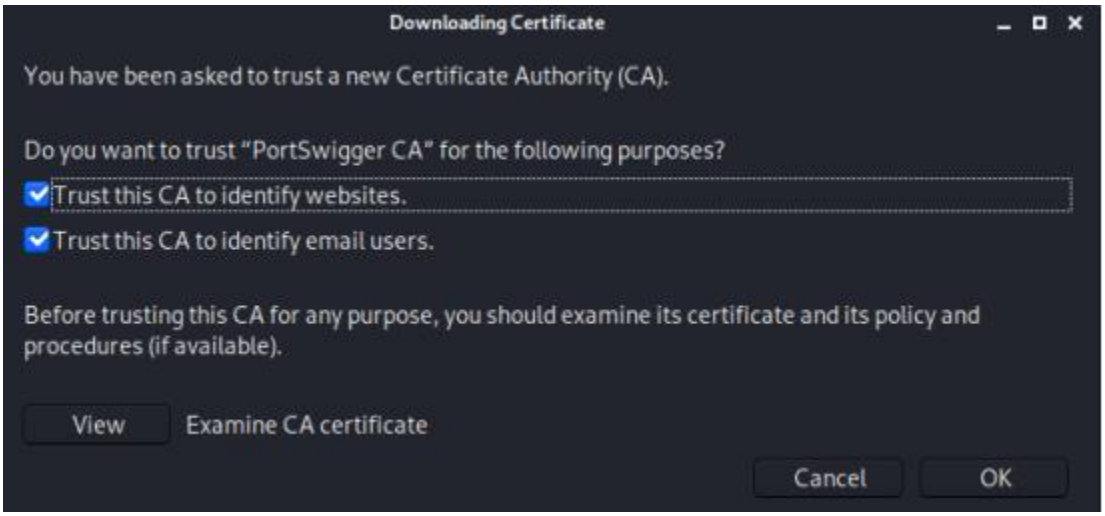


>> Now go to Privacy and security tab.

>> click on certificate and select view certificate.

>> click on import and select cacert.der file and open,

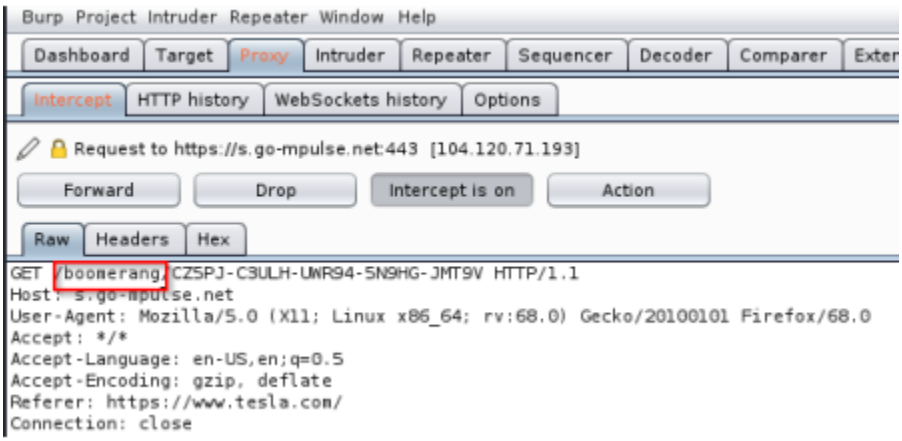
>> select both check box. And press ok



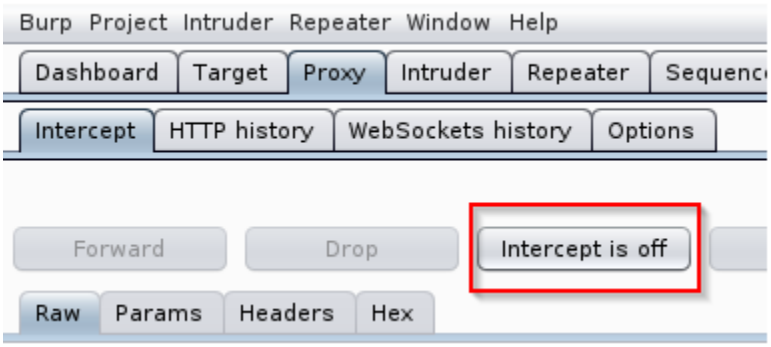
>> Now search website tesla.com and go to burp suite

>> go to proxy tab and click forward tab, # what we are doing the intercepting the request tesla is making out

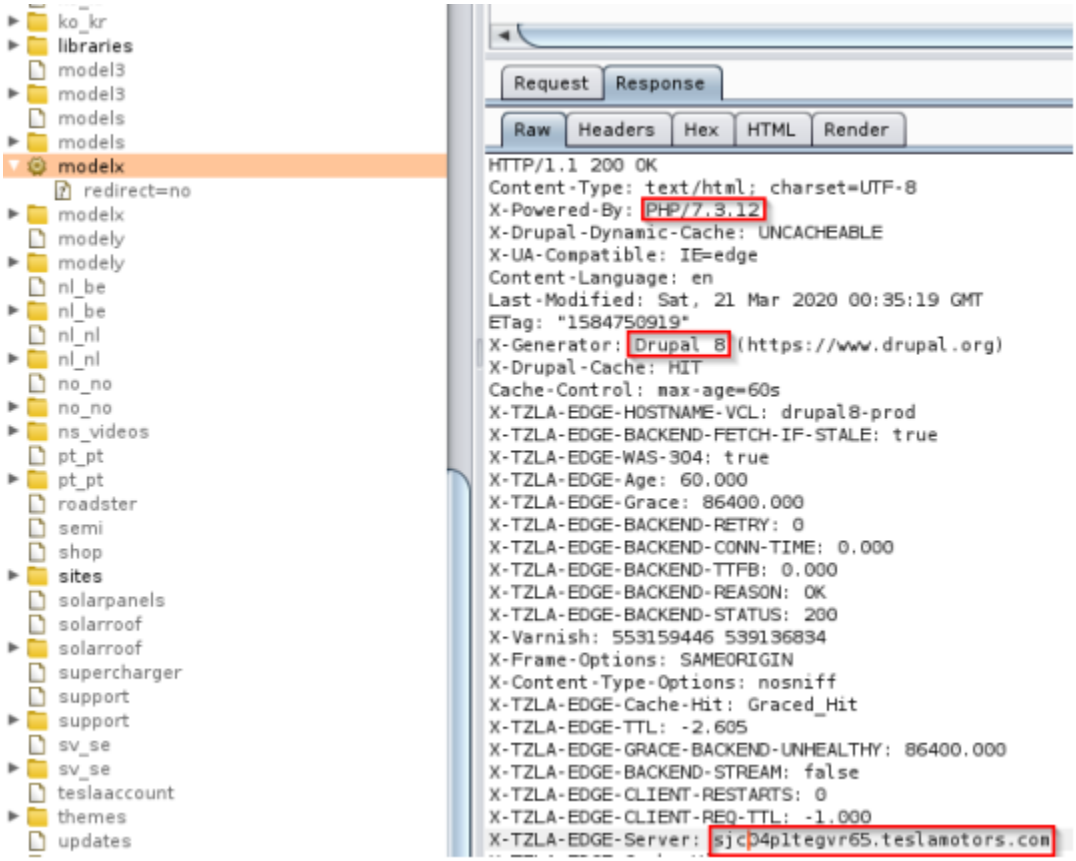
(We got the API request here we se boomerang request coming)



>> We can change to GET method to POST and turnoff the Intercept



>> go to target tab and check left side tesla.com and explore.



>> We can get the all information about it also if we purchase and pro version of burp suite and we can find vulnerability of website. ($400) cost pro edition burp suite.