***Gather information***

Ref: [S](https://portswigger.net/web-security/cross-site-scripting/exploiting)pin the hack YouTube channel

### ***1. Subdomain capture***

***https://github.com/blechschmidt/massdns***

***Setup***

mkdir tools

cd tools

git clone https://github.com/blechschmidt/massdns.git

cd massdns

make

cd bin

sudo cp massdns /usr/local/bin

***Run***

***Get domains and subdomains***

mkdir proj1

cd proj1

amass enum -d tesla.com -passive -o domain\_subdomains.txt

or

assetfinder tesla.com > domain\_subdomains.txt

cat domain\_subdomains.txt

massdns -r ../tools/massdns/lists/resolvers.txt -t A -o S -w live\_subdomain.txt dns\_file.txt

cat live\_subdomain.txt

sed 's/A.\*// ; s/CN.\*//; s/\..$//' live\_subdomain.txt > clean\_live\_subdomain.txt

### ***2. Gather other information***

a) Whois.domaintools.com

Enter the domain name

Get important information

b) sitereport.netcraft.com

Enter the domain name

Get Ipv4 address

IP location

character encoding

http compression

Web Browser Targeting

c) Port scan

nmap domain.com / ~~nmap -p0- -v -A -T4 scanme.nmap.org~~

This will show the reports of open ports

d) Gather DNS info

robotex.com

e) Find directory

dirb http://domain.com

f) Advanced subdomain finder or Knockpy

https://subdomainfinder.c99.nl/

knockpy domain.com > all\_domain.txt

Install all tools related to bug bounty hunting tools at bbht github

* git clone <https://github.com/nahamsec/bbht.git>
* cd bbht
* chmod +x install.sh
* ./install.sh

Check if http or https server are there are not using httprobe

cat domains.txt | httprobe --prefer-https

cat domains.txt | httprobe -p http:81 -p https:8443