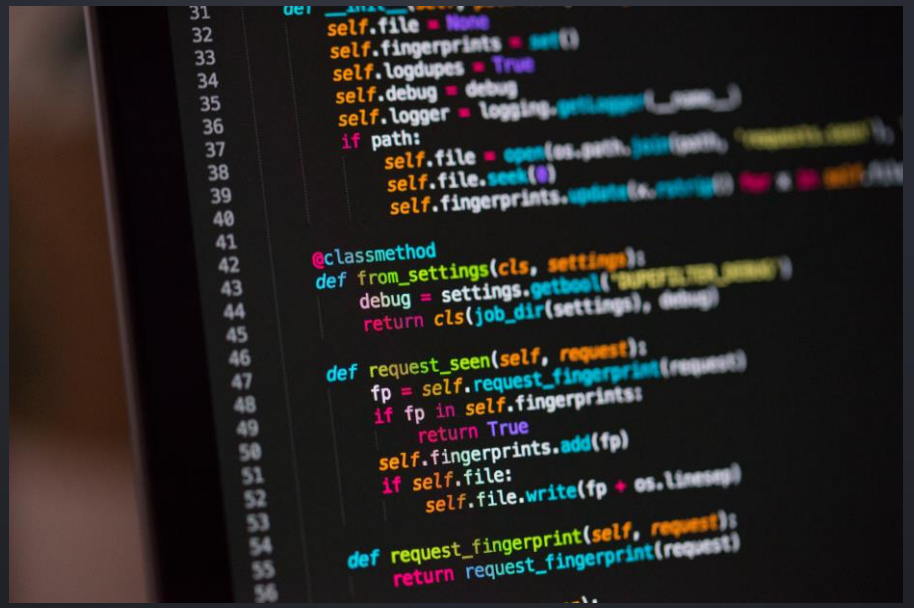
Python for Pentesters

نادي أمن الملعومات - جامعة الملك عبدالعزيز
تقديم : عبدالله محمد الكثيري

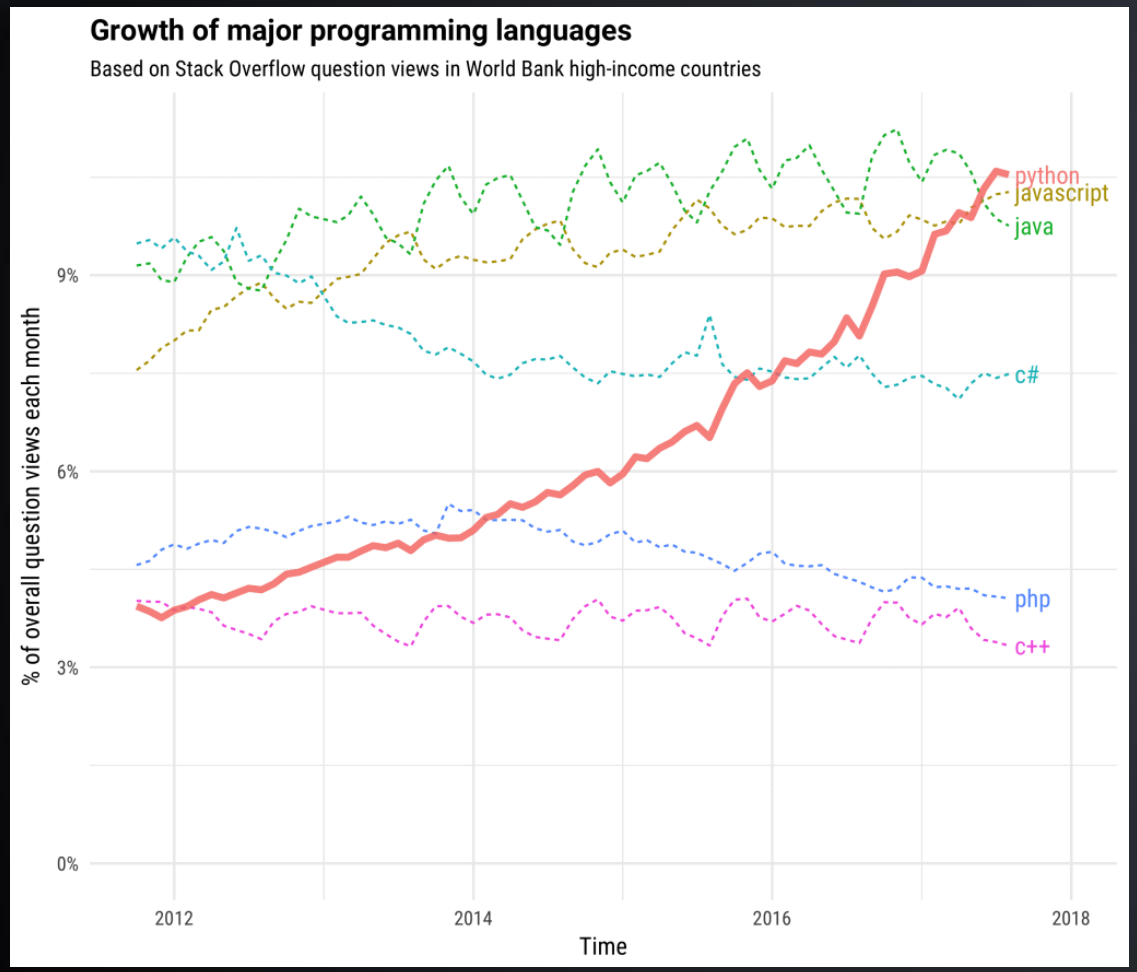
مقدمة عن لغة بايثون

تعتبر لغة بايثون قوية جدا في مجالات كثيرة مثل علوم البيانات والحساب الرياضي وتطوير الويب والبرامج والذكاء الاصطناعي وأيضا الأمن السيبراني
وذالك يعود لقوة وظائفها ومكتباتها والدعم القوي من المجتمع الخاص بها

حاليا تقوم الكثير من الجامعات الأمريكية والجامعات الأوروبية بتضمين مادة البرمجة وحل المشكلات في مناهجها



لماذا يجب علينا تعلم لغة بايثون ؟



- بايثون من أفضل اللغات التي يمكن تعلمها في البداية
سهلة التعلم، كتابتها بسيطة، سهلة التتبع Debugging

- مصادر تعلم كثيرة جداً ومجانية
بايثون لغة مفتوحة المصدر ولها دعم كبير من قبل المطورين

- يتم استخدامها في أغلب المجالات التقنية
ويب، تطبيقات سطح المكتب، الخوادم، أمن المعلومات، الخ.....

- اللغة بسيطة الكتابة، قريبة من اللغة الانجليزية
تبدوا اوامر لغة بايثون قريبة من الكلمات الانجليزية

لغة بايثون لمختبري الإختراق

- لغة بايثون سهلة التعلم والتطبيق

أغلب المتخصيين في مجال اختبار الإختراق يفضلونها لأنها سهلة التعلم ويوجد بها أهم الخصائص الأساسية

- كثرة المكتبات المضمنة في اللغة

الكثير من المكتبات المضمنة في اللغة يتم أستخدامها في تطبيقات أختبار الأختراق وعمليات كشف الثغرات، ايضا بحكم انها مدعومة بشكل كبير من قبل مجتمع المطورين فهذا يسهل عملية اضافة مكتبات جديدة في المجال

- خصائص التحكم بالذاكرة

توفر لغة بايثون اداة تسمى Python memory manager وهي اداة تقوم بالتحكم بعناصر الذاكرة ومسح المتغيرات الغير مستخدمة والعديد من المهام الأخرى، قد يتم إستخدام هذه الخاصية بشكل إيجابي أو سلبي

منهجية بناء اللغة Python Syntax

- طباعة النتائج أو المتغيرات Variables

```
x = 5
y = "John"
print(x)
print(y)
```

- التعليقات Comments

```
#This is a comment
print("Hello, World!")
```

- الجمل الشرطية If... else statements

```
a = 33
b = 200
if b > a:
  print("b is greater than a")
```

- الحلقات التكرارية loops

```
fruits = ["apple", "banana", "cherry"]
for x in fruits:
  print(x)
```

لغة بايثون في مجال نظم التشغيل

Library name	function	description
platform	platform.version()	more detailed system version
	platform.platform()	Get information about the platform
	platform.system()	Linux: Linux Mac: Darwin Windows: Windows
	platform.processor()	a real identifier for the processor
	platform.release()	operating system release number
	platform.python_version()	Get version of python installed on OS
	platform.node()	host name of the machine
	platform.uname()	Combination of some commands
Psutil (process and system utilities)	psutil.virtual_memory().total	Get some data about RAM on the OS
	psutil.disk_partitions() psutil.disk_usage(x) x=partition name	Get all partitions on your OS
	psutil.users()	Get list of users in the OS

مصادر :

https://pypi.org/project/psutil/

https://docs.python.org/3/library/platform.html

لغة بايثون في مجال الشبكات

يمكن لبعض المكتبات في البايثون أن تقوم بعمل اتصالات بين الاجهزة لإرسال أو إستقبال بعض الرسائل والملفات

لغة بايثون في مجال الويب

هي تقنية استخراج البيانات من مواقع الانترانت عن طريق برامج مخصصة وتسمى عادة بـ web scraping أو web crawling

Requests	lxml	Beautiful Soup	Selenium	Scrapy
make HTML requests to the website's server for retrieving the data on its page	HTML, and XML parsing Python library (advanced one)	creates a parse tree for parsing HTML and XML documents	Get the JS (dynamic) data from websites	entire web scraping framework

للإستزادة :

https://www.scrapinghub.com/what-is-web-scraping/

https://www.analyticsvidhya.com/blog/2020/04/5-popular-python-libraries-web-scraping/

شكرا لكم

حساب كلية الحاسبات

@FCITKAU

حساب مقدم اللقاء

@iiKatheri