Concepteur Intégrateur Cybersécurité

SECDEV 2 - Sécurité des applicatifs Python

Nicolas Palpacuer

https://github.com/NickPPC/python_training

FizzBuzz

Afficher les nombres de 1 à 100, mais

Multiple de 3 : Fizz

Multiple de 5: Buzz

Multiple de 3 et de 5: FizzBuzz

Tables de multiplication au résultats impairs

Afficher les table de multiplication dont les résultats sont impairs:

Ex:

1 x 1 = 1

1 x 3 = 3

List overlap – nombres communs

Trouver les nombres communs aux deux listes et les afficher

Reference vs Copy

```
>>> def foo(bar=[]):        # bar is optional and defaults to [] if not specified
...     bar.append("baz")
...     return bar


>>  foo()
```

Exceptions

```
>>> try:
...     l = ["a", "b"]
...     int(l[2])
... except ValueError, IndexError:
...     pass
```

Exceptions

```
>>> try:
...     l = ["a", "b"]
...     int(l[2])
... except ValueError, IndexError:
...     pass
...
Traceback (most recent call last):
  File "<stdin>", line 3, in <module>
IndexError: list index out of range
```

Exceptions

```
>>> try:
...     l = ["a", "b"]
...     int(l[2])
... except (ValueError, IndexError):  # To catch both exceptions, right?
...     pass
```

Scope

```
>>> x = 10
>>> def foo():
...     x += 1
...     print x
...
>>> foo()
```

Règle #1

Règle #1

Un code propre a moins de bugs et de failles de sécurité

“Any fool can write code that a computer can understand. Good programmers write code that humans can understand.” – Martin Fowler

Fichiers de code

https://github.com/NickPPC/python_training

Buffer overflow

Buffer overflow

Buffer overflow

Heartbleed

Buffer overflow

Heartbleed - SSL

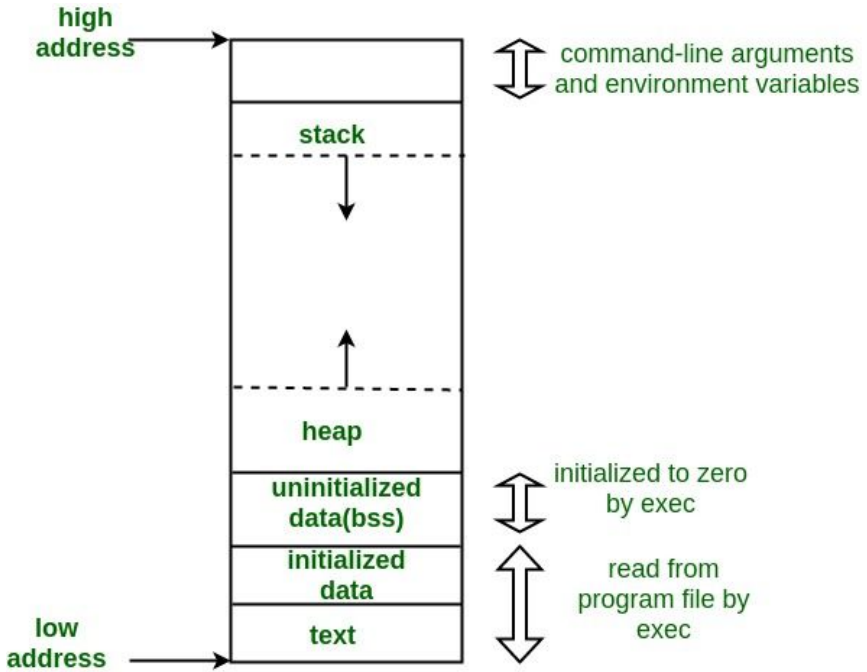
http://heartbleed.com/

Buffer overflow

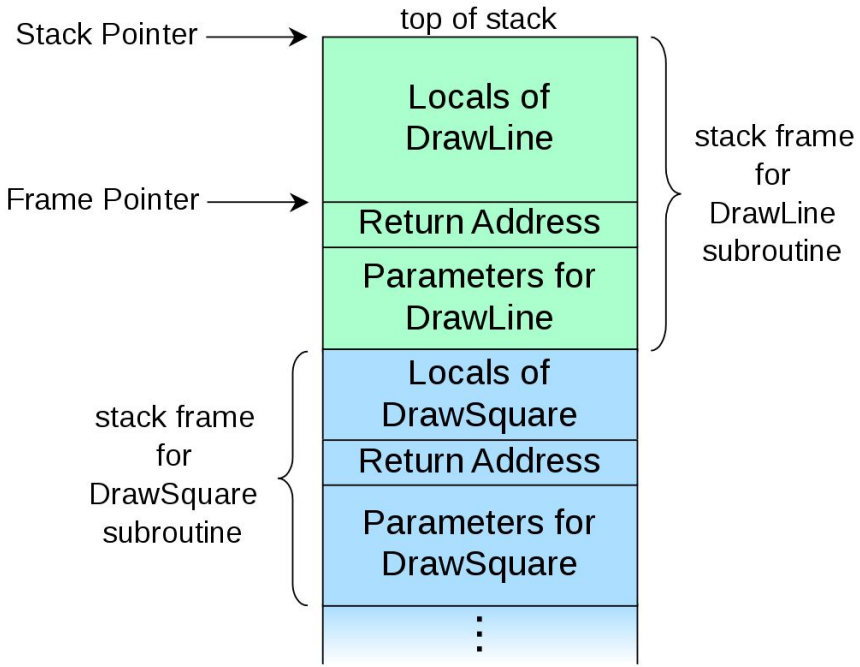
“En informatique, un **dépassement de tampon** ou **débordement de tampon** (en anglais, ***buffer overflow***) est un bug par lequel un processus, lors de *l'écriture* dans un tampon, écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus” - *Wikipedia*

Buffer overflow -

Heap vs Stack



Buffer overflow – Stack



Buffer overflow – Buffer

Buffer overflow – Stack attack

- Variables locales
- Return address
- Variables autres procedures

Buffer overflow – Heap attack

Corruption de données

Buffer overflow – ASLR

Address Space Layout Randomization

Buffer overflow – SSP

Stack-Smashing Protector

Canaries

Règle #2

Ne jamais faire confiance aux utilisateurs

*“*L'expérience prouve que celui qui n'a jamais confiance en personne ne sera jamais déçu.*”* – *Leonard de Vinci*

Multithreading - Synchronisation

Multithreading - Synchronisation

Locks

Multithreading - Synchronisation

Semaphores

Règle #3

La sécurité du système est aussi bonne que votre maillon le plus faible

“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted; none of these measures address the weakest link in the security chain.” – Kevin Mitnick, “The World’s Most Famous Hacker”

Règle #3 bis

Le maillon faible est souvent humain

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

– Bruce Schneier

Bonnes pratiques

Bonnes pratiques

OWASP checklist

Ressources

Cours gratuits de Python sur Openclassroom:

https://openclassrooms.com/fr/courses/235344-apprenez-a-programmer-en-python

Cours gratuits dans le domaine de l'IT et de la cybersécurité (en anglais):

https://www.cybrary.it/

Il existe aussi des vidéos sur Youtube pour tous les niveaux de Python