Codio Activity - Exploring Python Tools and Features

Part I

In this example, you will compile and run a program in C using the **Codio workspace** provided (Buffer Overflow in C). The program is already provided as bufoverflow.c - a simple program that creates a buffer and then asks you for a name, and prints it back out to the screen.

This is the code in bufoverflow.c (also available in the Codio workspace):

```
#include <stdio.h>
int main(int argc, char **argv)
{
	char buf[8]; // buffer for eight characters
	printf("enter name:");
	gets(buf); // read from stdio (sensitive function!)
	printf("%s\n", buf); // print out data stored in buf
	return 0; // 0 as return value
{
```

Now compile and run the code. To test it, enter your first name (or at least the first 8 characters of it) you should get the output which is just your name repeated back to you.

Run the code a second time (from the command window this can be achieved by entering ./bufoverflow on the command line). This time, enter a string of 10 or more characters.

- What happens?

```
ERROR!
gcc /tmp/TLVpL6iYdi.c -lm
/tmp/TLVpL6iYdi.c: In function 'main':
/tmp/TLVpL6iYdi.c:6:1: warning: implicit declaration of function 'gets'; did you
    mean 'fgets'? [-Wimplicit-function-declaration]
    6 | gets(buf); // read from stdio (sensitive function!)
      | ^~~~
      | fgets
/tmp/TLVpL6iYdi.c:9:1: error: expected declaration or statement at end of input
    9 | {
      | ^
/tmp/TLVpL6iYdi.c:9:1: error: expected declaration or statement at end of input
```

- What does the output message mean?

The code should let me enter my name, however, all I was able to get was an error message.

J. Irvine Secure Software Development

Part II

Now carry out a comparison of this code with one in Python (Buffer Overflow in Python), following these instructions:

In the Codio workspace, you will be using the file called Overflow.py:

```
buffer=[None]*10
for i in range (0,11):
    buffer[i]=7
print(buffer)
```

Run your code using: Python overflow.py (or use the codio rocket icon)

- What is the result?

Result
There was an error when run.

#File Overflow.py", line 10, in <module>in
buffer[i]=7
IndexError: list assignment index out of range

The error was caused by the index being out of range. This sis due to the buffer being 10 and the range being 0, 11 instead of 0, 10.

I changed the code in Overflow2.

```
buffer=[None]*10
for i in range (0,10):
    buffer[i]=7
print(buffer)
```

The output produced is below i.e. the number 7 outputted 10 times.

```
[7, 7, 7, 7, 7, 7, 7, 7, 7, 7]
```

J. Irvine Secure Software Development

Read about Pylint at http://pylint.pycqa.org/en/latest/tutorial.html

- Install pylint using the following commands:

  pip install pylint (in the command shell/ interpreter)

- Run pylint on one of your files and evaluate the output:

  pylint your_file

- (Make sure you are in the directory where your file is located before running Pylint)

- What is the result? Does this tell you how to fix the error above?

Pylint result on Overflow.

```
D:\Buffer Overflow>pylint Overflow.py
************* Module Overflow
Overflow.py:10:0: C0303: Trailing whitespace (trailing-whitespace)
Overflow.py:1:0: C0114: Missing module docstring (missing-module-docstring)
Overflow.py:1:0: C0103: Module name "Overflow" doesn't conform to snake_case naming style (invalid-name)

-----------------------------------
Your code has been rated at 2.50/10
```

Pylint result on Overflow2.

```
D:\Buffer Overflow>pylint Overflow2.py
************* Module Overflow2
Overflow2.py:5:14: C0303: Trailing whitespace (trailing-whitespace)
Overflow2.py:6:14: C0303: Trailing whitespace (trailing-whitespace)
Overflow2.py:8:16: C0303: Trailing whitespace (trailing-whitespace)
Overflow2.py:10:22: C0303: Trailing whitespace (trailing-whitespace)
Overflow2.py:12:15: C0303: Trailing whitespace (trailing-whitespace)
Overflow2.py:14:13: C0303: Trailing whitespace (trailing-whitespace)
Overflow2.py:1:0: C0114: Missing module docstring (missing-module-docstring)
Overflow2.py:1:0: C0103: Module name "Overflow2" doesn't conform to snake_case naming style (invalid-name)

-----------------------------------
Your code has been rated at 0.00/10
```

I took out the comments and any spaces and named the file Overflow 3.

Pylint result on Overflow3.

```
Your code has been rated at 0.00/10


D:\Buffer Overflow>pylint Overflow3.py
************* Module Overflow3
Overflow3.py:1:0: C0114: Missing module docstring (missing-module-docstring)
Overflow3.py:1:0: C0103: Module name "Overflow3" doesn't conform to snake_case naming style (invalid-name)

-------------------------------------------------------------------
Your code has been rated at 5.00/10 (previous run: 0.00/10, +5.00)
```

I have found Pylint can be useful at identifying errors and it also outlines whether you code is styled correctly and enforce standards. Although this is useful it was also frustrating and the suggestions it gave were good, however I had difficulty implementing them even in simple code.