

TP N°2: SEGURIDAD INFORMÁTICA



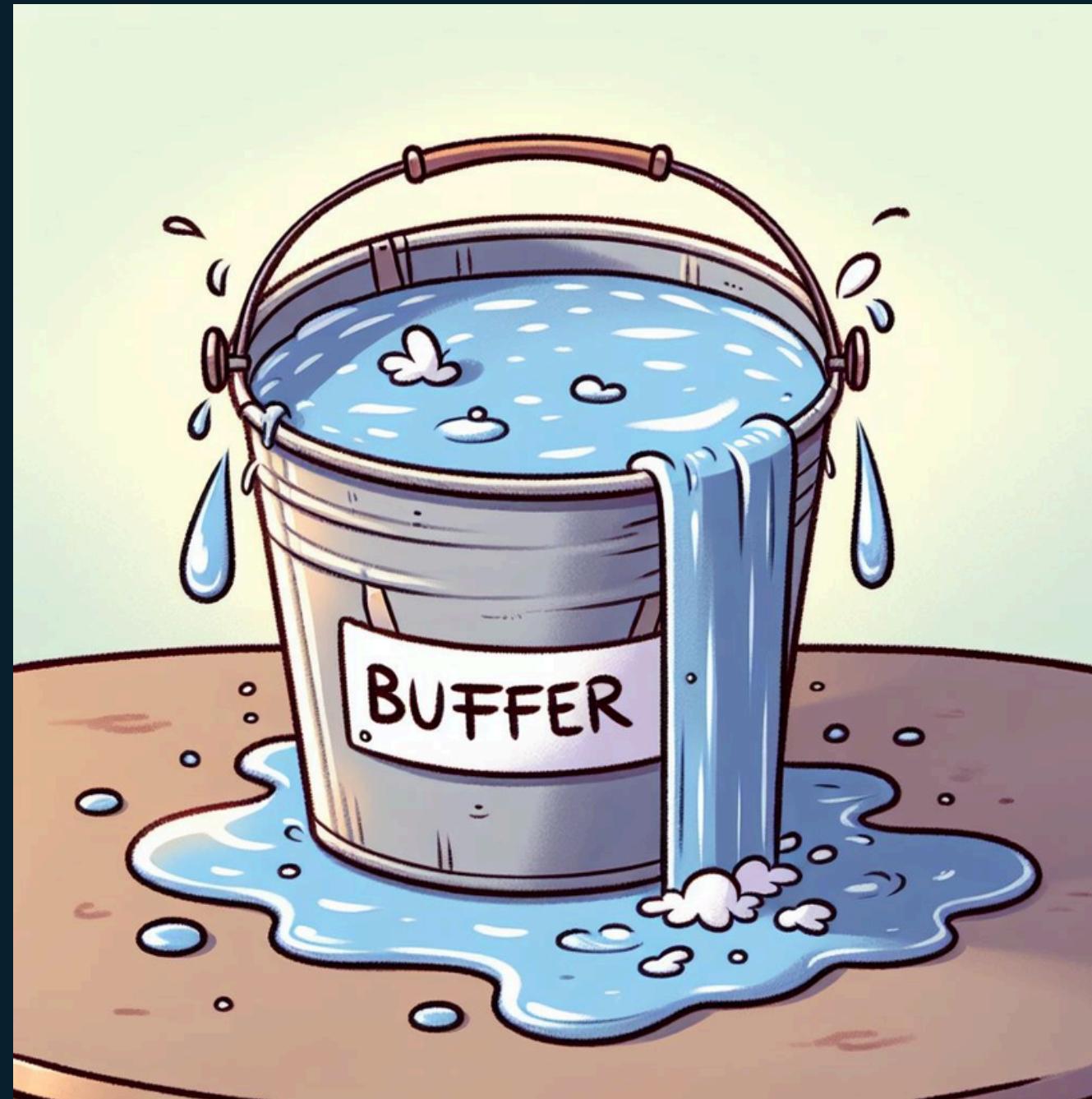
GRUPO 1

CHRISTIAN CHAMIZO
DARÍO ESPÍNOLA
MARCELO OVIEDO
MARTÍN ZAVALLA

TEMA ELEGIDO:

**VULNERABILIDADES
DE DESBORDAMIENTO**

¿ QUÉ ES EL BUFFER OVERFLOW ?



HERRAMIENTAS DE FUZZING: RADAMSA

- **¿QUÉ ES EL FUZZING?**

Es una técnica que consiste en proporcionar entradas aleatorias a un programa con el fin de descubrir fallos de seguridad

- **RADAMSA**

Es el fuzzer que usaremos en el TP

INSTALACIÓN DE RADAMSA

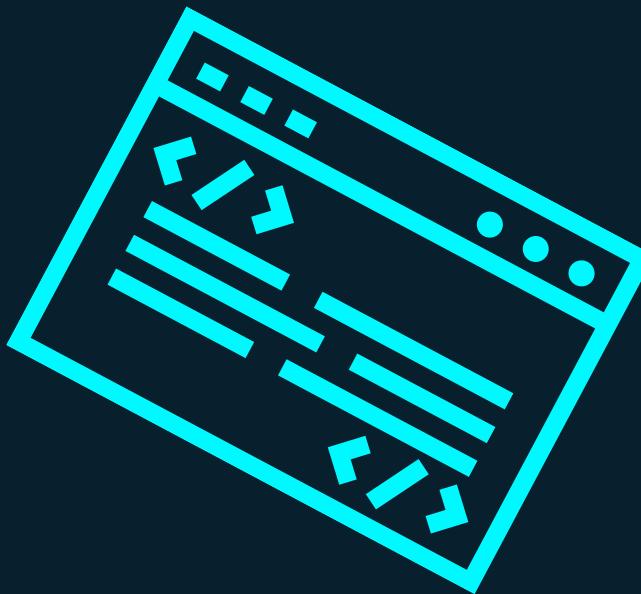


git clone <https://gitlab.com/akihe/radamsa.git>

cd radamsa

make

sudo make install



PRIMERAS PRUEBAS DE RADAMSA

- Vemos la alteraciones que realiza Radamsa sobre el mismo input

```
martin@DESKTOP-1DD67VP:~/CIBERSEC$ echo "hola" | radamsa  
//v8/  
ho@la  
martin@DESKTOP-1DD67VP:~/CIBERSEC$ echo "hola" | radamsa  
$18#888;\u0000hh1hhh1lahlolala  
martin@DESKTOP-1DD67VP:~/CIBERSEC$ echo "hola" | radamsa  
@hole  
martin@DESKTOP-1DD67VP:~/CIBERSEC$ echo "hola" | radamsa  
Ba
```

ANALISIS DEL PROGRAMA INSERT

```
1 #include <stdio.h>
2 #include <string.h>
3 #include <stdlib.h>
4
5 void insert_substring(char*, char*, int);
6 char* substring(char*, int, int);
7
8 int main()
9 {
10     char text[100], substring[100];
11     int position;
12
13     printf("Enter some text\n");
14     gets(text);
15
16     printf("Enter the string to insert\n");
17     gets(substring);
18
19     printf("Enter the position to insert\n");
20     scanf("%d", &position);
21
22     insert_substring(text, substring, position);
23
24     printf("%s\n", text);
25
26     return 0;
27 }
28
29 > void insert_substring(char *a, char *b, int position) ...
46
47 > char *substring(char *string, int position, int length) |...
64
```

ADVERTENCIAS

```
dario@lenovo:~/Documents/S0R2$ gcc insert.c -o insert
insert.c: In function 'main':
insert.c:14:4: warning: implicit declaration of function 'gets'; did you mean 'fgets'? [-Wimplicit-function-declaration]
  14 |     gets(text);
      |     ^
      |     fgets
/usr/bin/ld: /tmp/ccpFfmft.o: in function `main':
insert.c:(.text+0x3d): warning: the `gets' function is dangerous and should not be used.
```

EJECUCION DEL PROGRAMA INSERT

```
dario@lenovo:~/Documents/S0R2/sor2_projects/SEGURIDAD INFORMATICA$ ./insert
Enter some text
ejemplo.
Enter the string to insert
Esto es un
Enter the position to insert
1
Esto es un ejemplo.
```

CREACION DEL ARCHIVO INPUT

- El objetivo de este archivo será facilitar la automatización de testing del programa.
- crearemos un archivo “input.txt” el cual contendrá los datos que solicitaba insert.c cada uno en una línea diferente.

PASOS PARA LA EJECUCION DEL PROGRAMA/ARCHIVO

- El programa solicita al usuario dos cadenas de texto.
- Luego, pide una posición numérica de carácter dentro del primer texto.
- Finalmente, inserta la segunda cadena en esa posición del primer texto para generar una nueva salida.

- Visualizamos que Se toma el contenido de input.txt, se modifica con Radamsa y se pasa al programa, De esta forma logramos a partir de un input aleatorizar los inputs del programa.

```
martin@DESKTOP-1DD67VP:~/CIBERSEC$ touch input.txt
martin@DESKTOP-1DD67VP:~/CIBERSEC$ nano input.txt
martin@DESKTOP-1DD67VP:~/CIBERSEC$ cat input.txt
taza
kilometraje
3
martin@DESKTOP-1DD67VP:~/CIBERSEC$ cat input.txt | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
takilometrajeza
martin@DESKTOP-1DD67VP:~/CIBERSEC$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
ta{a
martin@DESKTOP-1DD67VP:~/CIBERSEC$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
taza
martin@DESKTOP-1DD67VP:~/CIBERSEC$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
tk@ilometraje@a
```

```
dario@lenovo:~/Documents$ cat input.txt | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
Ejemplo de entrada
dario@lenovo:~/Documents$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
Segmentation fault (core dumped)
dario@lenovo:~/Documents$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
dario@lenovo:~/Documents$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
dario@lenovo:~/Documents$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
dario@lenovo:~/Documents$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
Segmentation fault (core dumped)
dario@lenovo:~/Documents$ cat input.txt | radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
de entrada
```

- Otro ejemplo de ejecución de un programa con entradas de texto

```
alumno@alumno-virtualbox:~/Descargas$ cat input.txt
remo
playa
arena
alumno@alumno-virtualbox:~/Descargas$ cat input.txt |radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
playam
alumno@alumno-virtualbox:~/Descargas$ cat input.txt |radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
plava
```

RESULTADO FINAL

- Luego de ejecutar varias veces el archivo, nos encontramos con un error denominado “Stack smashing”

```
alumno@alumno-virtualbox:~/Descargas$ cat input.txt |radamsa |./insert
Enter some text
Enter the string to insert
Enter the position to insert
a♦♦♦pl
*** stack smashing detected ***: terminated
Abortado (`core' generado)
```

SCRIPT FIND ERROR



```
#!/bin/bash
count=0
while true; do
    cat input.txt | radamsa | tee last_input.txt | ./insert
    test $? -gt 127 && break
    count=$((count + 1)) # Incrementamos el contador
    if [ "$count" -ge 100 ]; then
        echo "Se Alcanzó el límite de 100 iteraciones."
        break
    fi
done
```

ERRORES ENCONTRADOS

- Segmentation Fault

```
marce998@marce-VM:~/Documentos/sor2/S0yR-2-Projects/SEGURIDAD INFORMATICA$ sh findError.sh
Enter some text
Enter the string to insert
Enter the position to insert
kt
lometraje
Enter some text
Enter the string to insert
Enter the position to insert
tak:ilometrajeza
Enter some text
Enter the string to insert
Enter the position to insert
Segmentation fault (core dumped)
```



**FROM ERROR TO SOLUTION
FIXING THE 'SEGMENTATION FAULT' IN LINUX**

ERRORES ENCONTRADOS

- Stack smashing

```
alumno@alumno-virtualbox:~/Descargas$ cat input.txt |radamsa | ./insert
Enter some text
Enter the string to insert
Enter the position to insert
a♦♦opl
*** stack smashing detected ***: terminated
Abortado (`core' generado)
```



**GRACIAS POR
SU ATENCIÓN!!!**

