

Práctica 1

Vulnerabilidades de Seguridad · MISTIC

Apartado 1

El recuadro verde indica la cantidad transferida en ambos casos

1. En block-ID11

```
pablo-riutort@SMACH-Opis:~/UOC/Vulnerabilidades/Pract1/ACMEBlockchain $ xxd block-ID11
00000000: 4143 4d45 0000 0000 4133 3831 3233 3435  ACME....A3812345
00000010: 4243 3031 3132 4444 8c00 0000 0100 0000  BC0112DD.....
00000020: 3132 4242 4137 3738 3233 3435 4330 4430  12BBA7782345C0D0
00000030: d007 0000 0000 0000 0000 0000 0000 0000  .....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000050: 0000 0000 0000 0000 0000 0000 4443 4442  .....DCDB
00000060: 3737 3837 4343 4141 3132 3231 c104 0000  7787CCAA1221....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000  .....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  .....
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000  .....
```

2. En block-ID11.out

```
pablo-riutort@SMACH-Opis:~/UOC/Vulnerabilidades/Pract1/ACMEBlockchain $ xxd block-ID11.out
00000000: 4143 4d45 0000 0000 4133 3831 3233 3435  ACME....A3812345
00000010: 4243 3031 3132 4444 8c00 0000 0200 0000  BC0112DD.....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000040: 0000 0000 0000 0000 4443 4442 3737 3837  .....DCDB7787
00000050: 4343 4141 3132 3231 c104 0000 3132 4242  CCAA1221....12BB
00000060: 4137 3738 3233 3435 4330 4430 d007 0000  A7782345C0D0....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000  .....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  .....
```

Apartado 2

Platform is x86_64-linux						
Variable				Memory region	Memory address	
type	name	line	size	stack/heap/global/text	absolute	relative
char*	inputFile	25	32 B	Stack	0x7fffffffdd610	0x00
char*	outputFile	26	32 B	Stack	0x7fffffffdd630	-0x32
Struct	header	38	32 B	Stack	0x7fffffffdd560	-0xB0
Struct	transaction	45	20 B	Stack	0x7fffffffdd540	-0xD0
Struct	block	54	140 B	Stack	0x7fffffffdd580	-0x90

Apartado 3

Account sender	12BBA778
Account receiver	2345C0D0
transaction	2000

Account sender	12BBA778
Account receiver	FFFFFFFF
transaction	2000

Apartado 4

b) Abriendo el fichero de entrada con un editor de texto localizamos la cuenta de destino

[illegible]

y ponemos la cuenta deseada

```
1 ACME^@^@^@A3812345BC0112DD<8c>^@^@^@A^@^@^@12BBA7782345C0D0D  
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
```

Finalmente, vemos que la cuenta destino sera la que sustituya a 2345c0d0, en este caso FFFFFFFF

```
pablo-riutort@SMACH-Opis:~/UOC/Vulnerabilidades/Pract1/ACMEBlockchain $ ./acme block-ID12 block-ID12.out
```

```
[BLOCKCHAIN]
```

```
[*] Software licensed to USER=pablo-riutort.  
[*] The account 12BBA778 has send 2000 coins to account FFFFFFFF
```

c) Para mejorar la seguridad de esta aplicación, se podría pedir al usuario una confirmación de la transacción a la cuenta destino donde verá que, efectivamente, ha sido interceptada y alterada la cuenta de destino