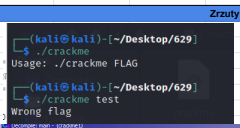
Autor:	f0rizen
Tytuł:	find a real key
Język:	C/C++
Platforma:	Unix/linux
Trudność:	2.2
Jakość:	4.6
Arch:	x86-64
Link:	https://crackmes.one/crackme/629e1e5833c5d4251e72375f
Opis:	Find a real key and recover a flag
Plik:	https://crackmes.one/static/crackme/629e1e5833c5d4251e72375f.zip

Krok	Rozwiązanie	Zrzuty Ekranu
1	Sprawdzenie jak działa plik .exe Działanie polega na flagi jako argumenty. Zwraca czy wartość jest poprawna czy nie.	
2	Odnalezienie głównej funkcji w programie za pomocą Symbol Tree. Pozmieniałem parę nazw żeby program był bardziej czytelny. Takich jak: parametry funkcji main iteratory inputy Efekty widać na zrzucie ekranu po prawej stronie	 
3	Z dłuższej analizy widać że na bazie podanej naszej flagi i wartości **"sup3r_s3cr3t_k3y_1337"** tworzona jest **tablica** z wartosciami i nastepnie **XOR** tej tablicy z naszym podanym wejsciem jest porównywany z **tablica_intów** Czyli musimy sobie ten proces odwrócić Zaczniemy od pierwszego **byte'u** **?** - reprezentuje nieznany dla nas znak który da dobre wyjsce **s ^ ? = 0x37** **0x73 ^ ? = 0x37** zamieniając to na binarke otrzymamy 01110011 s **XOR** xxxxxxxx ? 00110111 0x37 i teraz możemy odwrócić operację żeby poznac wartość **?** 01110011 s **XOR** 01000100 ? 00110111 0x37 dodatkowo można zauważyć że jeżeli teraz użyjemy **s XOR 0x37** to otrzymamy wartość **?** 110111 1110011 1000100	
4	Teraz możemy odwrócić proces Polecam stworzyć program w C++, żeby **XOR** za nas Otrzymalismy flage