

Merhabalar,

Cybercamp19 kamp son ctf yarışmasında çıkan tersine mühendislik **Rev-150** sorusu için yapmış olduğum çözüm şu şekilde;

Rev-150.exe

Çalıştırılabilir dosyamızı yürüttüğümüzde bize sorduğu soruya herhangi bir cevapla karşılık verince BAD! Tuzağına düşüyoruz.



(İlk writeup'a bakınca kafanızda birşeyler canlanmış olması lazım)

Yine ilk iş olarak GOOD vs BAD! Mesajlarını bularak tersten gitmeyi deneyelim.

Address	Disassembly	String
004012A5	mov dword ptr ss:[esp],rev150.403000	"Good!"
004012B3	mov dword ptr ss:[esp],rev150.403006	"Bad!"
004012EB	mov dword ptr ss:[esp],rev150.403008	"Enter 4 digit pin-code: "
004012FE	mov dword ptr ss:[esp],rev150.403024	"%d"

Bad! Uyarısının kontrol noktasına bakmayı deneyelim. Eğer bizi çok zorlamak istemiyorlarsa, birkaç normal karşılaştırma mantığını çözerek soruyu çözebiliriz diye düşünüyorum. Bad! Mesajının referans olarak kullanıldığı kod akışı ve fonksiyonlarına gelince:

00401290	\$ 55	PUSH EBP	
00401291	. 89E5	MOV EBP,ESP	
00401293	. 83EC 08	SUB ESP,8	
00401296	. 8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
00401299	. 35 39050000	XOR EAX,539	
0040129E	. 3D 4B140000	CMP EAX,144B	
004012A3	. 75 0E	JNZ SHORT rev150.004012B3	
004012A5	. C70424 00304000	MOV DWORD PTR SS:[ESP],rev150.00403000	ASCII "Good!"
004012AC	. E8 BF050000	CALL <JMP.&msvcrt.puts>	puts
004012B1	. EB 0C	JMP SHORT rev150.004012BF	
004012B3	> C70424 06304000	MOV DWORD PTR SS:[ESP],rev150.00403006	ASCII "Bad!"
004012BA	. E8 B1050000	CALL <JMP.&msvcrt.puts>	puts
004012BF	> C9	LEAVE	
004012C0	. C3	RETN	

Sizde dikkatinizi Xor eax,539 çekmiş olabilir. Ve bizi tek Bad! Tuzağına düşüren kontrol Xor işlemi sonucunun 144B'ye eşit olmaması durumu. Güzel o zaman:

$EAX \oplus 539 = 144B$ ise $EAX = 0539 \oplus 144B$ olarak hesaplarsak :=) Bingo

Decimal olarak çevirmeyi unutmayın ! **4466** doğru pincod'umuz olacak