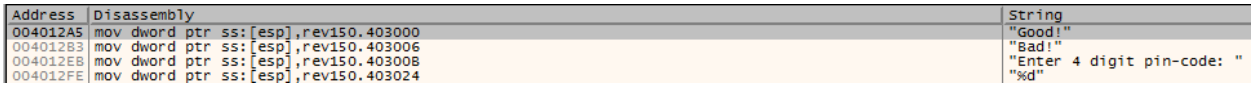
Merhabalar,

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

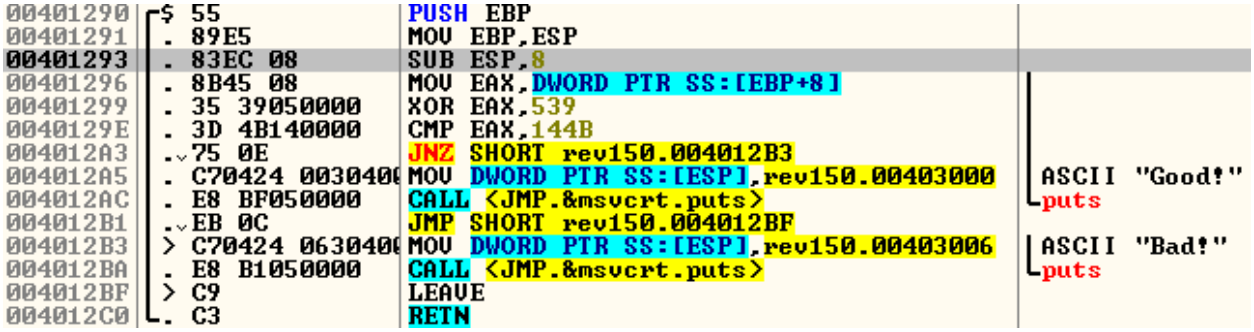
Rev-150.exe
Çalıştıralabilir dosyamızı yürüttüğümüzde bize sorduğu soruya herhangi bir cevapla karşılık verince BAD! Tuzağına düşüyoruz.

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

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



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:



Sizinde 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 ^ 539 = 144B ise > EAX = 0539 ^ 144B olarak hesaplarsak :=) Bingo

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