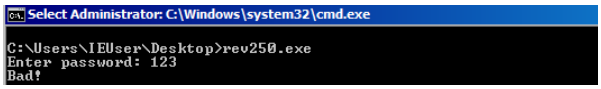
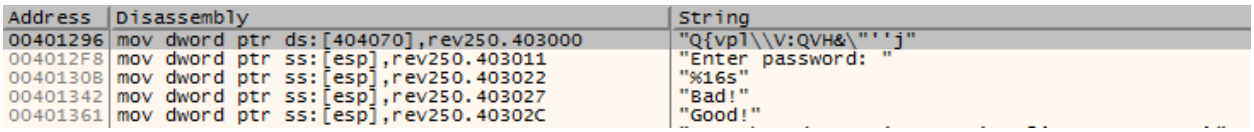
Merhabalar,

Cybercamp19 kamp son ctf yarışmasında çıkan tersine mühendislik **Rev-250** sorusu için yapmış olduğum çözüm şu şekilde;

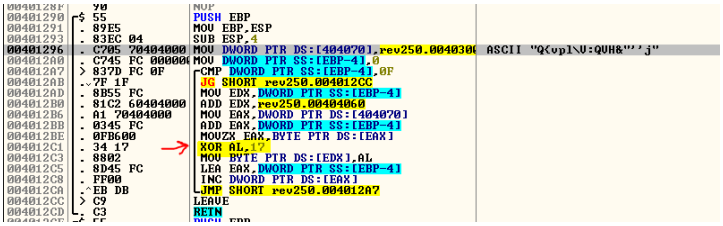
Yürütülebilir dosyamızı çalıştırdığımızda bize bir parola sormakta. Bunun diğer iki exe dosyasına göre biraz daha karmaşık olması yönünde beklentimiz varken incelemeye başlayalım;



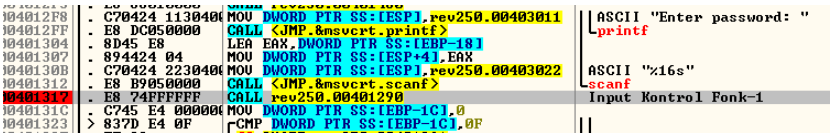
Aynı şekilde string kontrolü için göz attığımızda:



İlk baştaki ilginç char dizisi dikkatimiz çekti sanırım. Şöyle bir çağrıldığı fonksiyona göz atalım :

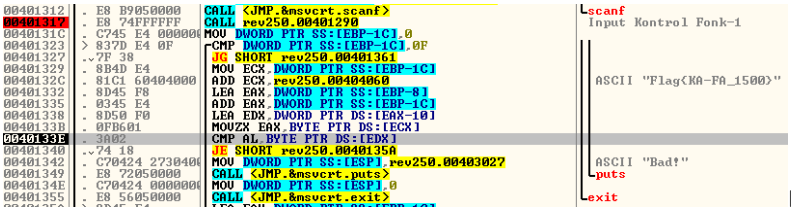


Eğer bu fonksiyona stringlerden referans aracılığıyla erişemeseydik şu programın ilk kontrollerindeki akışı takip ederek şunu yapabilirdik:



Password girildikten hemen sonra bizi götürdüğü “Input Kontrol Fonk-1” alt prosedürüne giderek üstteki ilginç Stringin kullanıldığı fonksiyonu bulabilirdik.

Çok uzatmadan programın bizden istediği şeye bakalım; İlginç stringi uzunluğu (0 ‘dan 0xf’e = 16 karakter) süren bir döngü içerisinde 0x17 hex değeriyle Xor işlemine tutuluyor Bu işlem bittikten sonra. Fonksiyonumuz ;



Bizim girmiş olduğumuz parola değeriyle Xor işleminden türeyen 16 karakterli Flag{.. char dizisiyle “cmp” işlemine tutarak sonuçları karşılaştırıyor ve Bad-Good noktalarına sonucun doğruluğuna göre yönlendirmekte.

Resimdende görmüş olduğunuz gibi **Flag{KA-FA_1500}** değerini bu şekilde bulabilirsiniz.

Diğer yöntem olarakta **Q{vpl\V:QVH&"'**'j değerini Xor bruteforce scriptleriyle FLAG değerini veren Xor değerini yakalayıp çözüme gidebilirdiniz. Bknz: OzanÇetin XOR BruteForce Script : https://goo.gl/Tq33YR