

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;

```
C:\Users\IEUser\Desktop>rev250.exe
Enter password: 123
Bad!
```

Aynı şekilde string kontrolü için göz attığımızda:

Address	Disassembly	String
00401296	mov dword ptr ds:[404070],rev250.403000	"Q{vpI\\V:QVH&\"'"j"
004012F8	mov dword ptr ss:[esp],rev250.403011	"Enter password: "
00401308	mov dword ptr ss:[esp],rev250.403022	"%16s"
00401342	mov dword ptr ss:[esp],rev250.403027	"Bad!"
00401361	mov dword ptr ss:[esp],rev250.40302C	"Good!"

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

```
00401296 70 MOV     EDI, rev250.00403000
00401297 55 PUSH    EBP
00401298 89 E5 MOV     EBP, ESP
00401299 8B EC SUB     ESP, 4
0040129A C7 05 70404000 MOV     DWORD PTR DS:[404070], rev250.00403000
0040129B C7 45 FC 000000 MOV     DWORD PTR SS:[EBP-4], 0
0040129C 83 7D FC CMP     DWORD PTR SS:[EBP-4], 0F
0040129D 7F 1F JG     SHORT rev250.004012C0
0040129E 8B 55 FC MOV     EDI, rev250.00404060
0040129F 81 C2 60404000 ADD     EDI, rev250.00404060
004012A0 A1 70404000 MOV     EAX, DWORD PTR DS:[404070]
004012A1 03 45 FC ADD     EAX, DWORD PTR SS:[EBP-4]
004012A2 0F B6 00 MOVZX  EAX, BYTE PTR DS:[EAX]
004012A3 34 17 XOR     AL, 17
004012A4 8B 02 MOV     BYTE PTR DS:[EDI], AL
004012A5 8D 45 FC LEA     EAX, DWORD PTR SS:[EBP-4]
004012A6 FF B0 INC     DWORD PTR DS:[EAX]
004012A7 EB DB JMP     SHORT rev250.004012A7
004012A8 C9 LEAVE
004012A9 C3 RETN
```

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

```
004012F8 C7 05 70404000 MOV     DWORD PTR DS:[404070], rev250.00403000
004012F9 E8 DC050000 CALL    <JMP.&msvcrt.printf>
00401304 8B 45 E8 MOV     EAX, DWORD PTR SS:[EBP-18]
00401307 89 4424 04 MOV     DWORD PTR SS:[ESP+4], EAX
0040130B C7 05 70404000 MOV     DWORD PTR DS:[404070], rev250.00403000
00401312 E8 B9050000 CALL    <JMP.&msvcrt scanf>
00401317 E8 74FFFFF0 CALL    rev250.00401290
0040131C C7 45 E4 000000 MOV     DWORD PTR SS:[EBP-1C], 0
00401323 83 7D E4 CMP     DWORD PTR SS:[EBP-1C], 0F
00401327 7F 38 JG     SHORT rev250.00401361
00401329 8B 4D E4 MOV     ECX, DWORD PTR SS:[EBP-1C]
0040132C 81 C1 60404000 ADD     ECX, rev250.00404060
0040132E 8D 45 F8 LEA     EAX, DWORD PTR SS:[EBP-8]
00401335 03 45 E4 ADD     EAX, DWORD PTR SS:[EBP-1C]
00401338 8D 50 F0 LEA     EDI, DWORD PTR DS:[EAX-10]
0040133B 0F B6 01 MOVZX  EDI, BYTE PTR DS:[EDI]
0040133C 8B 02 MOV     BYTE PTR DS:[EDI]
0040133D 74 18 JE     SHORT rev250.0040135A
00401342 C7 05 70404000 MOV     DWORD PTR DS:[404070], rev250.00403000
00401349 E8 72050000 CALL    <JMP.&msvcrt.puts>
0040134E C7 05 70404000 MOV     DWORD PTR DS:[404070], 0
00401355 E8 56050000 CALL    <JMP.&msvcrt.exit>
```

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; ilginç stringi uzunluğu (0 ‘dan 0xf’e = 16 karakter) süren bir döngü içerisinde 0x17 hex değeriyle Xor işlemine tutuluyor Bu işlem bittikten sonra. Fonksiyonumuz ;

```
00401312 E8 B9050000 CALL    <JMP.&msvcrt scanf>
00401317 E8 74FFFFF0 CALL    rev250.00401290
0040131C C7 45 E4 000000 MOV     DWORD PTR SS:[EBP-1C], 0
00401323 83 7D E4 CMP     DWORD PTR SS:[EBP-1C], 0F
00401327 7F 38 JG     SHORT rev250.00401361
00401329 8B 4D E4 MOV     ECX, DWORD PTR SS:[EBP-1C]
0040132C 81 C1 60404000 ADD     ECX, rev250.00404060
0040132E 8D 45 F8 LEA     EAX, DWORD PTR SS:[EBP-8]
00401335 03 45 E4 ADD     EAX, DWORD PTR SS:[EBP-1C]
00401338 8D 50 F0 LEA     EDI, DWORD PTR DS:[EAX-10]
0040133B 0F B6 01 MOVZX  EDI, BYTE PTR DS:[EDI]
0040133C 8B 02 MOV     BYTE PTR DS:[EDI]
0040133D 74 18 JE     SHORT rev250.0040135A
00401342 C7 05 70404000 MOV     DWORD PTR DS:[404070], rev250.00403000
00401349 E8 72050000 CALL    <JMP.&msvcrt.puts>
0040134E C7 05 70404000 MOV     DWORD PTR DS:[404070], 0
00401355 E8 56050000 CALL    <JMP.&msvcrt.exit>
```

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.

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

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