


İlk olarak hiçbir şeye bakmadan direk EXE dosyasını çalıştırdığımda şöyle bir ekran geldi:

 C:\Users\aseli\OneDrive\Masaüstü\CTF2019.exe

```
Kullanici Adi :root  
Parola :123456
```

Program bizden bir kullanıcı adı ve bir parola istiyordu. Rasgele değerler girdim fakat hiçbir şey olmadı.

Sonraki adım olarak program IDA'da açtım.

```
IDA View-A Pseudocode-A Hex View-1 Struct
22 v14 = 0;
23 v10 = 1957682669778961411i64;
24 LODWORD(v11) = 756220955;
25 v17 = 0;
26 v16 = 0;
27 *(_QWORD *)Str1 = 4280139i64;
28 v9 = 0;
29 strcpy(v7, "1.2.3.4.5");
30 printf("Kullanici Adi :");
31 scanf("%s", &Str2);
32 printf("Parola :");
33 scanf("%s", &v5);
34 v17 = strcmp(Str1, &Str2);
35 v16 = strcmp(v7, &v5);
36 if ( v17 )
37 {
38     printf("KullaniciAdi veya Parola Hatali");
39 }
40 else if ( v16 )
41 {
42     printf("HATA");
43 }
44 else
45 {
46     puts("KUZEY KIBRIS TURK CUMHURİYETİ KADERINE TERK EDİLEMEZ");
47     File = fopen(".KKTC.txt", "w");
48     if ( File )
49     {
50         v3 = (const char *)encryptDecrypt(&v10);
51         fputs(v3, File);
52         fclose(File);
53     }
54     system("attrib +h .KKTC.txt");
55 }
56 return 0;
57 }
```

Program kullanıcı adı ve parola olarak yalnızca birer değeri kabul ediyor, ardından ekrana “KUZEY KIBRIS TURK CUMHURİYETİ KADERINE TERK EDİLEMEZ” yazıyor, sonrasında programın çalıştığı dizinde bulunan .KKTC.txt dosyasına bir şeyler yazıyor, ardından da system fonksiyonu ile “attrib +h” yaparak dosyayı gizliyordu. Sisteme girmek için kullanılan parola açık bir şekilde duruyordu: “1.2.3.4.5” Kullanıcı adı ise 4280139i64 sayısından gelecekti.

Bu sayıya hexadecimal olarak baktığımda 0x414F4B sayısını elde ettim. Bu değerlerin ASCII karşılığı ise “AOK” idi. Fakat Little endian olarak bakmak gerektiği için kullanıcı adımız “KOA” olacaktı. Programa KOA kullanıcı adı ve 1.2.3.4.5 parolası ile girdiğimizde .KKTC.txt dosyasının içine flag yazılıyordu.



.KKTC.txt - Notepad

File Edit Format View Help

|STMCTF{KKTC}

FLAG: STMCTF{KKTC}