



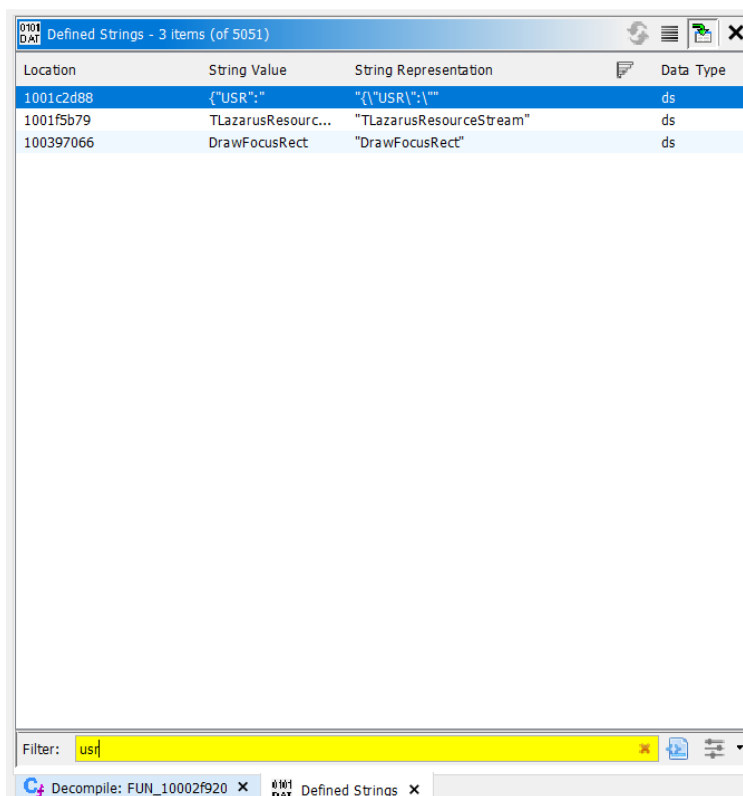
# DOCUMENTACIÓN DE PARCHE

Kevin Jacobo Hernández

Danilo Romualdo Cruz

Anayeli Rodríguez Zepeda

En el Defined String buscamos el string de USB y nos va a redirección de código ensamblador



Vamos a darle click en el FUN\_1002f920

```
      s_{"USR": "_1001c2d88"                                XREF[2]:    FUN_10002f920:100
                                                    FUN_10002f920:100
88 7b 22 55      ds      "{\\\"USR\\\":\\\"\"
53 52 22
3a 22 00
91 00          ??      00h
```

En el apartado de descompile tenemos lo siguiente:

Y vamos a ir la línea 54, vamos a darle click y tenemos al if y nos devolvemos al apartado de ensamblador

```

Decompile: FUN_10002f920 - (phackearme2.exe)
31 FUN_10012d0a0(*(undefined8 *) (param_1 + 0x7e0), &local_48);
32 if (local_48 != 0) {
33     FUN_10012d0a0(*(undefined8 *) (local_18 + 2000), &local_48);
34     if (local_48 != 0) {
35         local_20 = FUN_10000ddf0(&DAT_1001c2ee0, 1);
36         local_70 = "{\\\"USR\\\":\\\"";
37         FUN_10012d0a0(*(undefined8 *) (local_18 + 0x7e0), &local_78);
38         local_68 = local_78;
39         local_60 = "\\\", \\\"PASS\\\":\\\"";
40         FUN_10012d0a0(*(undefined8 *) (local_18 + 2000), &local_80);
41         local_58 = local_80;
42         local_50 = &DAT_1001c2dd8;
43         FUN_100009320(&local_28, &local_70, 4, 0);
44         FUN_10002fb60(local_20, &local_30, "http://45.76.173.114:8080/login_1001c2", 1);
45         if (local_30 == 0) {
46             FUN_10013b080("No se pudo conectar al servidor");
47         }
48         else {
49             FUN_100009720(&local_88, local_30, 0xfde9);
50             uVar1 = FUN_1000652d0(local_88, 1);
51             local_38 = FUN_10000dd10(&DAT_1001d6608, uVar1);
52             local_3c = FUN_100069ce0(local_38, &DAT_1001c2e68, 0);
53             FUN_10013b080(local_30);
54             if (local_3c == 200) {
55                 (**(code **))(**(longlong **)) (local_18 + 0x7f0) + 0x450))
56                 (*(undefined8 *) (local_18 + 0x7f0), 1);
57             }
58         }
59     }
60 }

```

Al darle click vemos que nos redirecciona a esta línea en el ensamblador, por lo que tenemos que cambiar ese JNZ LAB\_10002fad0 por un No operation y por lo que quedaría de este código:

```

cs 00 00 00
10002faad 75 21 JNZ LAB_10002fad0
10002faaf 48 8b 45 f0 MOV RAX,qword ptr [RBP + local_18]
10002fab3 48 8b 88 MOV RCX,qword ptr [RAX + 0x7f0]
f0 07 00 00
10002faba b2 01 MOV DL,offset s_.76.173.114:8080/login_1001c2
10002fab3 48 8b 45 f0 MOV RAX,qword ptr [RBP + local_18]
10002fac0 48 8b 80 MOV RAX,qword ptr [RAX + 0x7f0]
f0 07 00 00
10002fac7 48 8b 00 MOV RAX,qword ptr [RAX]
10002faca ff 90 50 CALL qword ptr [RAX + 0x450]
04 00 00
LAB_10002fad0 XREF[4]:

```

A este:

Por lo que ya no va existir esa comparación en el código gracias al NOP

```

10002faad 48 90      NOP
10002faaf 48 8b 45 f0    MOV     RAX,qword ptr [RBP + local_18]
10002fab3 48 8b 88      MOV     RCX,qword ptr [RAX + 0x7f0]
           f0 07 00 00
10002faba b2 01      MOV     DL,offset s_.76.173.114:8080/login_1001c2
10002fabc 48 8b 45 f0    MOV     RAX,qword ptr [RBP + local_18]
10002fac0 48 8b 80      MOV     RAX,qword ptr [RAX + 0x7f0]
           f0 07 00 00
10002fac7 48 8b 00      MOV     RAX,qword ptr [RAX]
10002faca ff 90 50      CALL    qword ptr [RAX + 0x450]
           04 00 00

```

Resultados del Decompiler:

```

if (local_30 == 0) {
    FUN_10013b080 ("No se pudo conectar al servidor" );
}
else {
    FUN_100009720 (&local_88,local_30,0xfde9);
    uVar1 = FUN_1000652d0 (local_88,1);
    local_38 = FUN_10000dd10 (&DAT_1001d6608,uVar1);
    local_3c = FUN_100069ce0 (local_38,&DAT_1001c2e68,0);
    FUN_10013b080 (local_30);
    (**(code **))(**(longlong **)(local_18 + 0x7f0) + 0x450))
        (*(undefined8 *) (local_18 + 0x7f0),1);
}

```

Al parchearlo de esa manera tenemos que dando igual el usuario y contraseña estaremos entrando al botón de “Presióname”.