



Instituto Tecnológico de San Juan del Río



Tópicos de ciberseguridad

P R E S E N T A:

Abelardo Garduño Fuertes 22590040

Alejandro Pérez Piña 22590068

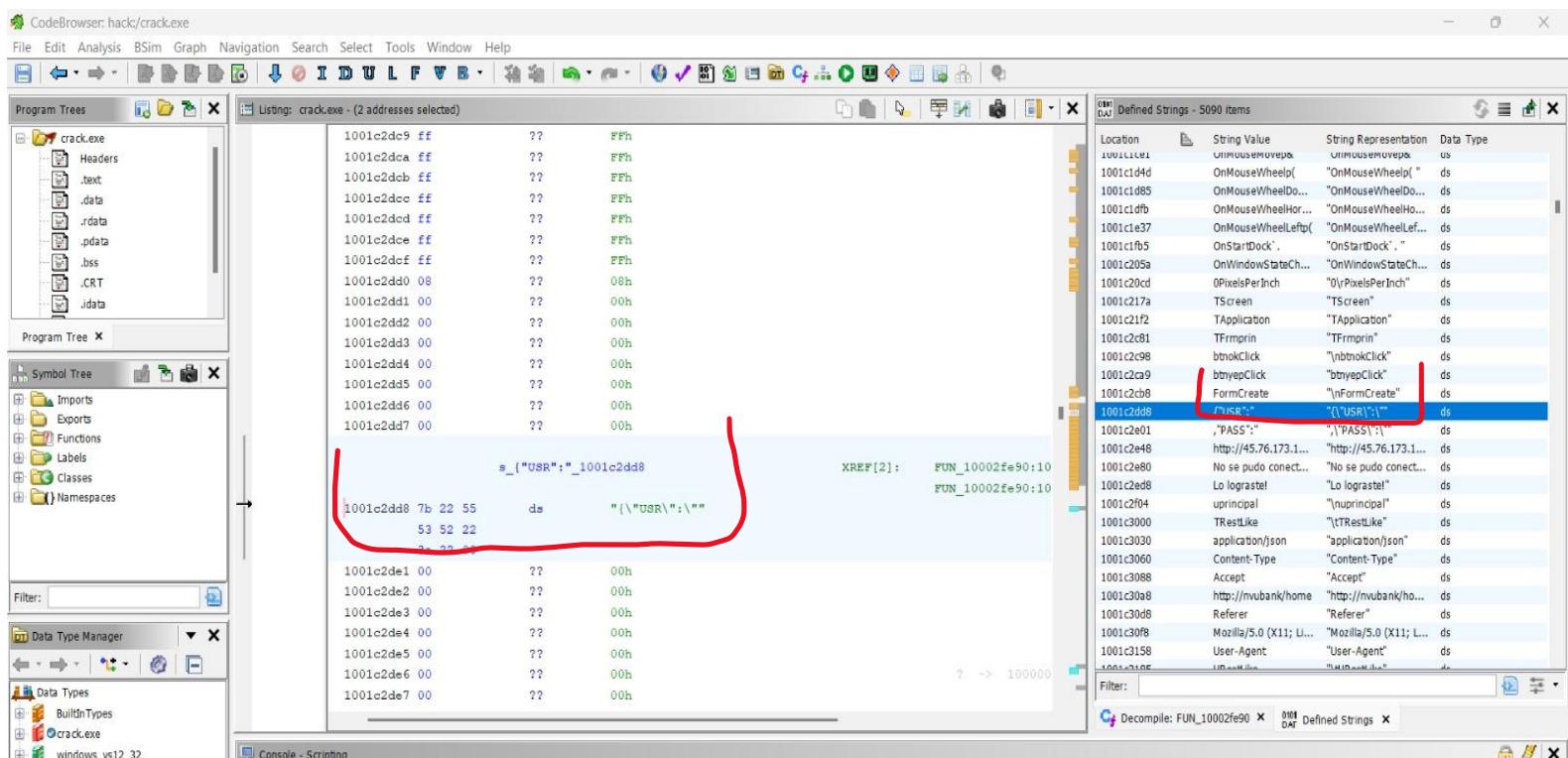
Brandon Ismael Trejo Hernández 22590049

Ingeniería en Sistemas Computacionales

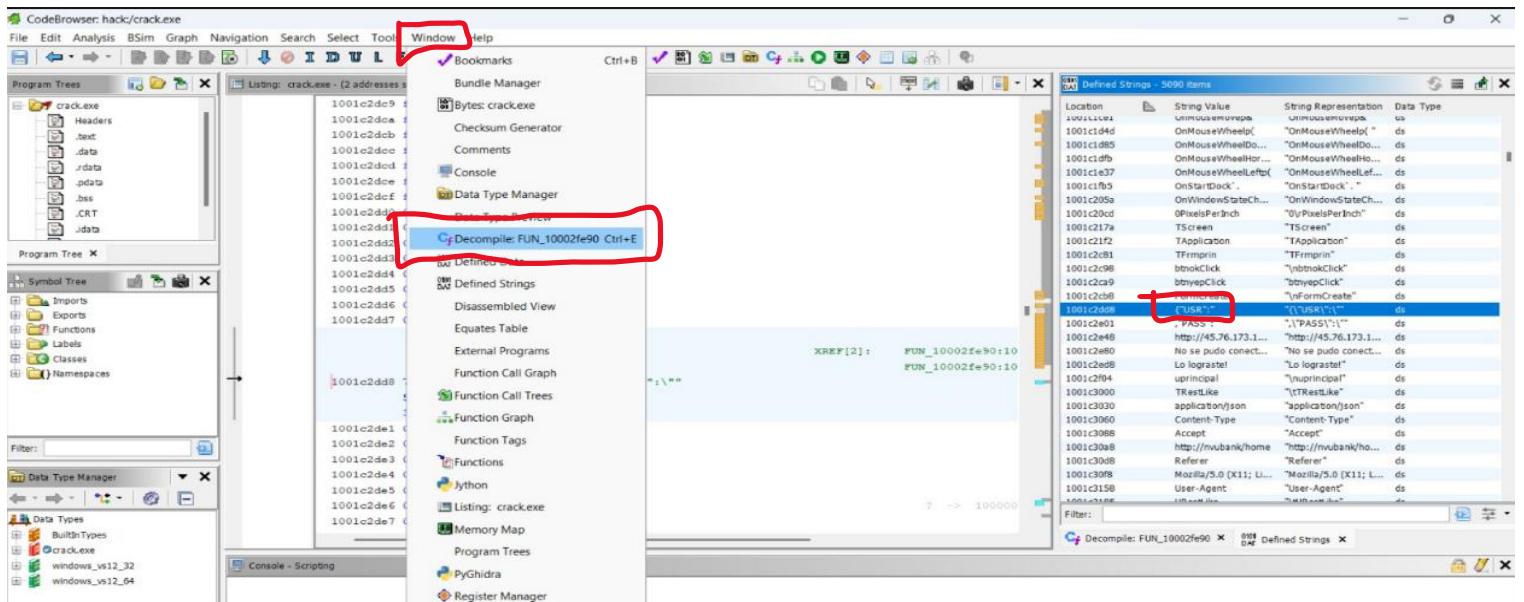
PERIODO [ENE-JUN 2026]

ENLACE AL VIDEO - <https://youtu.be/c3V1gDUp9kc>

Abrimos el ejecutable con ghidra y ocupamos la opción define strings y observamos que aparecen las variables donde se define el usuario y contraseña en la base de datos (“USR” y “PWD”).



En el apartado Window (Parte superior de la pantalla), seleccionamos la opción “Decompile” mientras seleccionamos la variable “USR” en el apartado define strings.



Una vez seleccionada esa opción, podemos ver el código, en donde, si prestamos atención, podemos ver que hay una parte en donde podemos ver una validación donde nos dice que no se pudo conectar al servidor. Siguiendo la lógica del código vista en clase, la siguiente validación es la que creemos que hace que valide el usuario accedido. Si damos click a ese if, podemos ver que en la parte de la izquierda hace un salto si es diferente de cero.

Si observamos, se resalta la posición de memoria en donde se encuentra ese salto. Conociendo la información, en el debug x64 buscamos esa posición de memoria a través del step over y step into, encontrando el salto.

The screenshot shows the assembly view of the x64dbg debugger. The assembly code is as follows:

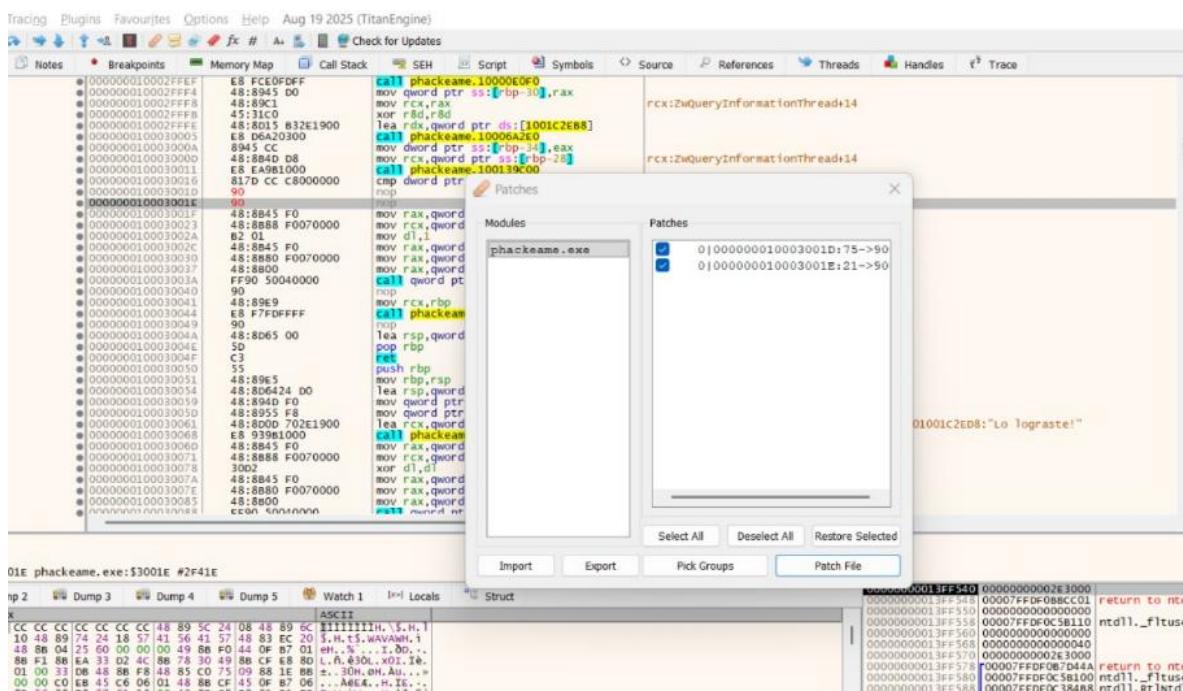
Address	Instruction	Description
000000010002FFEF	E8 FCE0FDFF	call phackeame.10000E0F0
000000010002FF4	48:8945 D0	mov qword ptr ss:[rbp-30],rax
000000010002FF8	48:89C1	mov rcx,rax
000000010002FFB	45:31C0	xor r8d,r8d
000000010002FFE	48:8D15 B32E1900	lea rdx,qword ptr ds:[1001C2EB8]
0000000100030005	E8 D6A20300	call phackeame.10006A2E0
000000010003000A	8945 CC	mov dword ptr ss:[rbp-34],eax
000000010003000D	48:8B4D D8	mov rcx,qword ptr ss:[rbp-28]
0000000100030011	E8 F8010000	call phackeame.100139C00
0000000100030016	817D CC C8000000	cmp dword ptr ss:[rbp-34],c8
000000010003001D	-75 21	je phackeame.100030040
000000010003001F	48:8B45 F0	mov rax,qword ptr ss:[rbp-10]
0000000100030023	48:8B88 F0070000	mov rcx,qword ptr ds:[rax+7F0]
000000010003002A	B2 01	mov d1,1
000000010003002C	48:8B45 F0	mov rax,qword ptr ss:[rbp-10]
0000000100030030	48:8B80 F0070000	mov rcx,qword ptr ds:[rax+7F0]
0000000100030037	48:8800	mov rax,qword ptr ds:[rax]
000000010003003A	FF90 50040000	call qword ptr ds:[rax+450]
0000000100030040	90	nop
0000000100030041	48:89E9	mov rcx,rbp
0000000100030044	E8 F7FDFFFF	call phackeame.10002FE40
0000000100030049	90	nop
000000010003004A	48:8D65 00	lea rsp,qword ptr ss:[rbp]
000000010003004E	5D	pop rbp

Desensamblamos el salto con click derecho y le ponemos nop y la parchamos.

```

0000000010003001F 48:0B4D D0 E8 EA9B1000    mov rax,qword ptr ss:[rbp-20]
00000000100030016 817D CC C8000000    call phackeame.100139C00
0000000010003001D v 75 21                   cmp dword ptr ss:[rbp-34],c8
                                                jne phackeame.100030040
0000000010003001E 48:8B45 F0               mov rax,qword ptr ss:[rbp-10]
00000000100030023 48:8B88 F00700000    mov rax,qword ptr ds:[rax+7F0]
0000000010003002A B2 01                   mov dl,1
0000000010003002C 48:8B45 F0               mov rax,qword ptr ss:[rbp-10]
00000000100030030 48:8B88 F00700000    mov rax,qword ptr ds:[rax+7F0]
00000000100030037 48:8B00                   mov rax,qword ptr ds:[rax]
0000000010003003A FF90 50040000    call qword ptr ds:[rax+450]
00000000100030040 90                      nop
00000000100030041 48:89E9                   mov rcx,rbp
00000000100030044 E8 F7FDFFFF    call phackeame.10002FE40
00000000100030049 90                      nop
0000000010003004A 48:8D65 00             lea rsp,qword ptr ss:[rbp]
0000000010003004E 5D                      pop rbp
0000000010003004F C3                      ret
00000000100030050 55                      push rbp
00000000100030051 48:89E5                   mov rbp,rs
00000000100030054 48:8D6424 D0           lea rsp,qw
00000000100030059 48:894D F0               mov qword
0000000010003005D 48:8955 F8               mov qword
00000000100030061 48:8D00 702E1900    lea rcx,qw
00000000100030068 E8 93981000    call phackeame.10002E88
0000000010003006D 48:8B45 F0               mov rax,qw
00000000100030071 48:8B88 F00700000    mov rcx,qw
00000000100030078 30D2                   xor dl,dl
0000000010003007A 48:8B45 F0               mov rax,qw
0000000010003007D 48:8B80 F00700000    mov rax,qword ptr ds:[rax+7F0]

```



Y finalmente, conseguimos hackear la app.

