You know 0xDiablos – Writeup

HackTheBox – Pwn – Easy

Written by Ron Jost

```
(base) hacker5preme:~/HTB/Challenges/rev_wide$ file wide
wide: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=13869bb7ce2c22f474b95ba21c9d7e9ff74ecc3f, not stripped
```

It is a Linux executable. It needs to be used with db.ex and shows the following.

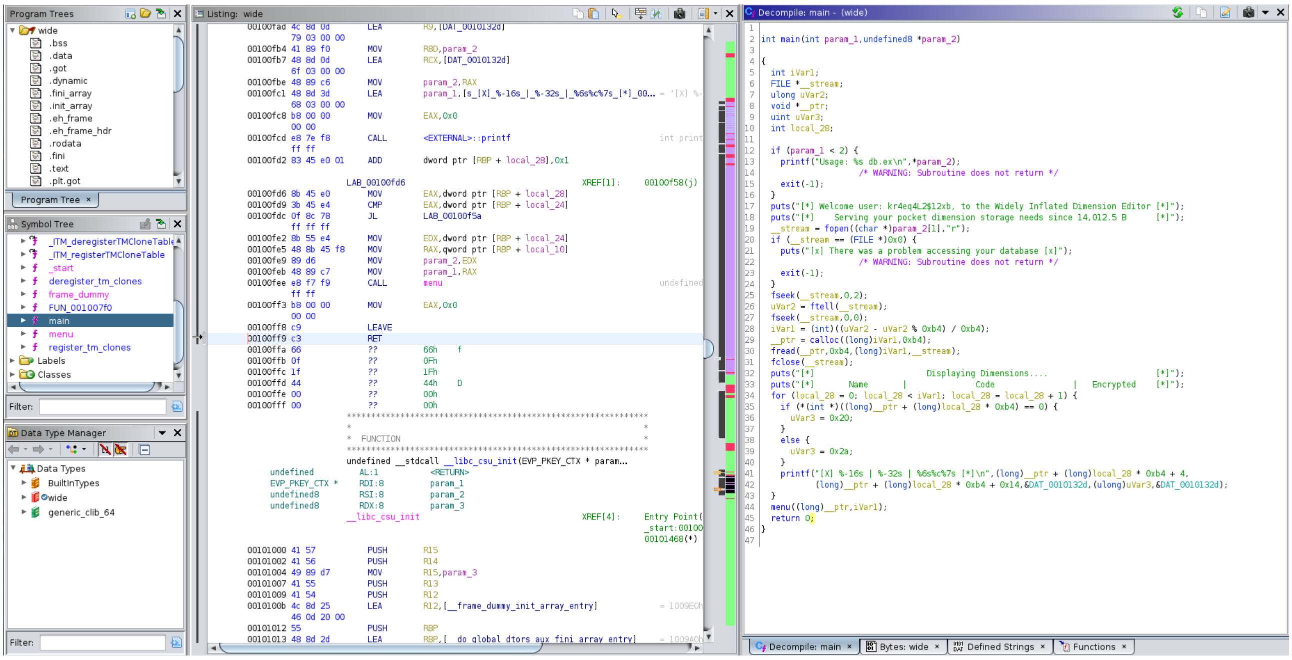
```
(base) hacker5preme:~/HTB/Challenges/rev_wide$ ./wide db.ex
[*] Welcome user: kr4eq4L2$12xb, to the Widely Inflated Dimension Editor [*]
[*]     Serving your pocket dimension storage needs since 14,012.5 B      [*]
[*]                        Displaying Dimensions....                      [*]
[*]       Name       |              Code                |   Encrypted     [*]
[X] Primus           | people breathe variety practice  |                 [*]
[X] Cheagaz          | scene control river importance   |                 [*]
[X] Byenoovia        | fighting cast it parallel        |                 [*]
[X] Cloteprea        | facing motor unusual heavy       |                 [*]
[X] Maraqa           | stomach motion sale valuable     |                 [*]
[X] Aidor            | feathers stream sides gate       |                 [*]
[X] Flaggle Alpha    | admin secret power hidden        |       *         [*]
Which dimension would you like to examine?
```

It allows us to input. First I tried to input the Names shown on the left, but it didn‘t work. Then I tried Numbers, and Primus is Number 1 and Flaggle Alpha is Number 6.

```
Which dimension would you like to examine? 6
[X] That entry is encrypted - please enter your WIDE decryption key:
```

How do we find our WIDE decryption key? Strings shows nothing, so we will use Ghidra to analyze the binary and find the decryption key.

We first navigate to the main function:



There we can see, that the menu function is called.

```
149     printf("[X] That entry is encrypted - please enter your WIDE decryption key: ");
150     fgets(local_c8,0x10,stdin);
151     mbstowcs(local_1c8,local_c8,0x10);
152     iVar1 = wcscmp(local_1c8,L"sup3rs3cr3tw1d3");
153     if (iVar1 == 0) {
154       for (local_1d4 = 0;
155           (local_1d4 < 0x80 && (*(char *)((long)&local_98 + (long)(int)local_1d4) != '\0'));
156           local_1d4 = local_1d4 + 1) {
157         *(byte *)((long)&local_98 + (long)(int)local_1d4) =
158              *(byte *)((long)&local_98 + (long)(int)local_1d4) ^
159              (char)(local_1d4 * 0x1b) + (char)((int)(local_1d4 * 0x1b) / 0xff);
160       }
161       puts((char *)&local_98);
162     }
163     else {
164       puts("[X]                          Key was incorrect                          [X]");
165     }
166   } while( true );
167 }
168
```

The wcsmp line (152) shows us the decryption key. Input it and you will get the flag :)