

# whitecr0w Easy Peasy

<https://crackmes.one/crackme/5d295dde33c5d410dc4d0d05>

Crackme by **b1h0** <https://crackmes.one/user/b1h0>

Date: 05/oct/2019

To analyze this file I have used **Ghidra** and **x64dbg**, simply by trying both tools and seeing the differences. It is good to contrast and train in both dynamic and static.

## Ghidra - notes

1. Load executable and Analyze.
2. Search in **Symbol Tree** left dialog the text "**main**".
3. In **Listing** you can see at address **0040155a** the username that is:  
**"iwonderhowitfeelstobeatimetravel"**
4. Next, at address **0040158c** the password is revealed to us:  
**heyamyspaceboardisbrokencanyouhelpmefindit?**
5. In the code decompilation window you can also see clearly.
6. I think we don't need anything else.



## x64dbg - notes

- Its a 64bits Windows exe
- Strings with the username and password are also revealed quickly and without problems from **00401553**: "**iwonderhowitfeelstobeatimetraveler**",  
**"heyamyspaceboardisbrokencanyouhelpmefindit?"**.

0000000000401543	48:8D45 DE	lea rax,qword ptr ss:[rbp-22]	Arg1 = rax:EntryPoint
0000000000401547	48:89C1	mov rcx,rax	Sub_4460A0
000000000040154A	E8 51480400	call easyeasy.sub_4460A0	Arg4 = rdx:EntryPoint
000000000040154F	48:8D55 DE	lea rdx,qword ptr ss:[rbp-22]	
0000000000401553	48:8D45 D0	lea rax,qword ptr ss:[rbp-30]	
0000000000401557	49:89D0	mov r8,rdx	Arg3 = rdx:EntryPoint
000000000040155A	48:8D15 9F6A0800	lea rdx,qword ptr ds:[488000]	Arg2 = "iwonderhowitfeels to beatimetraveler"
0000000000401561	48:89C1	mov rcx,rax	Arg1 = rax:EntryPoint
0000000000401564	E8 57DC0400	call easyeasy.sub_44F1C0	Sub_44F1C0
0000000000401569	48:8D45 DE	lea rax,qword ptr ss:[rbp-22]	
000000000040156D	48:89C1	mov rcx,rax	Arg1 = rax:EntryPoint
0000000000401570	E8 5B480400	call easyeasy.sub_446000	Sub_446000
0000000000401575	48:8D45 DF	lea rax,qword ptr ss:[rbp-21]	
0000000000401579	48:89C1	mov rcx,rax	Arg1 = rax:EntryPoint
000000000040157C	E8 1F480400	call easyeasy.sub_4460A0	Sub_4460A0
0000000000401581	48:8D55 DF	lea rdx,qword ptr ss:[rbp-21]	Arg4 = rdx:EntryPoint
0000000000401585	48:8D45 C0	lea rax,qword ptr ss:[rbp-40]	
0000000000401589	49:89D0	mov r8,rdx	Arg3 = rdx:EntryPoint
000000000040158C	48:8D15 956A0800	lea rdx,qword ptr ds:[488028]	Arg2 = "heyamyspaceboardisbroken can you help me find it?"
0000000000401593	48:89C1	mov rcx,rax	Arg1 = rax:EntryPoint
0000000000401596	E8 25DC0400	call easyeasy.sub_44F1C0	Sub_44F1C0
000000000040159B	48:8D45 DF	lea rax,qword ptr ss:[rbp-21]	

- The string in .rdata section at 0000000000488000

Dirección	Hex	ASCII
0000000000488000	69 77 6F 6E 64 65 72 68 6F 77 69 74 66 65 65 6C	iwonderhowitfeels to beatimetraveler.....heyamyspaceboardisbroken can you help me find it?.....Please, login with your credentials..Use rname:..Now, please insert the password..Password:..GTF0 you lame ass hacker..... You have successfully logged into the system....
0000000000488010	73 74 6F 62 65 61 74 69 6D 65 74 72 61 76 65 6C	
0000000000488020	65 72 00 00 00 00 00 00 68 65 79 61 6D 79 73 70	
0000000000488030	61 63 65 62 6F 61 72 64 69 73 62 72 6F 68 65 6E	
0000000000488040	63 61 6E 79 6F 75 68 65 6C 70 6D 65 66 69 6E 64	
0000000000488050	69 74 3F 00 00 00 00 00 50 6C 65 61 73 65 2C 20	
0000000000488060	6C 6F 67 69 6E 20 77 69 74 68 20 79 6F 75 72 20	
0000000000488070	63 72 65 64 65 6E 74 69 61 6C 73 2E 00 55 73 65	
0000000000488080	72 6E 61 6D 65 3A 00 00 4E 6F 77 2C 20 70 6C 65	
0000000000488090	61 73 65 20 69 6E 73 65 72 74 20 74 68 65 20 70	
00000000004880A0	61 73 73 77 6F 72 64 2E 00 50 61 73 73 77 6F 72	
00000000004880B0	64 3A 00 47 54 46 4F 20 79 6F 75 20 6C 61 6D 65	
00000000004880C0	20 61 73 73 20 68 61 63 68 65 72 2E 00 00 00 00	
00000000004880D0	59 6F 75 20 68 61 76 65 20 73 75 63 63 65 73 73	
00000000004880E0	66 75 6C 6C 79 20 6C 6F 67 67 65 64 20 69 6E 74	
00000000004880F0	6F 20 74 68 65 20 73 79 73 74 65 6D 2E 00 00 00	

- What else?

```

crackmes.one\whitecr0w-Easy_Peasy>EasyPeasy.exe
Please, login with your credentials.
Username:heyamyspaceboardisbroken can you help me find it?
GTF0 you lame ass hacker.

crackmes.one\whitecr0w-Easy_Peasy>EasyPeasy.exe
Please, login with your credentials.
Username:iwonderhowitfeels to beatimetraveler
Now, please insert the password.
Password:heyamyspaceboardisbroken can you help me find it?
You have successfully logged into the system.

crackmes.one\whitecr0w-Easy_Peasy>_

```