The crackme2 file is an ELF file.

```
└─$ ./crackme2
Usage : ./crackme2 password
Good luck, read the source
```

It says Good luck, read the source.

Using strings ,strcmp or ltrace doesn't give us anything.

```
UH-H
[]A\A]A^A_
password OK
password "%s" not OK
Usage : %s password
Good luck, read the source
;*3$"
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.symtab
```

```
└─$ ltrace ./crackme2
__libc_start_main(0×400711, 1, 0×7ffda5463468, 0×400760 <unfinished ...>
printf("Usage : %s password\nGood luck, r"..., "./crackme2"Usage : ./crackme2 password
Good luck, read the source
)                                 = 55
+++ exited (status 0) +++
```

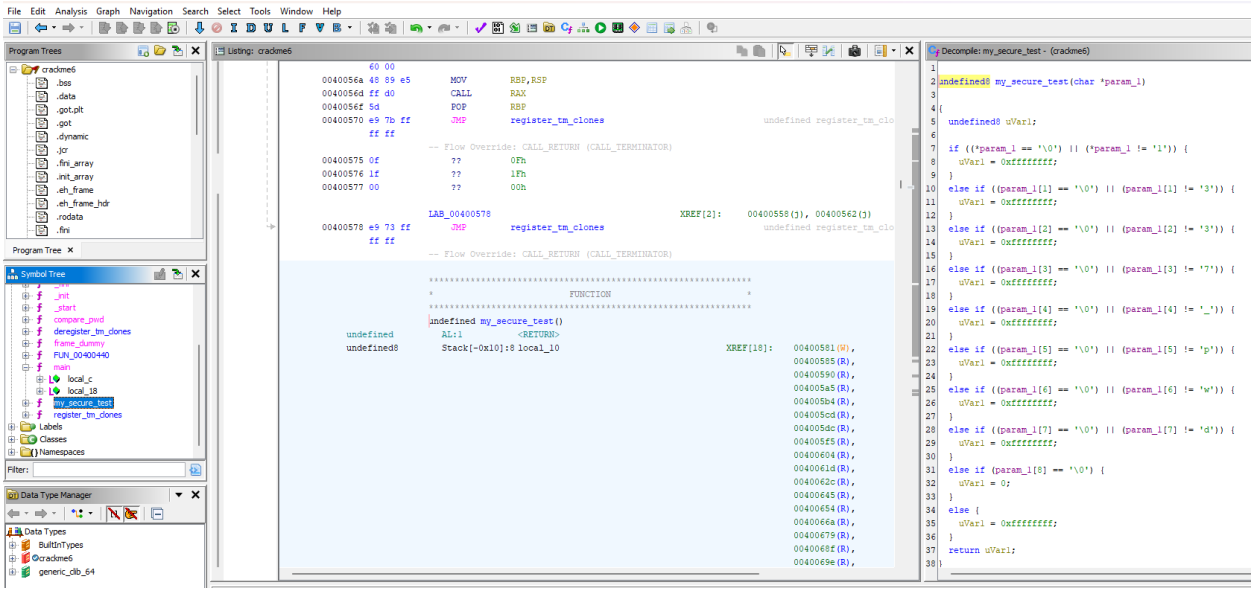
So, we run this file in Ghidra(Ghidra is a reverse engineering tool).

There seems to be nothing of use in the main function

Decompile: main - (crackme6)

```
1
2 undefined8 main(int param_1,undefined8 *param_2)
3
4 {
5   if (param_1 == 2) {
6     compare_pwd(param_2[1]);
7   }
8   else {
9     printf("Usage : %s password\nGood luck, read the source\n",*param_2);
10  }
11  return 0;
12 }
13
```

Going to the my_secure_test function,

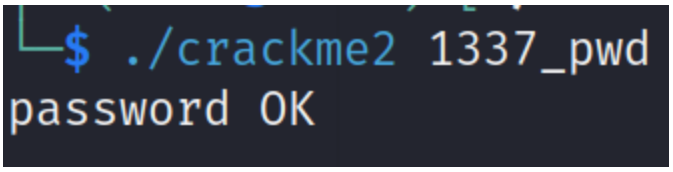


We see some text being passed in the param_1 variable.

Decompile: my_secure_test - (crackme6)

```
1
2 undefined8 my_secure_test(char *param_1)
3
4 {
5   undefined8 uVar1;
6
7   if ((*param_1 == '\0') || (*param_1 != '1')) {
8     uVar1 = 0xffffffff;
9   }
10  else if ((param_1[1] == '\0') || (param_1[1] != '3')) {
11    uVar1 = 0xffffffff;
12  }
13  else if ((param_1[2] == '\0') || (param_1[2] != '3')) {
14    uVar1 = 0xffffffff;
15  }
16  else if ((param_1[3] == '\0') || (param_1[3] != '7')) {
17    uVar1 = 0xffffffff;
18  }
19  else if ((param_1[4] == '\0') || (param_1[4] != '_')) {
20    uVar1 = 0xffffffff;
21  }
22  else if ((param_1[5] == '\0') || (param_1[5] != 'p')) {
23    uVar1 = 0xffffffff;
24  }
25  else if ((param_1[6] == '\0') || (param_1[6] != 'w')) {
26    uVar1 = 0xffffffff;
27  }
28  else if ((param_1[7] == '\0') || (param_1[7] != 'd')) {
29    uVar1 = 0xffffffff;
30  }
31  else if (param_1[8] == '\0') {
32    uVar1 = 0;
33  }
34  else {
35    uVar1 = 0xffffffff;
36  }
37  return uVar1;
38 }
```

“1337_pwd” is being stored in param_1. Could this be the password?



Indeed it was.

There we have our flag as “**flag{1337_pwd}**”.