

# System Security HW3

## Komalika Virendra Acharya

### 117336238

#### Part 1 - crackme1

CodeBrowser: cse509\_hw3/hw3.zip/hw3/crackme1

Location	String Value	String Representation	Data Type
.shstrtab:0000009c	.eh_frame	u8".eh_frame"	u8
.shstrtab:000000a6	.int_array	u8".int_array"	u8
.shstrtab:000000b2	.fini_array	u8".fini_array"	u8
.shstrtab:00000008	.dynamic	u8".dynamic"	u8
.shstrtab:000000c7	.got.plt	u8".got.plt"	u8
.shstrtab:0000000d	.data	u8".data"	u8
.shstrtab:00000028	.bss	u8".bss"	u8
.shstrtab:000000db	.comment	u8".comment"	u8
00100001	.ELF	"ELF"	ds
001002a8	/lib/x86_64-linux-gnu/libc.so.6	"/lib/x86_64-linux-gnu/libc.so.6"	ds
00100000	GNU	"GNU"	ds
00100019	_co_.finalize	u8".co_.finalize"	u8
00100429	__libc_start_main	u8"__libc_start_main"	u8
0010043b	printf	u8"printf"	u8
00100441	stdin	u8"stdin"	u8
00100447	fgets	u8"fgets"	u8
0010044d	strchr	u8"strchr"	u8
00100454	puts	u8"puts"	u8
00100459	libc.so.6	u8"libc.so.6"	u8
00100463	GLIBC_2.2.5	u8"GLIBC_2.2.5"	u8
0010046f	_JTM_deregisterTMClone	u8"_JTM_deregisterTMClone"	u8
0010048b	_gmon_start_	u8"_gmon_start_"	u8
0010049a	_JTM_registerTMClone	u8"_JTM_registerTMClone"	u8
00102009	Enter password:	"Enter password:"	ds
0010201b	ACCESS GRANTED	"ACCESS GRANTED"	ds
0010202a	ACCESS DENIED	"ACCESS DENIED"	ds
00102079	ZR	"ZR"	ds
00102099	ZR	"ZR"	ds

Console - Scripting

```
SUNYSB.EDU+kacharya@LIBL-9PV5FL3 MINGW64 ~/Downloads/cse509hw1
$ ./ssh_to_qemu.sh
user@127.0.0.1's password:
Linux debian 5.10.0-35-amd64 #1 SMP Debian 5.10.237-1 (2025-05-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Oct 10 00:19:48 2025 from 10.0.2.2
user@debian:~$ ls
crackme1  hw1  psi.py
user@debian:~$ ./crackme1
-bash: ./crackme1: Permission denied
user@debian:~$ chmod +x crackme1
user@debian:~$ ./crackme1
Enter password: Zdsffff@2!
ACCESS GRANTED
user@debian:~$ |
```

Using Defined Strings we can find out the value for strcmp and hence what the password is.

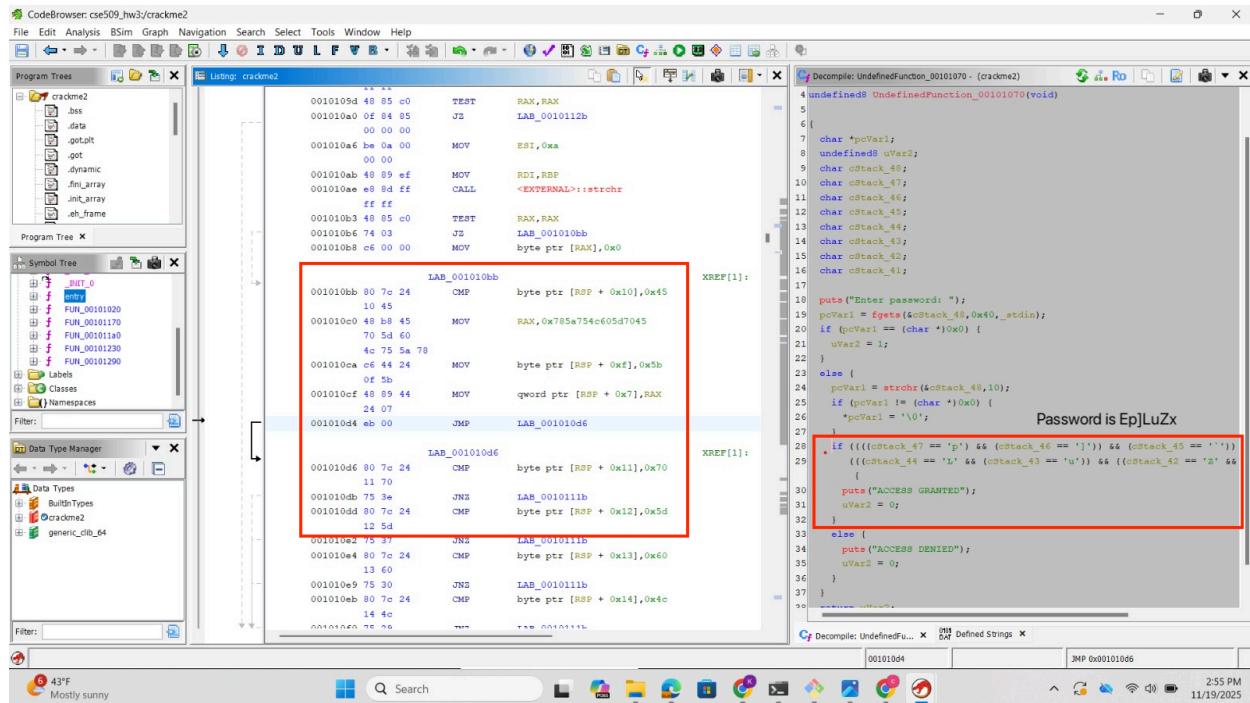
On fgets/sccanf line: // reads up to 0x40 bytes into buffer

On first cmp line: // compares buffer[0] to 'Z' (0x5A)

On subsequent cmp lines: // compares buffer[1] == 'd', buffer[2] == 's', ...

On conditional jump to success: // if all comparisons true -> ACCESS GRANTED

## Part 2 - crackme2



```

SUNYSB.EDU+kacharya@LIBL-9PV5FL3 MINGW64 ~/Downloads/cse509hw1
$ ./ssh_to_qemu.sh
user@127.0.0.1's password:
Linux debian 5.10.0-35-amd64 #1 SMP Debian 5.10.237-1 (2025-05-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 19 13:49:40 2025 from 10.0.2.2
user@debian:~$ chmod +x crackme2
user@debian:~$ ./crackme2
Enter password:
Ep]`LuZx
ACCESS GRANTED
user@debian:~$

```

Key evidence: fgets reads input and strchr strips newline; the code then compares buffer chars directly to hard-coded characters.

Checks: cStack\_48=='E', cStack\_47=='p', cStack\_46==']', cStack\_45=='',  
cStack\_44=='L', cStack\_43=='u', cStack\_42=='Z', cStack\_41=='x'.

input[0] must be 'E'  
input[1] must be 'p'  
... input[7] must be 'x'  
if all true -> puts("ACCESS GRANTED")

CMP compares input byte to stored value JNZ = jump if not equal → ACCESS DENIED  
If no jumps taken → ACCESS GRANTED

Recovered password (tested): Ep]LuZx — entering this prints "ACCESS GRANTED".

## Part 3 - crackme2 patch

The screenshot shows the Immunity Debugger interface with the assembly listing for the crackme2 binary. The assembly code is as follows:

```

1 /* WARNING: Globals starting with '_' overlap smaller symbols at the same address
2
3 undefined8 UndefinedFunction_00101070(void)
4
5 {
6     char *pcVar1;
7     undefined8 uVar2;
8     char acStack_48 [64];
9
10    puts("Enter password: ");
11    pcVar1 = fgets(acStack_48,0x40,_stdin);
12    if ((pcVar1 == (char *)0x0)) {
13        uVar2 = 1;
14    }
15    else {
16        pcVar1 = strchr(acStack_48,10);
17        if ((pcVar1 != (char *)0x0)) {
18            *pcVar1 = '\0';
19        }
20        puts("ACCESS GRANTED");
21        uVar2 = 0;
22    }
23
24    return uVar2;
25 }
26

```

A red box highlights the unconditional jump instruction `JMP LAB_00101107` at address `001010d4`. Another red box highlights the `puts("ACCESS GRANTED")` instruction at address `00101107`.

```

SUNYSB.EDU+kacharya@LIBL-9PV5FL3 MINGW64 ~/Downloads/cse509hw1
$ ./ssh_to_qemu.sh
user@127.0.0.1's password:
Linux debian 5.10.0-35-amd64 #1 SMP Debian 5.10.237-1 (2025-05-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 19 22:17:33 2025 from 10.0.2.2
user@debian:~$ chmod +x crackme2_patched
user@debian:~$ ./crackme2_patched
Enter password:

ACCESS GRANTED
user@debian:~$
```

Changed the conditional jump at `01010d4` (originally `JNZ`) to an unconditional `JMP` so the success path is always taken, since changing first if allows us to bypass the next ifs as well.

`JMP` to the address where we print `ACCESS GRANTED` so it always goes to that path.

Original: `JNZ 010111b // jump to failure if not equal`  
Patched: `JMP 0101107 // forced success path (PATCHED)`  
`ACCESS_GRANTED` path → `puts("ACCESS GRANTED")`

Test: running `./crackme2_patched` (terminal shown) confirms bypass even with blank input we get `ACCESS GRANTED`.