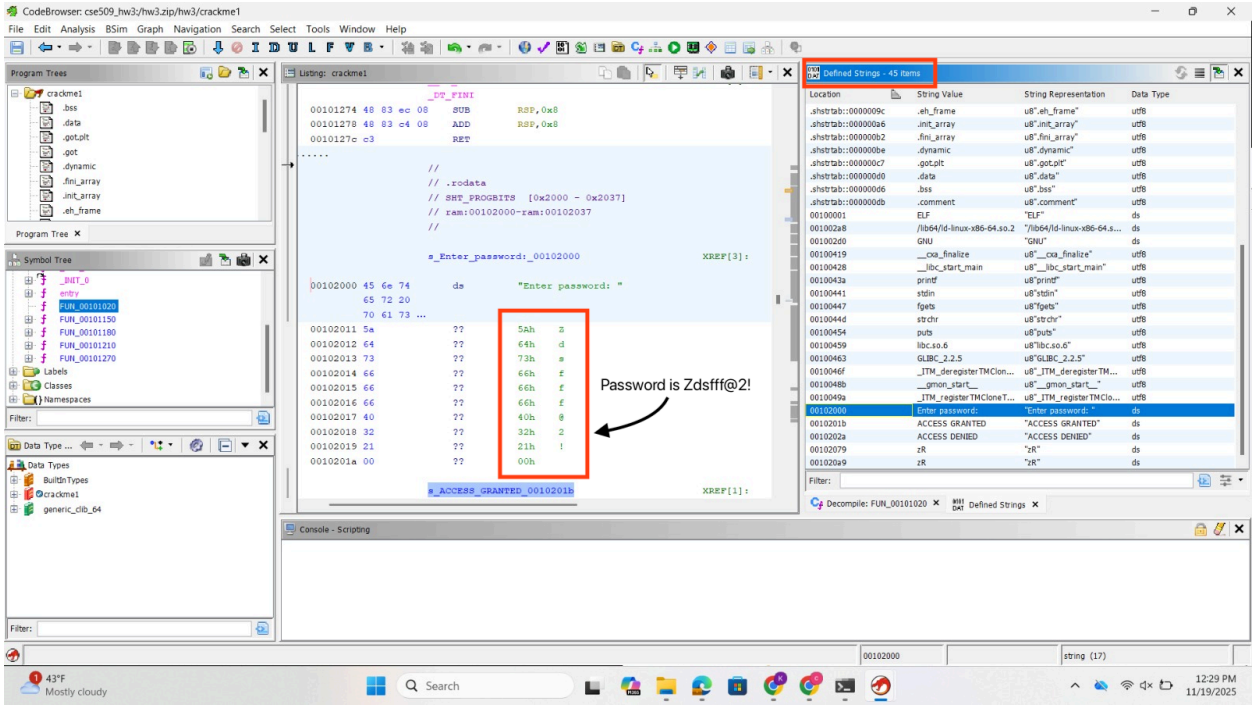
System Security HW3
Komalika Virendra Acharya
117336238

Part 1 - crackme1



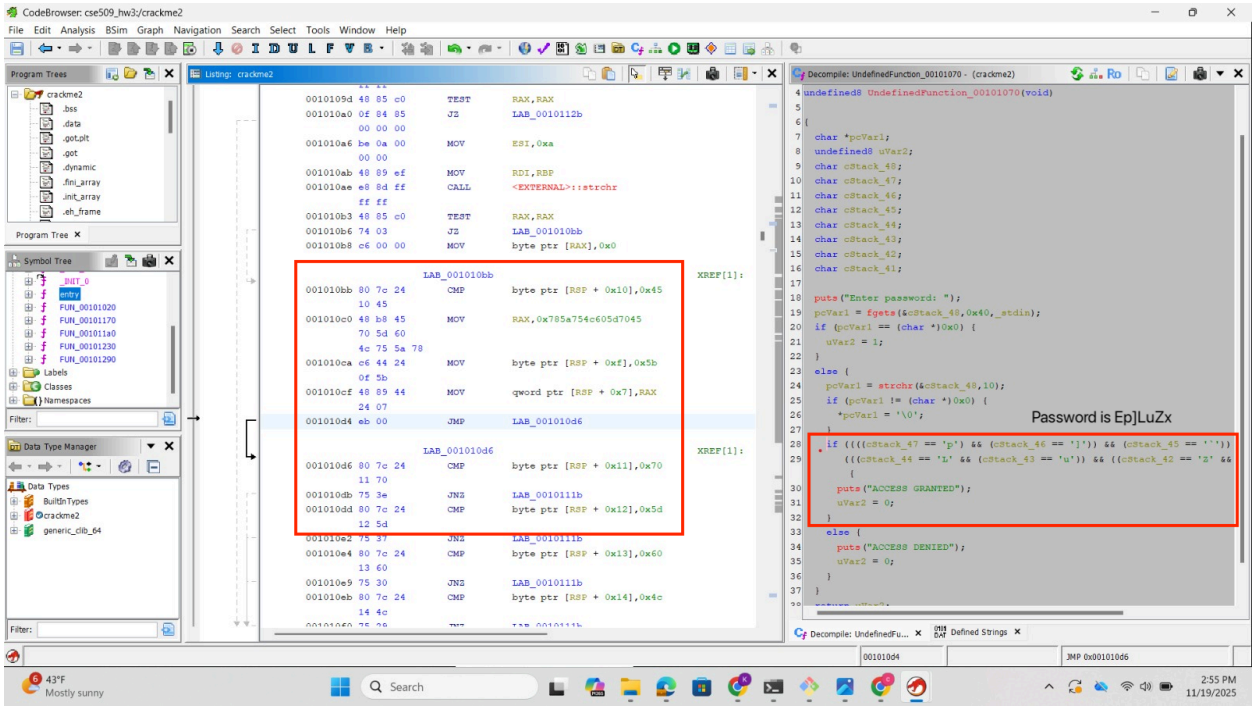

```
SUNYSB.EDU+kacharya@LIBL-9PV5FL3 MINGW64 ~/Downloads/cse509hw1
$ ./ssh_to_qemu.sh
user@127.0.0.1's password:
Linux debian 5.10.0-35-amd64 #1 SMP Debian 5.10.237-1 (2025-05-19) x86_64

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: Zdsfff@2!
ACCESS GRANTED
user@debian:~$
```

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

On fgets/scanf 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:~$
```

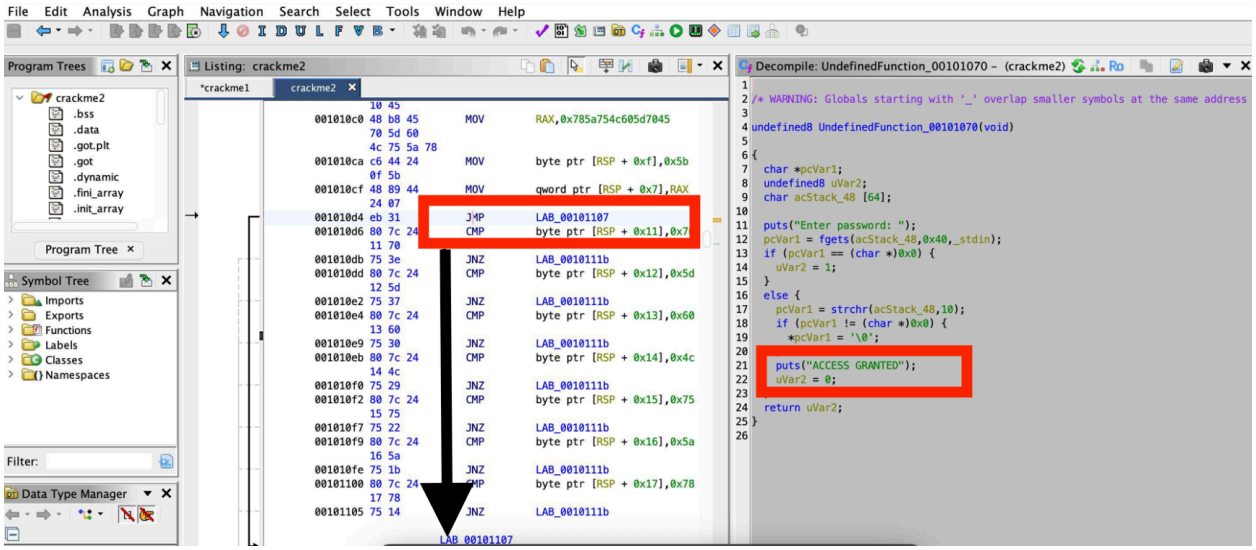
Key evidence: fgets reads input and strchr strips newline; the code then compares buffer chars directly to hard-coded characters.
Checks: cStack_48=='E', cStack_47=='p', cStack_46==']', cStack_45==", cStack_44=='L', cStack_43=='u', cStack_42=='Z', cStack_41=='x'.

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




```
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.

CMP byte ptr [RSP+0x11],0x70 // compare input byte 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.