```
login as: level9
level9@192.168.98.133's password:
[level9@ftz level9]$ pwd
/home/level9
[level9@ftz level9]$ ls
hint  public_html  tmp
```

Hint 파일 확인

```
[level9@ftz level9]$ cat hint


다음은 /usr/bin/bof의 소스이다.

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

main(){

  char buf2[10];
  char buf[10];

  printf("It can be overflow : ");
  fgets(buf,40,stdin);

  if ( strncmp(buf2, "go", 2) == 0 )
   {
        printf("Good Skill!\n");
        setreuid( 3010, 3010 );
        system("/bin/bash");
   }

}

이를 이용하여 level10의 권한을 얻어라.
```

fgets → 파일을 통해 한 행의 문자열을 입력 받음

"₩n"문자를 만날때까지 문자열을 읽지만 두번째로 넣은 매개변수 수-1개의 문자열을 기준으로 문자열을 판단해서 가지고 온다. → 수-1보다 작은데 ₩n이 나오면 해당 문자열까지만 읽고 수-1 까지 읽었는데 ₩n이 없더라도 수-1까지만 읽는다

fgets(buf, 40, stdin) → 문자열을 최대 40자리까지 읽어서 buf에 담는다.

strncmp(buf2, "go", 2) → buf2, "go" : 비교할 문자열 / 2 : 비교할 문자열의 길이

➔ buf2가 go라면 실행

```
if ( strncmp(buf2, "go", 2) == 0 )
 {
      printf("Good Skill!\n");
      setreuid( 3010, 3010 );
      system("/bin/bash");
 }
```

buf2와 go를 두번째 문자열까지 비교하여 같으면 Good Skill! 출력

setreuid(uid_t ruid, uid_t euid) → uid와 euid 각각 원하는 대로 바꿀 수 있다.

uid_t ruid = real user id(실제 id), uid_t euid = effective user id(현재 권한) /

/bin/bash이용시 setreuid(0,0)을 걸어줘야 루트 권한을 얻을 수 있음

하는 도중 에러남