Quiz

재미있는 문제 : 무임승차

이번엔 재미있는 실습 문제를 하나 풀어 볼 시간입니다.
지난 시간에 메모리 주소에 대해 알아보았는데요, 아직 '버퍼오버플로우 공부를 하는데 메모리 주소는 왜 알아야 하는 거지?'라는 생각이 드실 겁니다. 이 궁금점을 해소시켜 드리기 위해 재밌는 문제를 하나 준비해 보았습니다.

이는 메모리 주소의 개념을 알아야 풀 수 있는 문제이며, 동시에 버퍼 오버플로우와 깊은 관련을 가지고 있는 문제입니다.

./quiz/quiz.c

```
main()
{
        int auth = 0;
        char passwd[20];

        printf("패스워드를 입력하세요 : ");
        gets(passwd);

        // 패스워드가 "secretkey"라면 인증 통과
        if(strcmp(passwd, "secretkey") == 0)
                auth = 1;

        if(auth)
                printf("축하합니다. 인증에 통과하였습니다!₩n");
        else
                printf("인증에 실패하였습니다.₩n");
}
```

Quiz 재미있는 문제 : 무임승차

앞의 코드를 실습 서버에서 컴파일 한 후 실행해 봅니다.

```
$ cd quiz
$ gcc -o quiz quiz.c
$ ./quiz
패스워드를 입력하세요 : abcd
인증에 실패하였습니다.
$
```

이번엔 제대로 된 패스워드를 넣어보겠습니다.

```
$ ./quiz
패스워드를 입력하세요 : secretkey
축하합니다. 인증에 통과하였습니다!
$
```

우리는 소스 코드에 적힌 패스워드를 볼 수 있기 때문에 정확한 패스워드를 알 수 있었습니다.

그럼 제가 문제 파일을 컴파일하기 전에 "secretkey"라는 패스워드를 다른 값으로 살짝 바꾸면 어떻게 될까요?

그리고 소스 코드를 볼 수 없도록 삭제해 버린다면?
그래도 패스워드를 맞출 수 있을까요!?

Quiz 재미있는 문제 : 무임승차

./quiz/real_quiz.c

```
main()
{
        int auth = 0;
        char passwd[20];

        printf("패스워드를 입력하세요 : ");
        gets(passwd);

        if(strcmp(passwd, "[???????]") == 0)
                auth = 1;

        if(auth)
                printf("축하합니다. 인증에 통과하였습니다!₩n");
        else
                printf("인증에 실패하였습니다.₩n");
}
```

실습 서버에 로그인한 후 ./quiz 폴더로 이동하면 real_quiz라는 파일이 있습니다.

한 번 패스워드를 맞춰서 인증을 통과해 보세요!
잠깐, 파일을 에디터로 열어서 패스워드에 해당하는 문자열을 찾아보면 되지 않냐고요?

그런 쉬운 방법은 막기 위해 읽기(r) 권한을 제거했습니다.
그렇기 때문에 여러분은 다른 방법을 찾아 문제를 푸셔야 합니다.

이제 한번 풀어보세요! good luck!