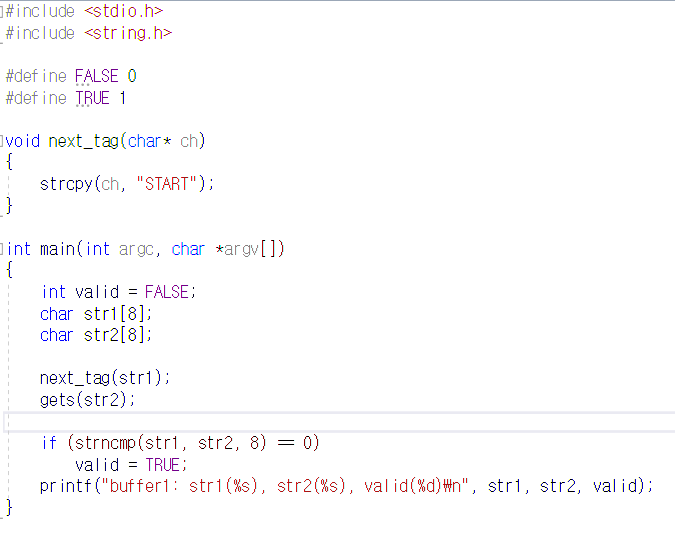
**Assignment3 Report**

2018008613 안상욱

1. **코드 작성**



다음과 같이 코드를 작성한 후 buffer1.c라는 이름으로 저장해 주었습니다.

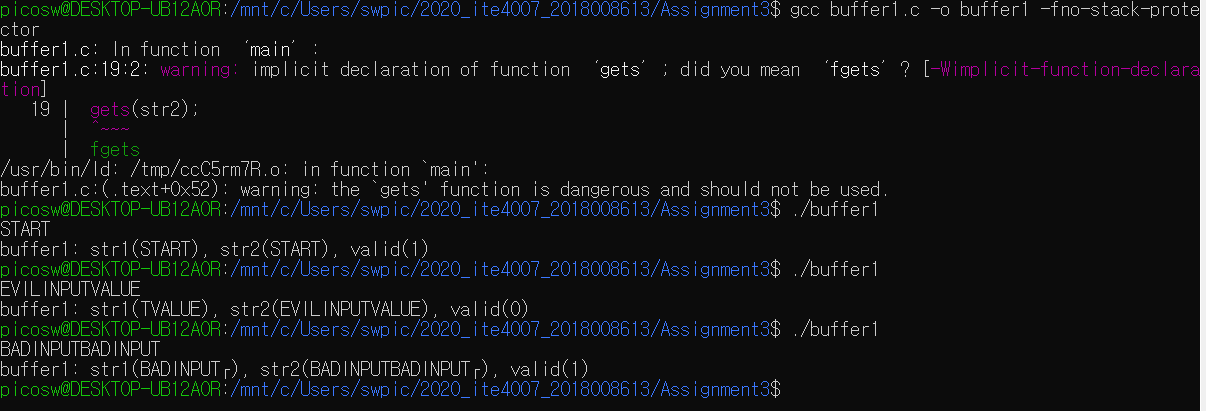
Valid의 값을 FALSE로 초기화해 주었습니다.

Next\_tag 함수는 ch라는 parameter의 값을 START로 바꾸어 주는 함수입니다.

이 함수를 이용해 str1의 초기값을 START로 지정해주고, gets 함수를 이용해 str2의 값을 입력 받은 뒤 str1과 str2의 값을 비교해서 같으면 valid의 값을 TRUE로 바꾸어 주었습니다.

그 후 str1, str2, valid의 값을 출력해 주었습니다.

1. **실행 결과**



Wsl 설치 후 실행 결과 다음과 같습니다.

START를 입력하면 str2에 START가 입력되어 str1과 같은 값을 나타내므로 valid 값이 TRUE가 되어 1이 출력됩니다.

EVILINPUTVALUE를 입력하면 이 값이 str2에 저장되는데 str2의 크기는 8칸이므로, EVILINPU 8단어 뒤의 TVALUE 값이 overflow되어서 str1에 저장됩니다. Strcmp 결과 EVILINPU와 TVALUE 값이 다르므로 valid가 0이 됩니다

BADINPUTBADINPUT을 입력하면 이 값이 str2에 저장되는데 str2의 크기는 8칸이므로, BADINPUT 8단어 뒤의 BADINPUT 값이 overflow 되어서 str1에 저장됩니다. Strcmp 결과 BADINPUT과 BADINPUT 값이 같으므로 valid가 1이 되어 buffer overflow 공격이 성공하게 됩니다.