

버퍼 오버플로우

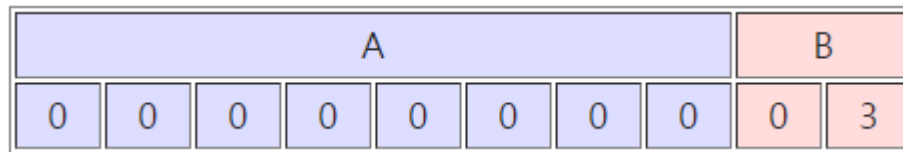
차례

- 버퍼 오버플로우
- 'Scanf'와 'Scanf_s'
- 이용, 보호 대응 종류

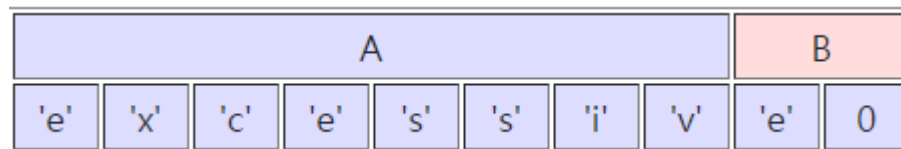
버퍼 오버플로우 Buffer Overflow

- **버퍼** : 어떤 장치에서 다른 장치로 데이터를 송신할 때 일어나는 시간의 차이나 데이터 흐름의 속도 차이를 조정하기 위해 일시적으로 데이터를 기억시키는 장치
- 메모리를 다루는 데에 오류가 발생하여 잘못된 동작을 하는 프로그램 취약점

버퍼 오버플로우



문자열 "excessive"를 A 버퍼에 저장



한 바이트짜리 0값: 스트링의 끝

'Scanf'와 'Scanf_s'

```
1  #include <stdio.h>
2
3  int main() {
4      int value;
5
6      scanf("%d", &value);
7      printf("Hello return");
8
9      return 1;
10 }
11
```

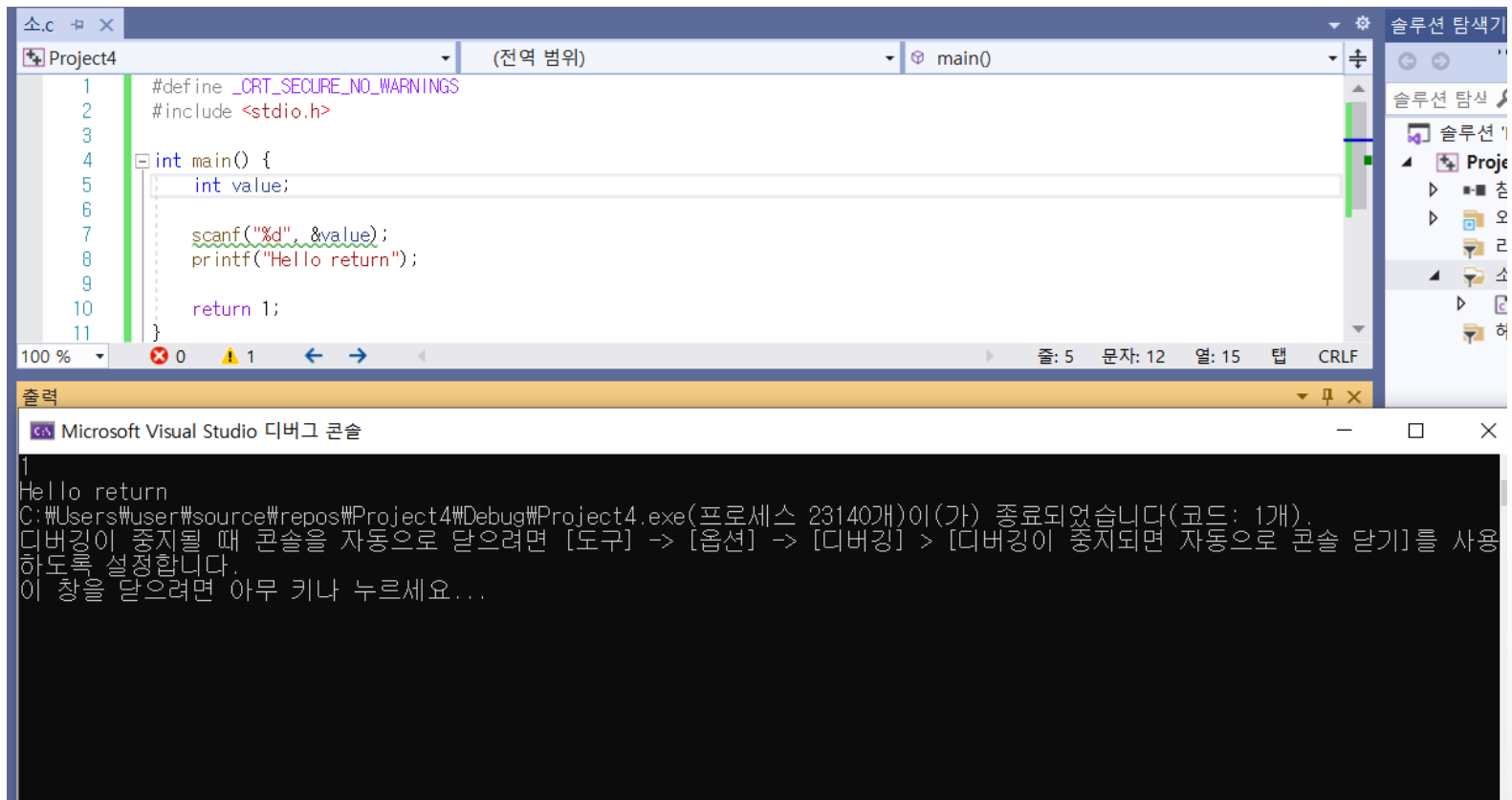
1 % | 문제가 검색되지 않음 | 줄: 8 문자: 5 탭 CR

류 목록

체 솔루션 | 1 오류 | 0/1 경고 | 0 메시지 | 빌드 + IntelliSense | 검색 오류 목록

코드	설명	프로젝트	파일	줄	비표시 오류(Suppress)
C4996	'scanf': This function or variable may be unsafe. Consider using scanf_s instead. To disable deprecation, use <code>_CRT_SECURE_NO_WARNINGS</code> . See online help for details.	Project4	소.c	6	

‘Scanf’와 ‘Scanf_s’



The screenshot displays the Visual Studio IDE with a C program in the main editor and its execution output in the debug console.

Source Code (Project4.c):

```
1 #define _CRT_SECURE_NO_WARNINGS
2 #include <stdio.h>
3
4 int main() {
5     int value;
6
7     scanf("%d", &value);
8     printf("Hello return");
9
10    return 1;
11 }
```

Debug Console Output:

```
1
Hello return
C:\Users\User\source\repos\Project4\Debug\Project4.exe(프로세스 23140개)이(가) 종료되었습니다(코드: 1개).
디버깅이 중지될 때 콘솔을 자동으로 닫으려면 [도구] -> [옵션] -> [디버깅] > [디버깅이 중지되면 자동으로 콘솔 닫기]를 사용
하도록 설정합니다.
이 창을 닫으려면 아무 키나 누르세요...
```

‘Scanf’와 ‘Scanf_s’

```
scanf_s("형식지정자", &변수);
```

```
scanf_s("형식지정자", &변수, sizeof(버퍼사이즈));
```

이용 종류

- NOP 슬라이드 기법
- 레지스터에 저장된 주소로 건너뛰기

보호 대응 종류

- 프로그래밍 언어 선택
- 안전한 라이브러리 사용
- 버퍼 오버플로 보호
- 포인터 보호
- 실행 공간 보호
- 주소 공간 배치 난수화
- 심층 패킷 조사

감사합니다