FSB INDEX CONTENTS

Format String Bug

2학년 송지현

INDEX

FSB의 개념

문자열 포맷 처리 함수 사용할 때 발생할 수 있는 취약점

C언어에서 가장 많이 발생

주로 print함수와 scanf 함수에서 발생

```
printf("%d", num);
scanf("%d", &num);
```

FSB의 개념

포맷 인자

각 포맷 인자는 함수의 인자로 넘겨지며,

Format String에 3개의 포맷 인자가 있으면

함수에도 3개의 인자가 존재 해야함

Format String	Type	Meaning
%d	int	정수
%f	float	실수
%c	char	문자
%s	string	문자열
%u	decimal	10진수
%x	hexadecimal	16진수
%n	int	출력된 문자의 개수

FSB 발생 원리

```
printf(buf);
```

사용자 입력

정상 출력

```
printf("hello");
printf("%x");
printf("%s");
```

Undefined Behavior

FSB 대응 방안

Format string을 함수의 입력 파라미터로 사용 X

```
printf(argv[1]);
```

```
printf("%s", argv[1]);
```

함수 사용 시, format string을 지정하여 간접적으로 참조가 되도록 한다.

FSB의 실습

```
[jini@fedora ~]$ cd wlgus
[jini@fedora wlgus]$ vi apple.c
```

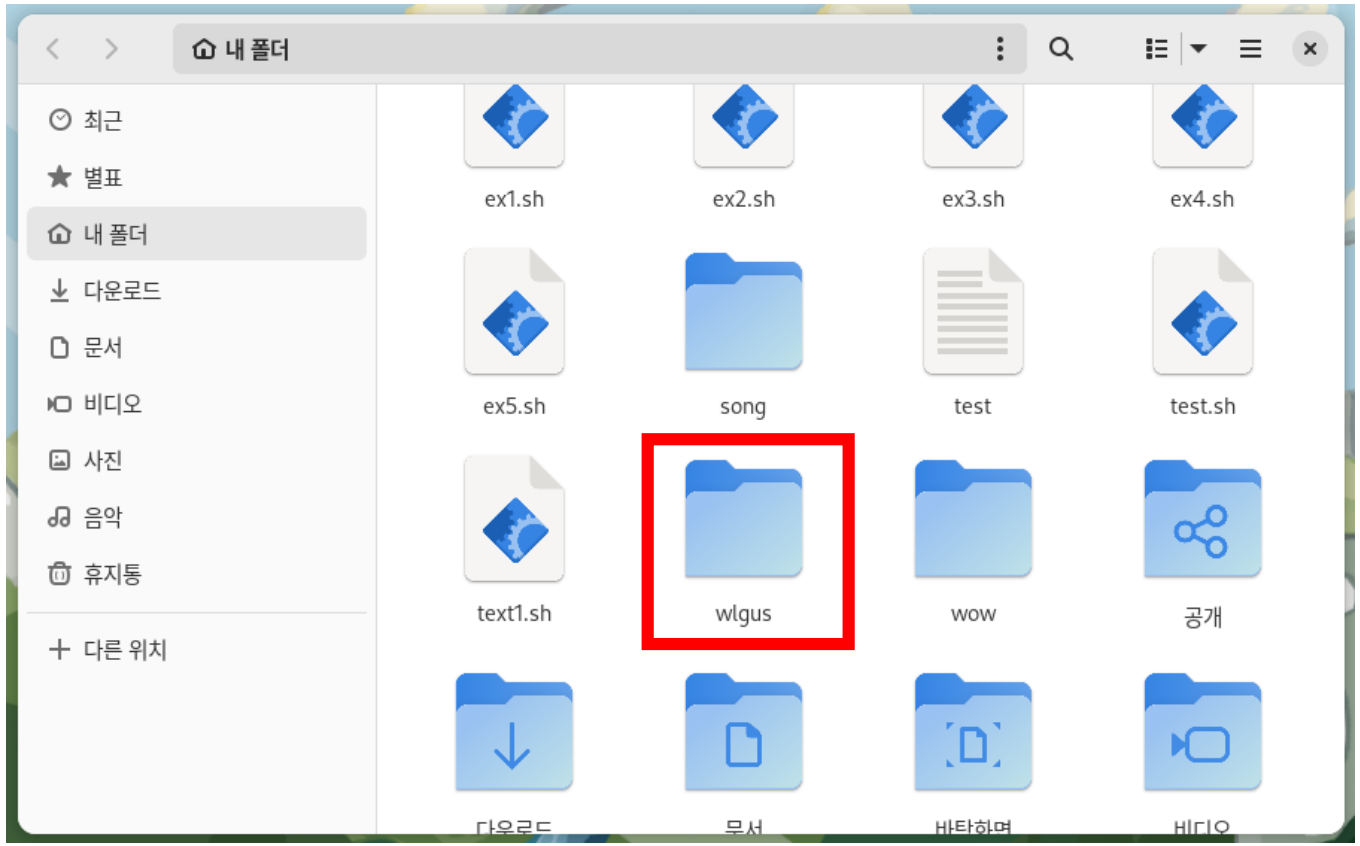
```
#include <stdio.h>

int main(int argc, char* argv[])
{
        char buf[100];
        strcpy(buf, argv[1]);
        printf(buf);
        return 0;
}
~
```

FSB의 실습

```
[jini@fedora wlgus]$ gcc -o apple apple.c
```

```
[jini@fedora wlgus]$ ls
apple   apple.c
```

FSB의 실습



apple

apple.c

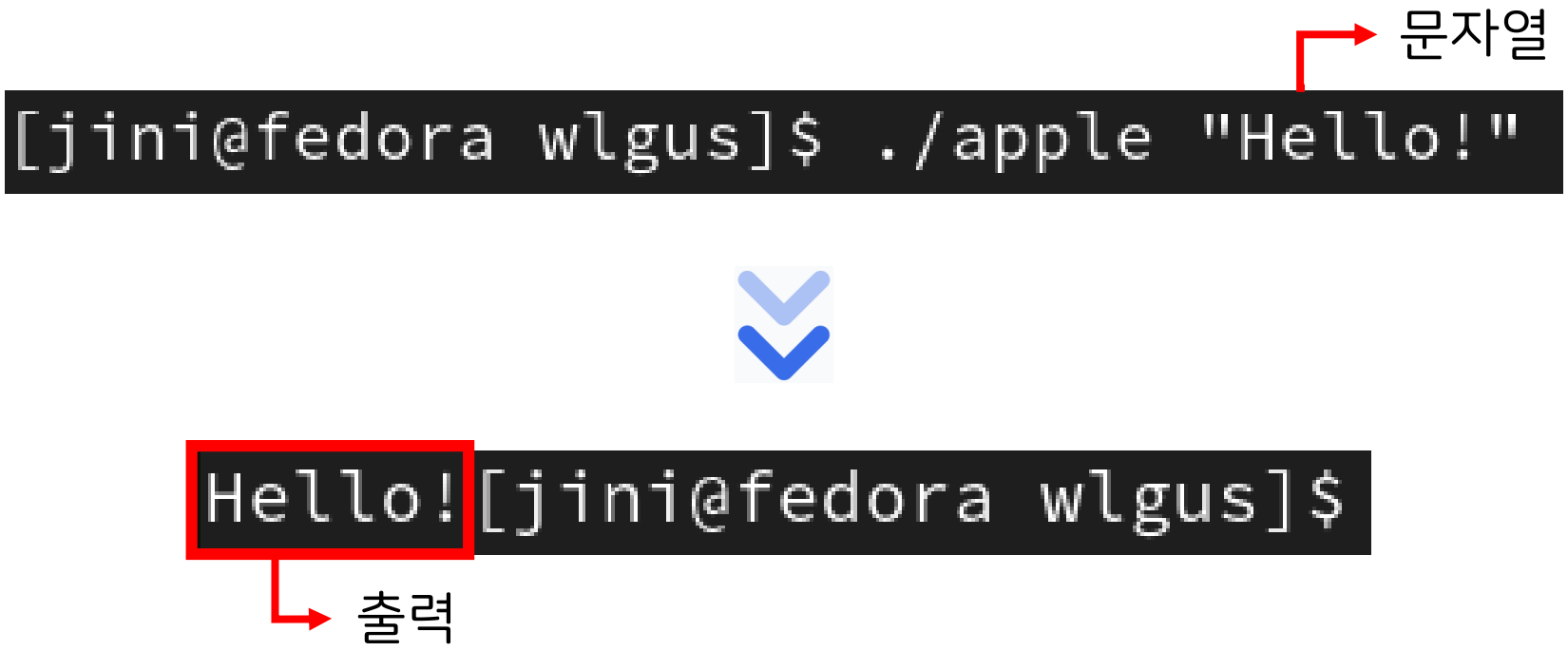
FSB의 실습

apple

apple.c

```c
#include <stdio.h>

int main(int argc, char* argv[])
{
        char buf[100];
        strcpy(buf, argv[1]);
        printf(buf);
        return 0;
}
```

FSB의 실습


문자열 입력
[jini@fedora wlgus]$ ./apple "Hello!"
Hello![jini@fedora wlgus]$
출력

FSB의 실습

포맷 문자열

```
[jini@fedora wlgus]$ ./apple "%x"
```

```
f3f22404[jini@fedora wlgus]$
```

스택 메모리에 저장된 값 출력

FSB의 실습 결과

서식 문자열을 사용자 입력에서 받아 처리하는 경우

서식 문자열에 따라 스택 메모리에 있는 값 노출시키는 취약점 발생

FSB의 실습 - 2

```c
#include <stdio.h>

int main()
{
    char buf[256];

    printf("이름 내놔 : ");
    scanf_s("%s", &buf);
    printf("Hiyo, ");

    printf(buf);
    printf("\n");

    return 0;
}
```

사용자 입력 그대로 출력

Format string을 입력하면 format string bug 발생

FSB의 실습 - 2

Format string으로 인식

해당 메모리 주소에 있는 값 출력

FSB의 실습 - 2

메모리 덤프(memory dump)

메모리 덤프에서 발견된 것, 보통 프로그램의 스택 메모리 영역에 저장된 데이터

Format string bug와 같은 취약점을 이용

메모리 상의 다른 데이터를 읽거나 조작 가능

FSB의 실습 - 2

```c
#include <stdio.h>

int main()
{
    char buf[256];

    printf("이름 내놔 : ");
    scanf_s("%s", &buf);
    printf("Hiyo, ");

    printf(buf);
    printf("\n");

    return 0;
}
```

```c
printf("%s", buf);
```

Format string을 명시적으로 지정

Q & A

감사합니다