

Abstraction example - Integers

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Variable semantics

- What does the following line of code do?

```
unsigned k = 0;
```

Assignment Project Exam Help

- Allocates space for the variable <https://powcoder.com>

- Associates the space with a variable [Add WeChat powcoder](#)

- Defines how the variable is interpreted

- Initialises the storage

Let's test this

Example

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

```
int main() {  
    int i;  
    int sum = 0;  
  
    for (i = 0; i < 10; i++)  
        sum += i;  
  
    printf("The sum is %d\n", sum);  
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

```
_main:
```

```
    pushq    %rbp  
    movq     %rsp, %rbp  
    leaq     L_.str(%rip), %rdi  
    movl     $45, %esi  
    xorl     %eax, %eax  
    callq    _printf  
    xorl     %eax, %eax  
    popq     %rbp  
    retq
```

```
L_.str:
```

```
    .asciz   "The sum is %d\n"
```

Compiler abstractions

- The compiler generates a **concrete implementation** of an **abstract program** description
- Preserves semantics (to some extent)
- Changes implementation details
 - May not match intuition
- We need to understand the abstraction

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Unsigned integers

- What is the output from:

\$ count 4

\$ count 2949

\$ count 67295

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

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

int main(int c, char **v) {
    unsigned i, n;

    n = strtoul(v[1], NULL, 0);

    for (i = n; i < n+10; i++)
        printf("%u\n", i);
}
```

Unsigned Integer Representation

- Collection

- Representation

- n dependent

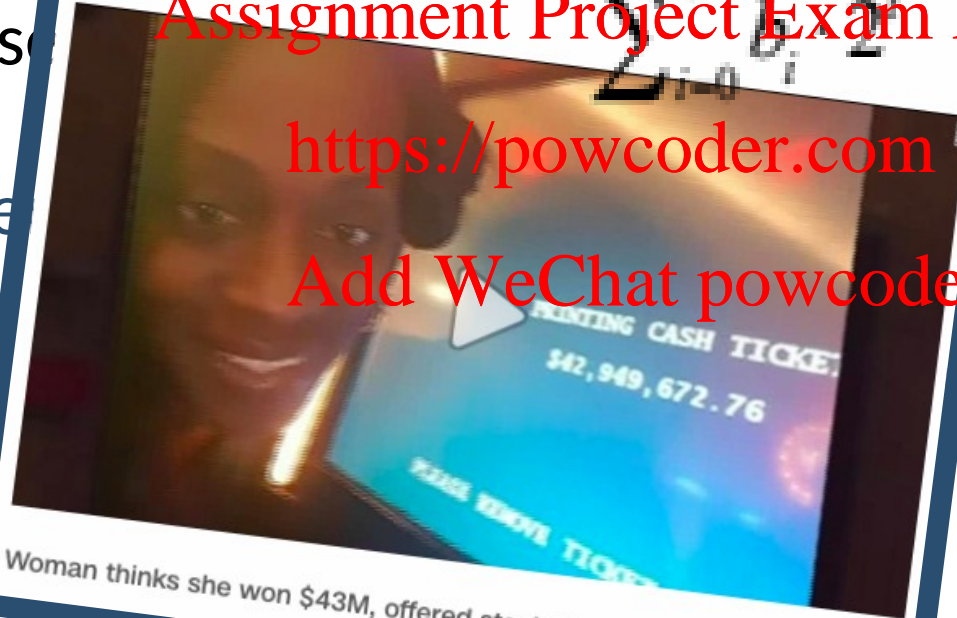
- An overview

- All a

Woman denied \$43 million jackpot, offered steak dinner instead

By Sophie Lewis, CNN

Updated 1553 GMT (2353 HKT) November 2, 2016



Woman thinks she won \$43M, offered steak dinner instead 02:08

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

implementation

ger than 2^n

Signed Integers

- One sign bit s and $n-1$ value bits $b_0 \dots b_{n-2}$
- Three possible interpretations:
 - Sign magnitude $(1-2s) \sum_{i=0}^{n-2} b_i \cdot 2^i$
 - Ones' complement $(1-2s) \sum_{i=0}^{n-2} (b_i \oplus s) \cdot 2^i$
 - Two's complement $\sum_{i=0}^{n-2} b_i \cdot 2^i + s \cdot 2^{n-1}$
- Most modern processors use two's complement

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Signed integer overflow

- Undefined behaviour

- Use modulo 2^{n-1} arithmetic

- Return maximum or minimum values

- Return zero

- Do nothing

- Cause a trap

- Launch \$500M fireworks

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Integer overflow vulnerabilities

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The screenshot shows a Forbes article page. At the top is the Forbes logo and a banner with the text "A LIFETIME OF BENEFITS." and an image of a classical building facade. The article title is "Stagefright: It Only Takes One Text To Hack 950 Million Android Phones". The author is Thomas Fox-Brewster, a Forbes Staff member, with a profile picture and publication date of Jul 27, 2015, 06:00am, and 145,299 views. Below the title, there are social media sharing icons for Facebook and Twitter. The article text begins with "Six critical vulnerabilities have left 95 per cent of Google" followed by a stock price ticker "GOOGL +1.47%". To the right of the article is a video player showing two women talking. Below the video is an advertisement for Hewlett Packard Enterprise and Intel, featuring a server rack and the text "3PAR All-Flash" and "The only storage to guarantee 99.99%".

Forbes

A LIFETIME OF BENEFITS.

Stagefright: It Only Takes One Text To Hack 950 Million Android Phones

Thomas Fox-Brewster Forbes Staff
Jul 27, 2015, 06:00am • 145,299 views

f

Google GOOGL +1.47%

Six critical vulnerabilities have left 95 per cent of Google Android phones open to an attack delivered by a simple multimedia text, a

Hewlett Packard Enterprise intel

3PAR All-Flash

The only storage to guarantee 99.99%

Make storage

*For more d

Stagefright

- Before

```
uint8_t *buffer = new (std::nothrow) uint8_t[size + chunk_size];  
if (buffer == NULL) {  
    return ERROR_MALFORMED;  
}
```

Assignment Project Exam Help

Why not use

`chunk_size + size >= SIZE_MAX ?`

- After

```
if (SIZE_MAX - chunk_size <= size) {  
    return ERROR_MALFORMED;  
}
```

<https://powcoder.com>

Add WeChat powcoder

```
uint8_t *buffer = new uint8_t[size + chunk_size];  
if (buffer == NULL) {
```

Type Conversion

```
bool isValidAddition(uint16_t x, uint16_t y)
{
    if (x + y < x)
        return false;
    return true;
}
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

```
if ((uint16_t) (x + y) < x)
```

CVE-2017-7602 (LibTIFF)

ma is positive

```
ma=(tmsize_t)td->td_striposffset[strip];  
mb=ma+size;
```

mb >= size
(overflow ignored)

```
if ((td->td_striposffset[strip] > (uint64)TIFF_TMSIZE_T_MAX) || (ma>tif->tif_size))  
    n=0;  
else if ((mb<ma) || (mb<size) || (mb>tif->tif_size))  
    n=tif->tif_size-ma;  
else  
    n=size;
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

test removed!

Fix: test for overflow

```
if ((td->td_stripoffset[strip] > (uint64)TIFF_TMSIZE_T_MAX)||  
    ((ma=(tmsize_t)td->td_stripoffset[strip])>tif->tif_size))  
{  
    n=0;  
}  
else if( ma > TIFF_TMSIZE_T_MAX - size )  
{  
    n=0;  
}  
else
```

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Best practices

- Know the language

- Undefined behaviours are dangerous

Assignment Project Exam Help

- Test user input for overflow

<https://powcoder.com>

- Special attention to input that affects allocation

- Use safe tests

Add WeChat powcoder

- Subtract from maximum

- Use explicit casts when using types smaller than `int`

Language Support

- Java:
 - `Math.multiplyExact`, `Math.addExact`, etc.
- C/C++ compilers:
 - `-fwrapv`, `-ftrapv`
 - `-fsanitize`
- C#
 - `checked`

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder