

#UnderhandedAppSec

Alexey Goncharov
[@alyoshapotter](#)

$$2+2=5$$


Write a program that *seemingly* adds the numbers 2 and 2 and outputs 5

5th

C#

```
using System;
namespace TwoPlusTwo
{
    class Calc
    {
        static void Main(string[] args)
        {
            var x = 2;
            var y = 2;
            // This will never happen
            if (1 == 0) ;
            {
                ++x;
            }
            Console.WriteLine(x + y);
        }
    }
}
```

5

```
using System;
namespace TwoPlusTwo
{
    class Calc
    {
        static void Main(string[] args)
        {
            var x = 2;
            var y = 2;
            // This will never happen
            if (1 == 0) ; 
            {
                ++x;
            }
            Console.WriteLine(x + y);
        }
    }
}
```

4th

C

```
#include <stdio.h>

int main(void)
{
    int a=3, b=2;

    printf("%d + %d = %d", --a, b, a + b);
}
```

```
$ ./twoplustwo
2 + 2 = 5
```

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

```
int main(void)
```

```
{
```

```
    int a=3, b=2;
```

```
    // gcc evaluates the function parameters from right to left.
```

```
    // When a+b is evaluated, a is still 3.
```

```
    printf("%d + %d = %d", --a, b, a + b);
```

```
}
```


3rd

Bash

```
#!/usr/bin/env bash
```

```
v=2          #v is 2
v+=2         #v is 4
v=$((v*5))   #v is 20
v=$((v-16))  #v is 4
v=$(bc<<<"sqrt($v)+2") #v is 4 (sqrt(4) is 2)
v=$(bc<<<"$v/4+3")    #v is 4 (4/4 = 1)
echo '2 + 2 =' $v     #So v is 4...?
```

```
$ ./twoplustwo.sh
2 + 2 = 5
```

```
#!/usr/bin/env bash
# The second line concatenates v and 2 instead of adding them, to make 22.
v=2                                #v is 2
v+=2                                #v is 22
v=$((v*5))                         #v is 110
v=$((v-16))                        #v is 94
v=$(bc<<<"sqrt($v)+2")             #v is 11 (by default bc rounds to integers)
v=$(bc<<<"$v/4+3")                 #v is 5 (11/4 = 2 with rounding)
echo '2 + 2 =' $v                  #TADAAAAM!
```

More fun with CLI: <https://twitter.com/climagic>

2nd

Python

```
#!/usr/bin/env python
```

```
patch = '\x31\x2D7'
```

```
import ctypes
```

```
ctypes.c_int8.from_address(id(len(patch)) + 16).value = eval(patch)
```

```
print('2+2=', 2 + 2)
```

```
$ python two_plus_two.py  
( '2+2=', 5)
```

```
#!/usr/bin/env python
```

```
patch = '\x31\x2D7' # 12-7
```

```
import ctypes
```

```
# CPython uses the same memory location for any copy of the first few small integers.
```

```
# This goes in and directly edits that memory location via ctypes.
```

```
ctypes.c_int8.from_address(id(len(patch)) + 16).value = eval(patch)
```

```
print('2+2=', 2 + 2)
```

1st

Java

```
public class TwoPlusTwo {  
    // 20 * .1 = 2  
    private static double two() {  
        double two = 0;  
        for(int i = 0; i < 20; i++) {  
            two += .1;  
        }  
        return two;  
    }  
  
    public static void main(String... args) {  
        double two = two();  
        System.out.format("Variable two = %.15f%n", two);  
        double four = Math.ceil(two + two); // round just in case  
        System.out.format("two + two = %.15f%n", four);  
    }  
}
```

```
$ java TwoPlusTwo  
Variable two = 2,000000000000000  
two + two = 5,000000000000000
```



```
public class TwoPlusTwo {
    // 20 * .1 = 2
    private static double two() {
        double two = 0;
        for(int i = 0; i < 20; i++) {
            // Doubles are stored in base 2 internally.
            // Only fractions where the denominator is a 2^N have a finite number of "decimals".
            // 1/10 for example is .001100110011... in base 2
            // Use class BigDecimal to avoid round problems
            two += .1;
        }
        return two;
    }

    public static void main(String... args) {
        double two = two();
        // 15 isn't enough digits to show that the two() actually produces 2.0000000000000004
        System.out.format("Variable two = %.15f\n", two);
        double four = Math.ceil(two + two); // round just in case
        System.out.format("two + two = %.15f\n", four);
    }
}
```

More about double in Java
<https://habrahabr.ru/post/219595/>

More examples:

<http://codegolf.stackexchange.com/questions/28786/write-a-program-that-makes-2-2-5>

Alexey Goncharov
@alyoshapotter
#underhandedappsec