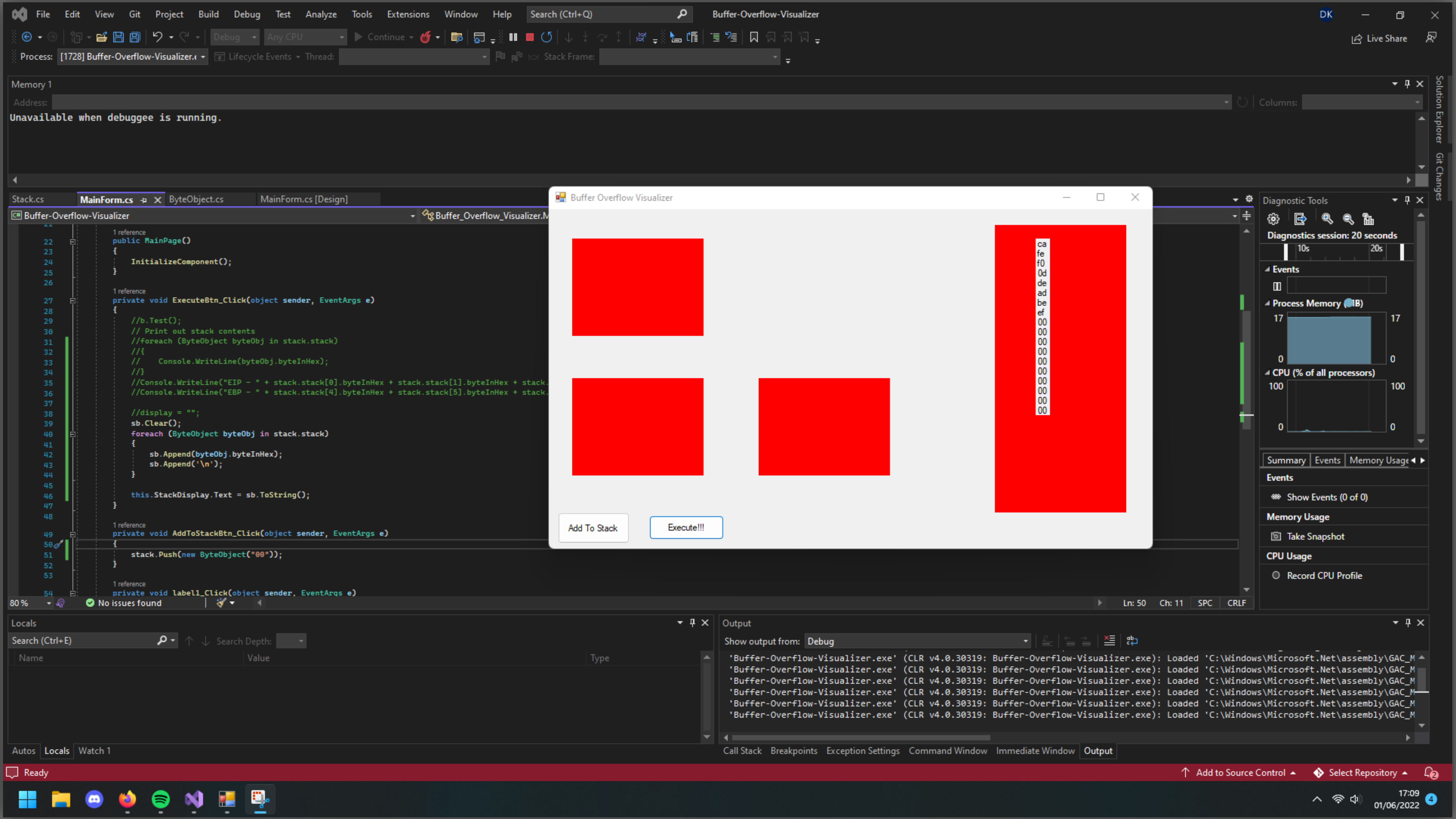
Buffer Overflow Visualizer

Python Tkinter Project

Devlog

1st June 2022 (01/06/2022)



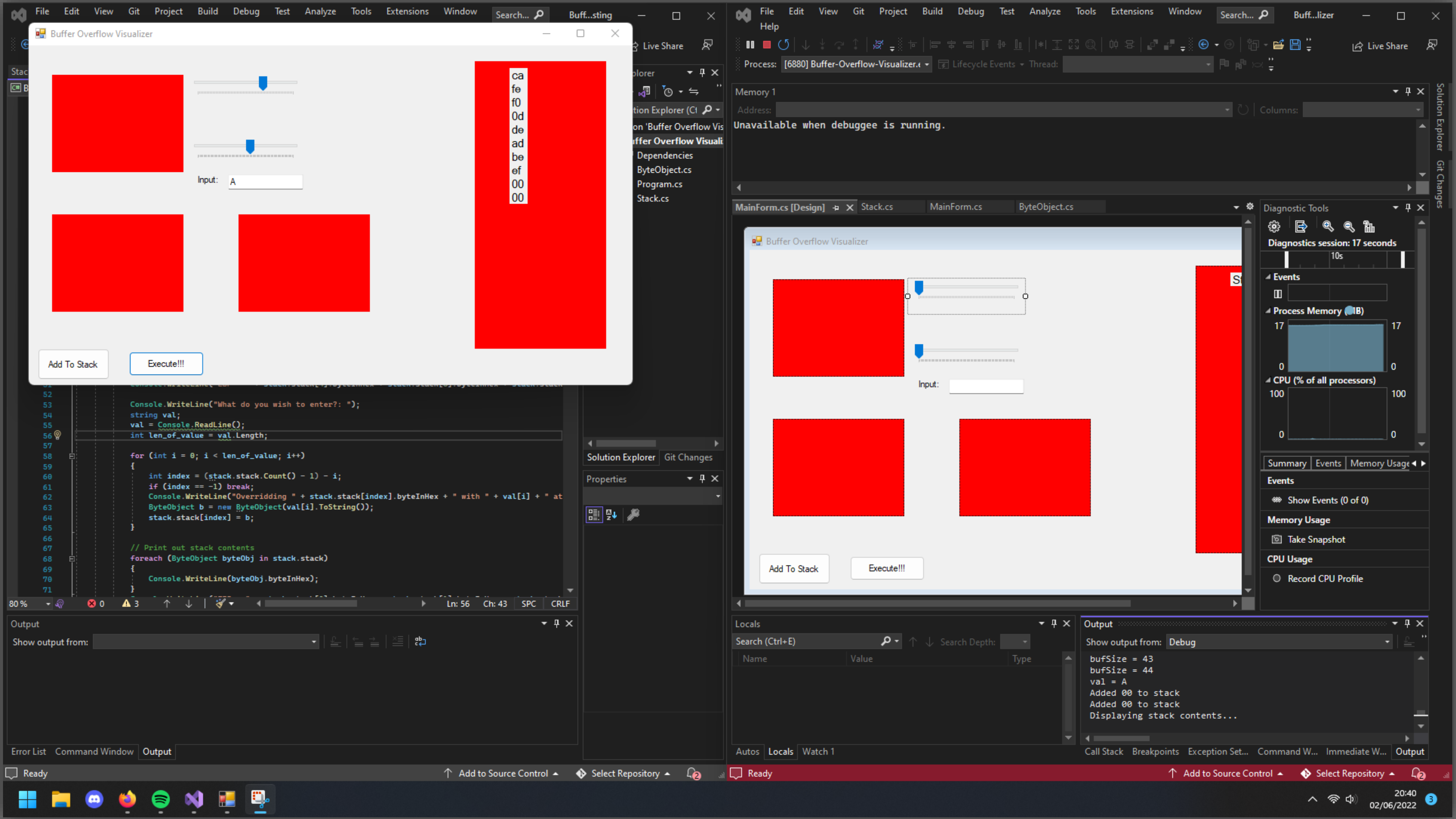
```
Unavailable when debuggee is running.
```

```
        1 reference
        public MainPage()
        {
            InitializeComponent();
        }

        1 reference
        private void ExecuteBtn_Click(object sender, EventArgs e)
        {
            //b.Test();
            // Print out stack contents
            //foreach (ByteObject byteObj in stack.stack)
            //{
            //    Console.WriteLine(byteObj.byteInHex);
            //}
            //Console.WriteLine("EIP - " + stack.stack[0].byteInHex + stack.stack[1].byteInHex + stack.
            //Console.WriteLine("EBP - " + stack.stack[4].byteInHex + stack.stack[5].byteInHex + stack.

            //display = "";
            sb.Clear();
            foreach (ByteObject byteObj in stack.stack)
            {
                sb.Append(byteObj.byteInHex);
                sb.Append('\n');
            }

            this.StackDisplay.Text = sb.ToString();
        }

        1 reference
        private void AddToStackBtn_Click(object sender, EventArgs e)
        {
            stack.Push(new ByteObject("00"));
        }

        1 reference
        private void label1_Click(object sender, EventArgs e)
```

```
ca
fe
f0
0d
de
ad
be
ef
00
00
00
00
00
00
00
00
00
00
```

```
'Buffer-Overflow-Visualizer.exe' (CLR v4.0.30319: Buffer-Overflow-Visualizer.exe): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_M
'Buffer-Overflow-Visualizer.exe' (CLR v4.0.30319: Buffer-Overflow-Visualizer.exe): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_M
'Buffer-Overflow-Visualizer.exe' (CLR v4.0.30319: Buffer-Overflow-Visualizer.exe): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_M
'Buffer-Overflow-Visualizer.exe' (CLR v4.0.30319: Buffer-Overflow-Visualizer.exe): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_M
'Buffer-Overflow-Visualizer.exe' (CLR v4.0.30319: Buffer-Overflow-Visualizer.exe): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_M
'Buffer-Overflow-Visualizer.exe' (CLR v4.0.30319: Buffer-Overflow-Visualizer.exe): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_M
```

2nd June 2022 (02/06/2022)



```
ca
fe
f0
0d
de
ad
be
ef
00
00
```

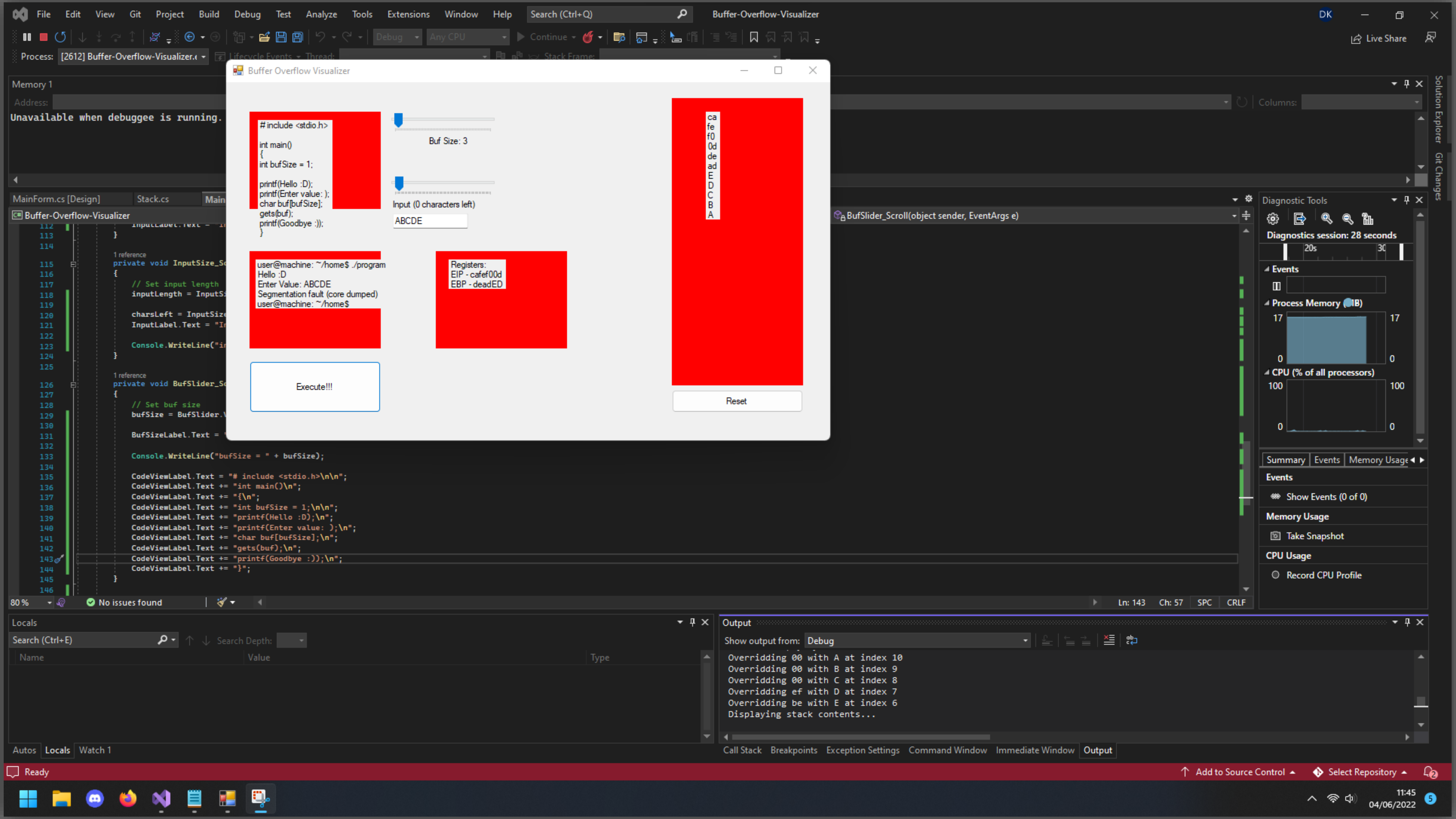
Unavailable when debuggee is running.

```
Console.WriteLine("What do you wish to enter?: ");
string val;
val = Console.ReadLine();
int len_of_value = val.Length;

for (int i = 0; i < len_of_value; i++)
{
    int index = (stack.stack.Count() - 1) - i;
    if (index == -1) break;
    Console.WriteLine("Overridding " + stack.stack[index].byteInHex + " with " + val[i] + " at
    ByteObject b = new ByteObject(val[i].ToString());
    stack.stack[index] = b;
}

// Print out stack contents
foreach (ByteObject byteObj in stack.stack)
{
    Console.WriteLine(byteObj.byteInHex);
}
```

Show output from: Debug

```
bufSize = 43
bufSize = 44
val = A
Added 00 to stack
Added 00 to stack
Displaying stack contents...
```

4th June 2022 (04/06/2022)



Buffer Overflow Visualizer

```
# include <stdio.h>

int main()
{
int bufSize = 1;

printf(Hello :D);
printf(Enter value: );
char buf[bufSize];
gets(buf);
printf(Goodbye :));
}
```

Buf Size: 3

Input (0 characters left)

ABCDE

```
user@machine: ~/home$ ./program
Hello :D
Enter Value: ABCDE
Segmentation fault (core dumped)
user@machine: ~/home$
```

```
Registers:
EIP - cafef00d
EBP - deadED
```

```
ca
fe
f0
0d
de
ad
E
D
C
B
A
```

Execute!!!

Reset

Memory 1

Unavailable when debuggee is running.

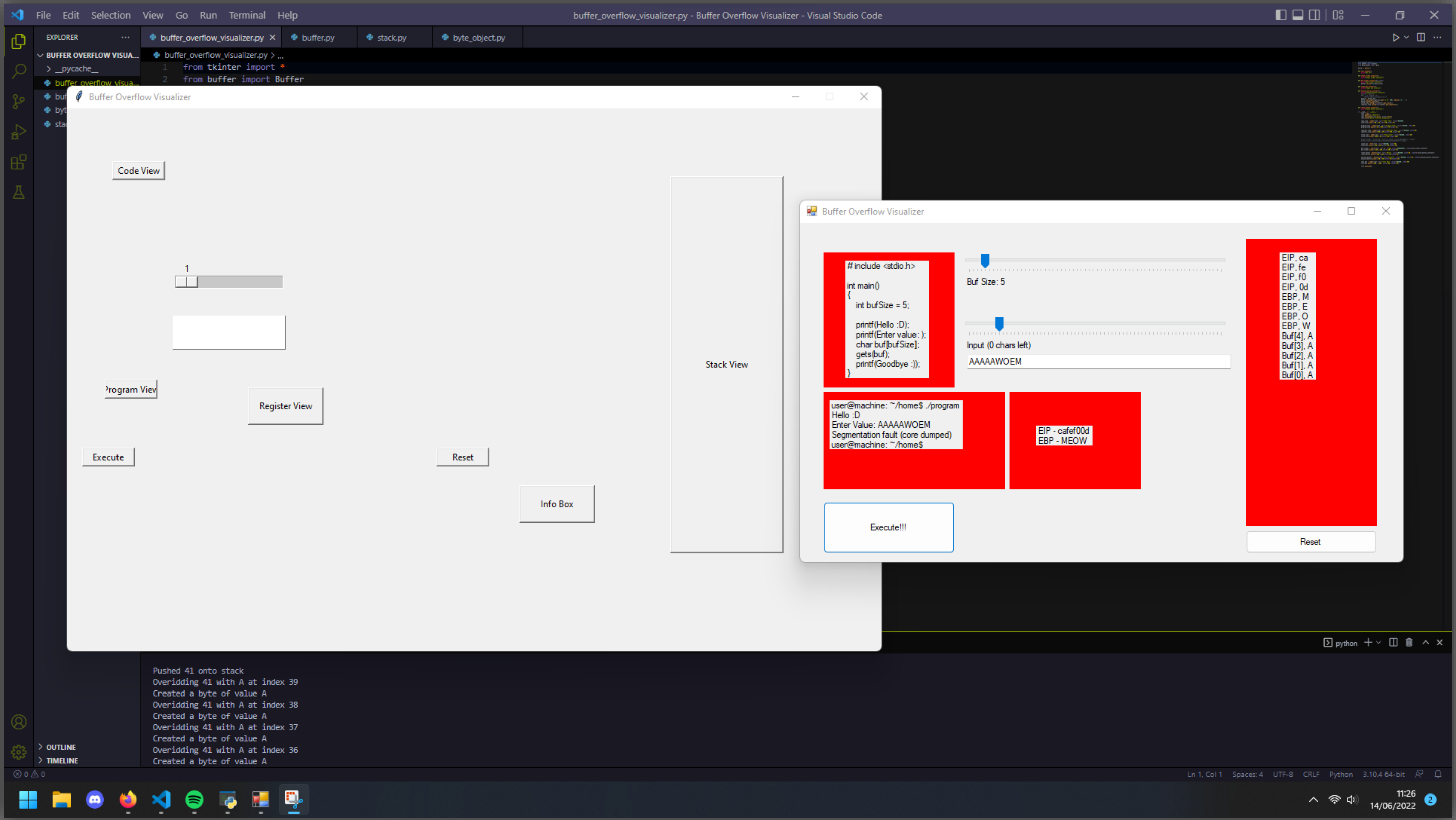
```
        }

        1 reference
        private void InputSize_Sc
        {
            // Set input length
            inputLength = InputSi

            charsLeft = InputSize
            InputLabel.Text = "In

            Console.WriteLine("in
        }

        1 reference
        private void BufSlider_Sc
        {
            // Set buf size
            bufSize = BufSlider.V

            BufSizeLabel.Text = "

            Console.WriteLine("bufSize = " + bufSize);

            CodeViewLabel.Text = "# include <stdio.h>\n\n";
            CodeViewLabel.Text += "int main()\n";
            CodeViewLabel.Text += "{\n";
            CodeViewLabel.Text += "int bufSize = 1;\n\n";
            CodeViewLabel.Text += "printf(Hello :D);\n";
            CodeViewLabel.Text += "printf(Enter value: );\n";
            CodeViewLabel.Text += "char buf[bufSize];\n";
            CodeViewLabel.Text += "gets(buf);\n";
            CodeViewLabel.Text += "printf(Goodbye :));\n";
            CodeViewLabel.Text += "}";
        }
```

Output — Show output from: Debug

```
Overridding 00 with A at index 10
Overridding 00 with B at index 9
Overridding 00 with C at index 8
Overridding ef with D at index 7
Overridding be with E at index 6
Displaying stack contents...
```

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
Buffer-Overflow-Visualizer
Process: [2612] Buffer-Overflow-Visualizer.e
MainForm.cs [Design]
Stack.cs
BufSlider_Scroll(object sender, EventArgs e)
Diagnostic Tools
Diagnostics session: 28 seconds
Process Memory (MB)
CPU (% of all processors)
Summary Events Memory Usage
Take Snapshot
Record CPU Profile
No issues found
Ln: 143 Ch: 57 SPC CRLF
Locals
Call Stack Breakpoints Exception Settings Command Window Immediate Window Output
Ready
Add to Source Control
Select Repository
11:45
04/06/2022

14th June 2022 (14/06/2022)



```python
from tkinter import *
from buffer import Buffer
```

```
1
```

```c
# include <stdio.h>

int main()
{
    int bufSize = 5;

    printf(Hello :D);
    printf(Enter value: );
    char buf[bufSize];
    gets(buf);
    printf(Goodbye :));
}
```

```
AAAAAWOEM
```

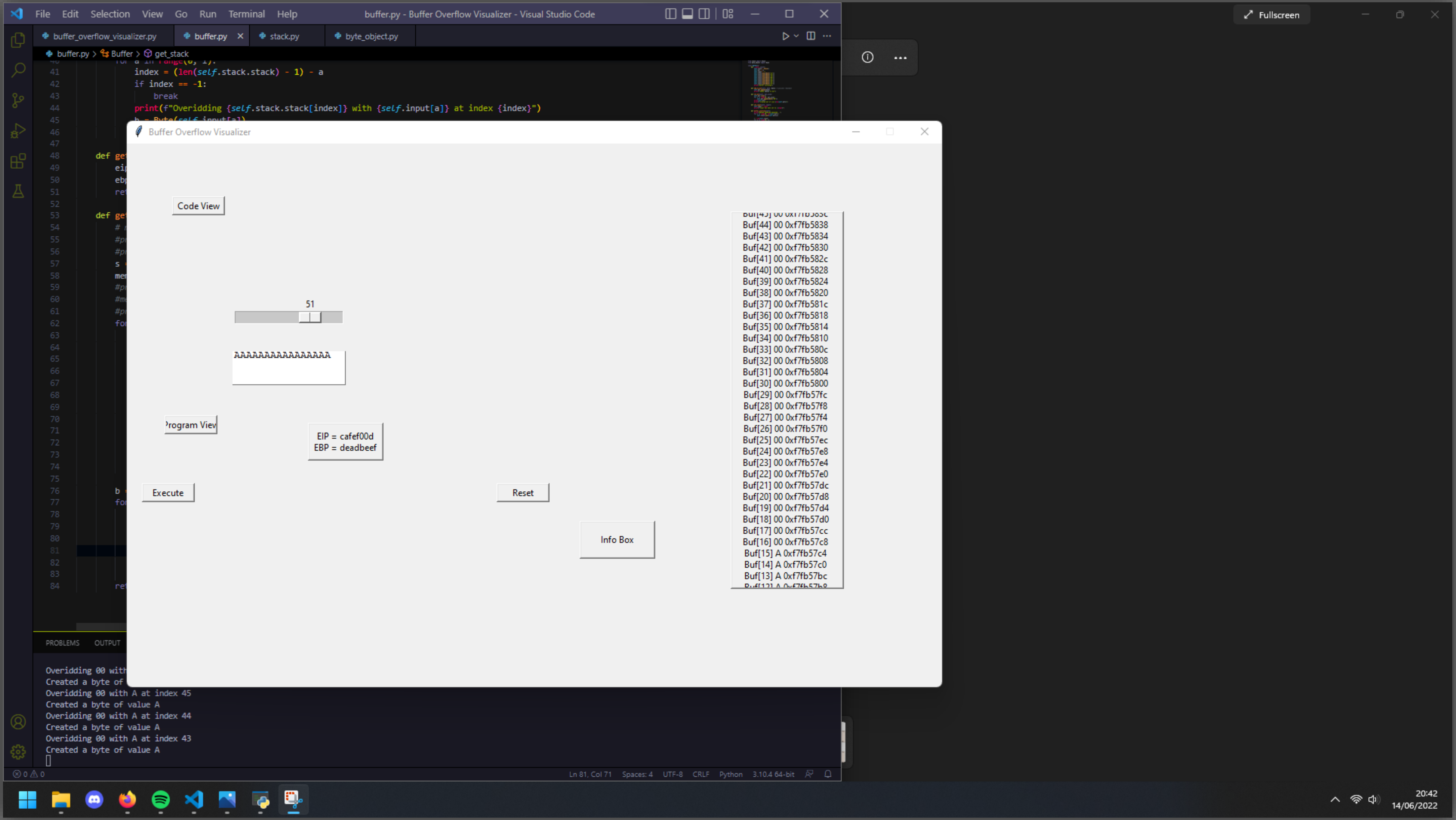
```
user@machine: ~/home$ ./program
Hello :D
Enter Value: AAAAAWOEM
Segmentation fault (core dumped)
user@machine: ~/home$
```

```
EIP - cafef00d
EBP - MEOW
```

```
EIP, ca
EIP, fe
EIP, f0
EIP, 0d
EBP, M
EBP, E
EBP, O
EBP, W
Buf[4], A
Buf[3], A
Buf[2], A
Buf[1], A
Buf[0], A
```

```
Pushed 41 onto stack
Overidding 41 with A at index 39
Created a byte of value A
Overidding 41 with A at index 38
Created a byte of value A
Overidding 41 with A at index 37
Created a byte of value A
Overidding 41 with A at index 36
Created a byte of value A
```

14th June 2022 (14/06/2022)



```
            index = (len(self.stack.stack) - 1) - a
            if index == -1:
                break
            print(f"Overidding {self.stack.stack[index]} with {self.input[a]} at index {index}")
```

51

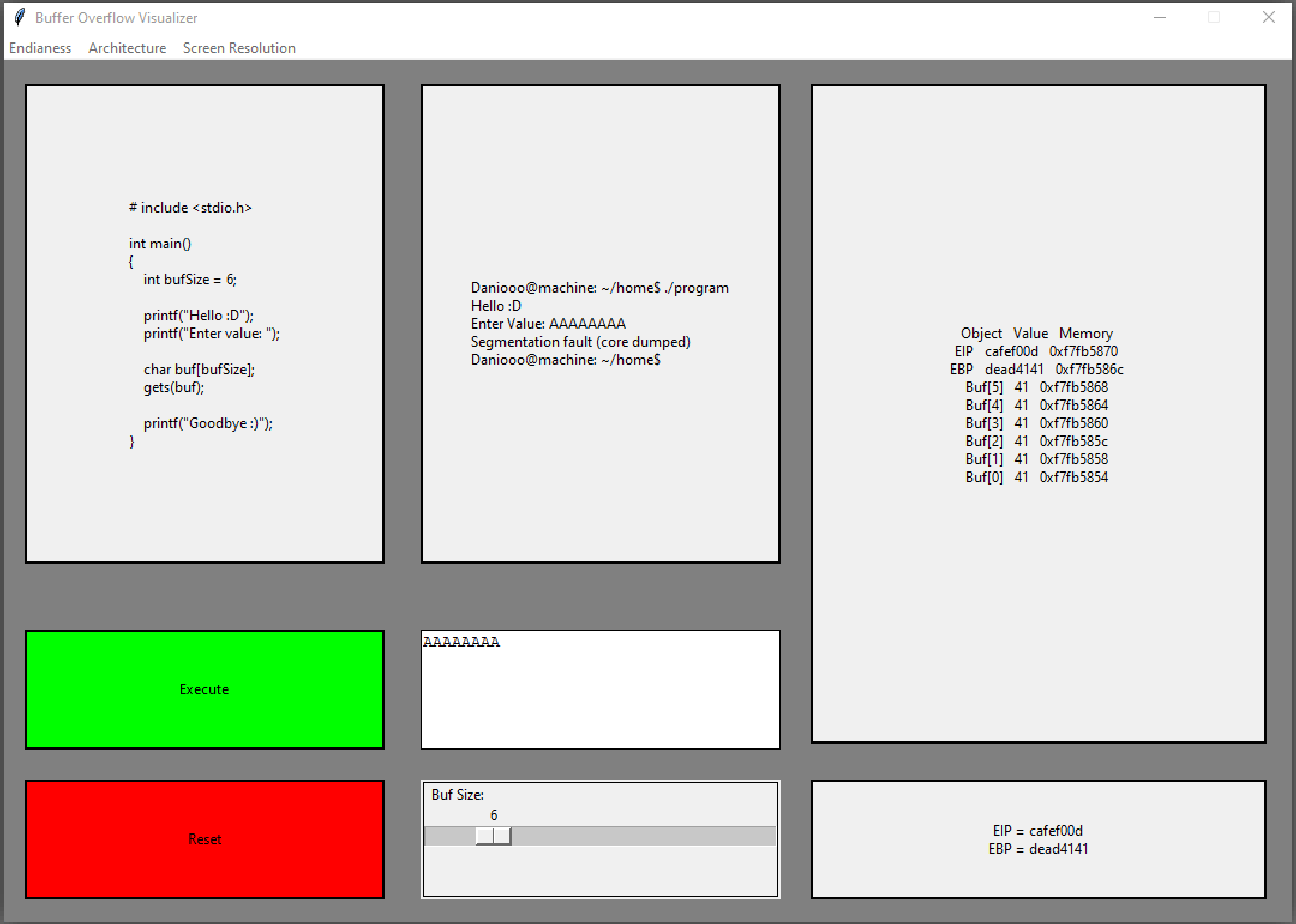
AAAAAAAAAAAAAAAA

EIP = cafef00d
EBP = deadbeef

```
Buf[44] 00 0xf7fb5838
Buf[43] 00 0xf7fb5834
Buf[42] 00 0xf7fb5830
Buf[41] 00 0xf7fb582c
Buf[40] 00 0xf7fb5828
Buf[39] 00 0xf7fb5824
Buf[38] 00 0xf7fb5820
Buf[37] 00 0xf7fb581c
Buf[36] 00 0xf7fb5818
Buf[35] 00 0xf7fb5814
Buf[34] 00 0xf7fb5810
Buf[33] 00 0xf7fb580c
Buf[32] 00 0xf7fb5808
Buf[31] 00 0xf7fb5804
Buf[30] 00 0xf7fb5800
Buf[29] 00 0xf7fb57fc
Buf[28] 00 0xf7fb57f8
Buf[27] 00 0xf7fb57f4
Buf[26] 00 0xf7fb57f0
Buf[25] 00 0xf7fb57ec
Buf[24] 00 0xf7fb57e8
Buf[23] 00 0xf7fb57e4
Buf[22] 00 0xf7fb57e0
Buf[21] 00 0xf7fb57dc
Buf[20] 00 0xf7fb57d8
Buf[19] 00 0xf7fb57d4
Buf[18] 00 0xf7fb57d0
Buf[17] 00 0xf7fb57cc
Buf[16] 00 0xf7fb57c8
Buf[15] A 0xf7fb57c4
Buf[14] A 0xf7fb57c0
Buf[13] A 0xf7fb57bc
```

```
Overidding 00 with
Created a byte of
Overidding 00 with A at index 45
Created a byte of value A
Overidding 00 with A at index 44
Created a byte of value A
Overidding 00 with A at index 43
Created a byte of value A
```

24th June 2022 (24/06/2022)



```c
# include <stdio.h>

int main()
{
    int bufSize = 6;

    printf("Hello :D");
    printf("Enter value: ");

    char buf[bufSize];
    gets(buf);

    printf("Goodbye :)");
}
```

```
Daniooo@machine: ~/home$ ./program
Hello :D
Enter Value: AAAAAAAA
Segmentation fault (core dumped)
Daniooo@machine: ~/home$
```

```
    Object  Value   Memory
  EIP   cafef00d  0xf7fb5870
 EBP   dead4141  0xf7fb586c
    Buf[5]  41   0xf7fb5868
    Buf[4]  41   0xf7fb5864
    Buf[3]  41   0xf7fb5860
    Buf[2]  41   0xf7fb585c
    Buf[1]  41   0xf7fb5858
    Buf[0]  41   0xf7fb5854
```

AAAAAAAA

Buf Size:
6

```
EIP = cafef00d
EBP = dead4141
```