Vladislav Sidorenko 192896IVSB

Lab 5

For my Lab work I picked up a challenge from hackthebox.eu/home/challenges/Reversing.

The name of the challenge was a **"Bypass"**. This is a CTF-like challenge that was released on the 6th of March 2020.

Description of the challenge is the following:
The Client is in full control. Bypass the authentication and read the key to get the Flag.

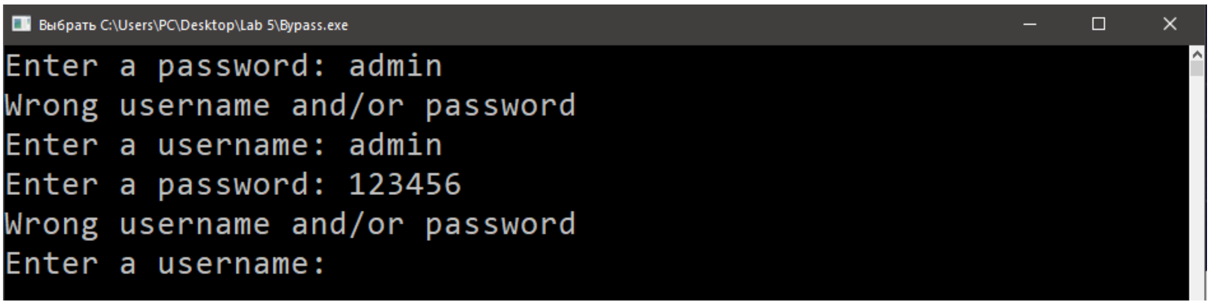
To decide what tools to use I referred to this write-up
https://medium.com/swlh/hack-the-boxdwriteup-rev-1-a94282cb0c63

Tools

1. ILSpy Decompiler https://github.com/icsharpcode/ILSpy/
2. Reflexil assembly editor, runs as a plugin for ILSpy https://github.com/sailro/Reflexil

Solution

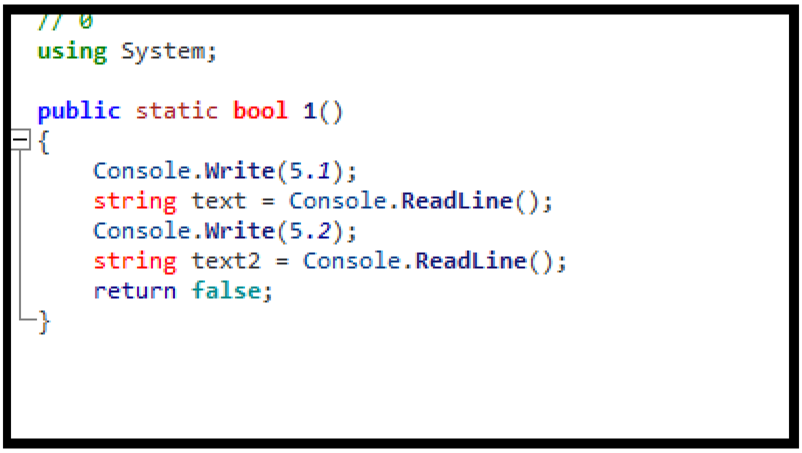
My first step was to execute the program



```
Enter a password: admin
Wrong username and/or password
Enter a username: admin
Enter a password: 123456
Wrong username and/or password
Enter a username:
```

It seems like there is nothing to do in command prompt yet, let's try using our tools.
Run ILSpy and open the file **bypass.exe.**
I've analyzed the headers and the whole structure of this file and came to a conclusion that the part we need to work with is most probably in the "Module:0" section.

The function we seem to interact with is this one:

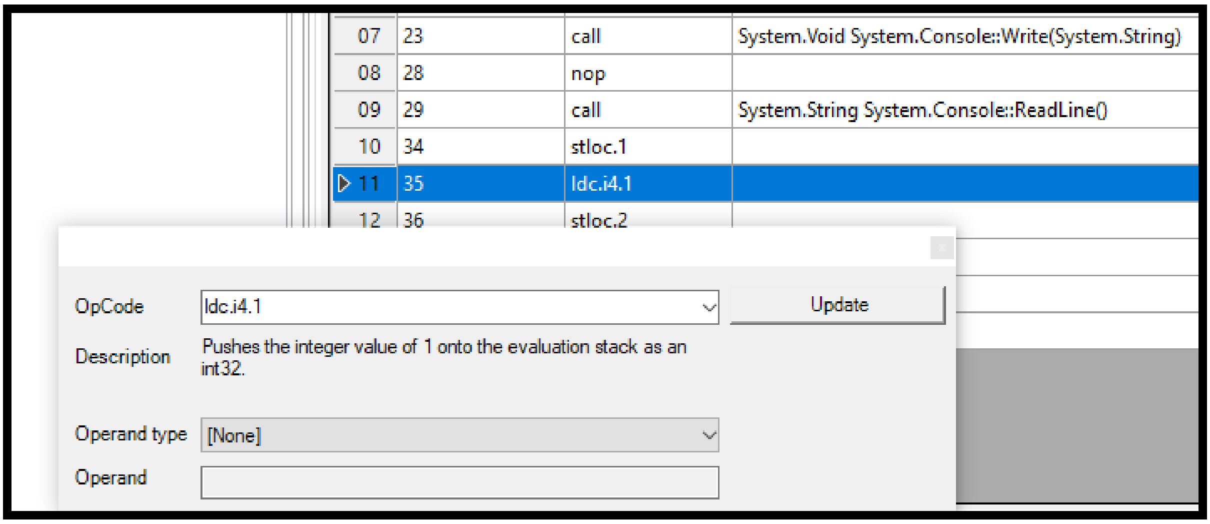


```
// 0
using System;

public static bool 1()
{
    Console.Write(5.1);
    string text = Console.ReadLine();
    Console.Write(5.2);
    string text2 = Console.ReadLine();
    return false;
}
```

Here, the console writes something and then takes the input (username), same for password, and then it returns boolean **false.** We can try to change **false** to **true**. For that we have to open a Reflexil plugin with a gearwheel button at the top of ILSpy.

We are interested in **idc.i4.0** value, changing it to anything between **idc.i4.1** and **idc.i4.8** will work.



07	23	call	System.Void System.Console::Write(System.String)
08	28	nop	
09	29	call	System.String System.Console::ReadLine()
10	34	stloc.1	
11	35	ldc.i4.1	
12	36	stloc.2	

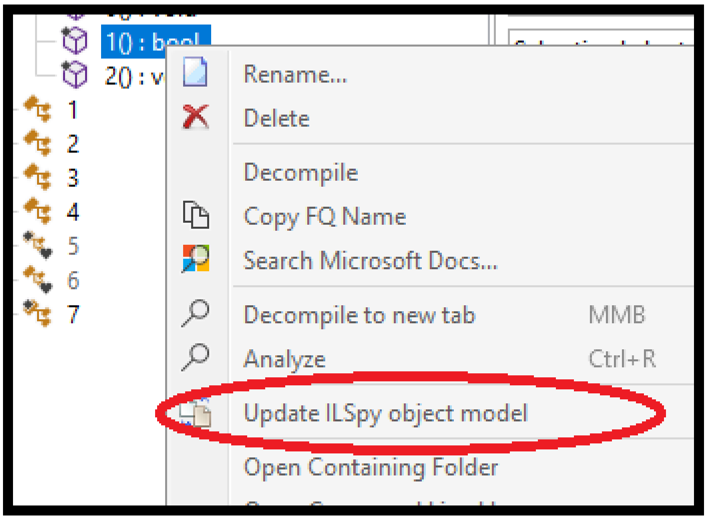
OpCode: ldc.i4.1

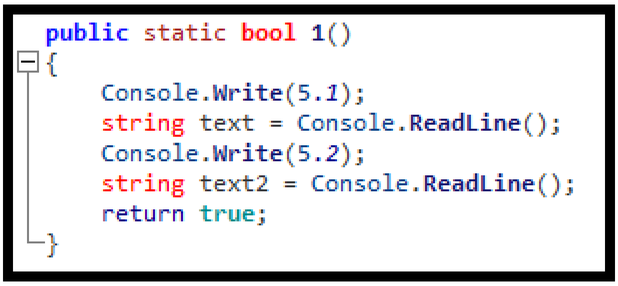
Description: Pushes the integer value of 1 onto the evaluation stack as an int32.

Operand type: [None]

Operand:

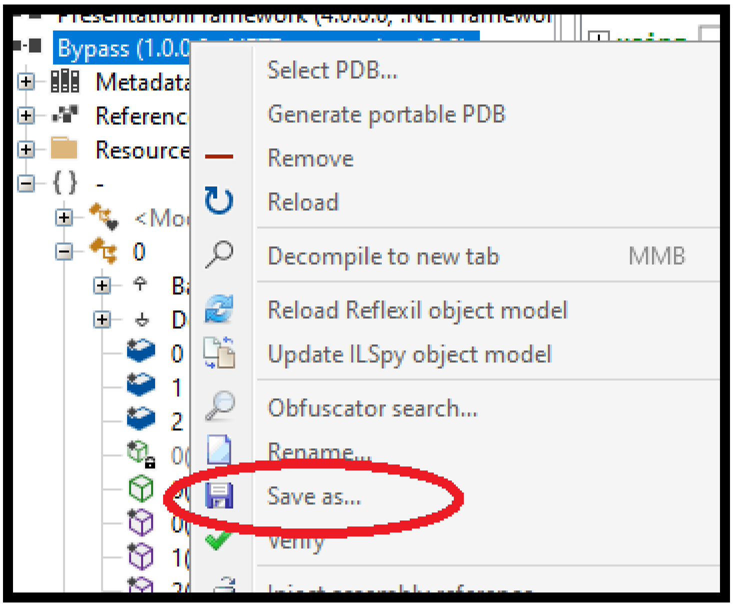
Now update the code, **return** value should now be **“true”**.

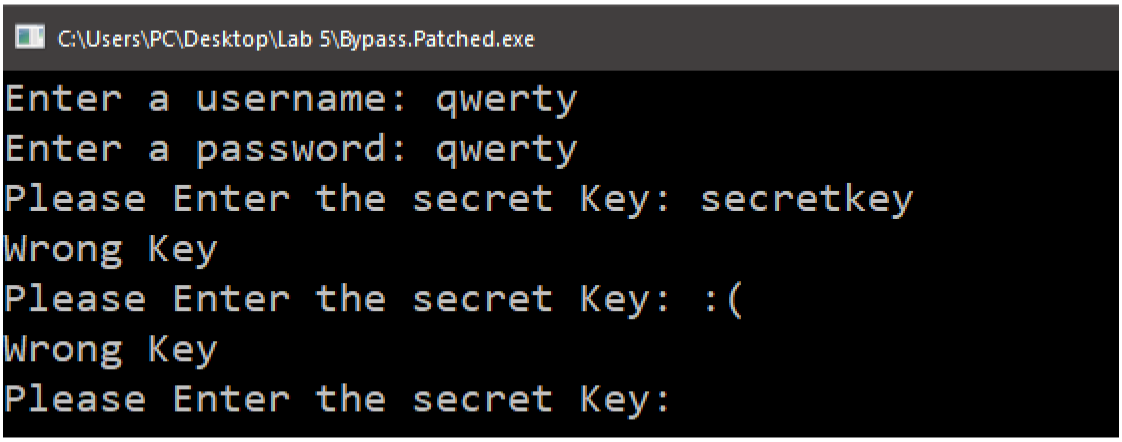




```
public static bool 1()
{
    Console.Write(5.1);
    string text = Console.ReadLine();
    Console.Write(5.2);
    string text2 = Console.ReadLine();
    return true;
}
```

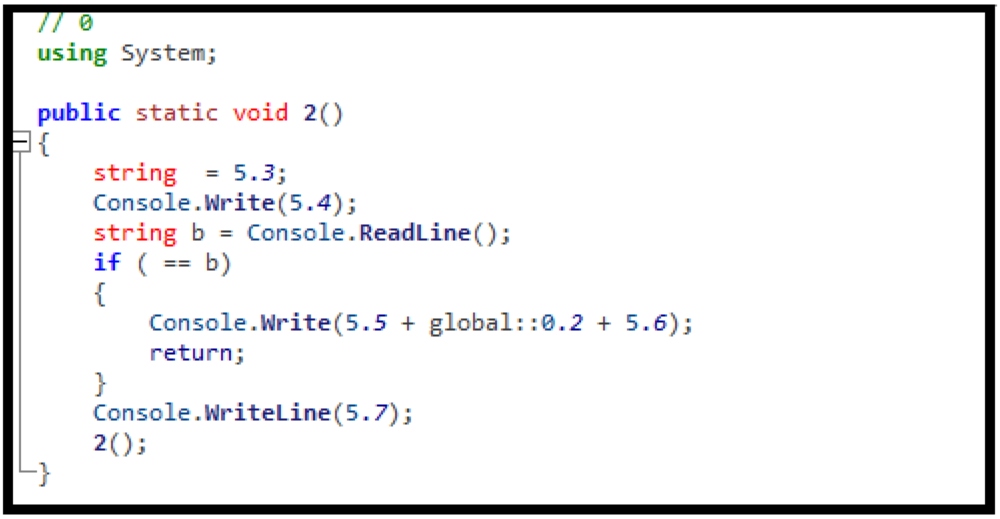
We can now save our program with the update code and run it.





```
Enter a username: qwerty
Enter a password: qwerty
Please Enter the secret Key: secretkey
Wrong Key
Please Enter the secret Key: :(
Wrong Key
Please Enter the secret Key:
```

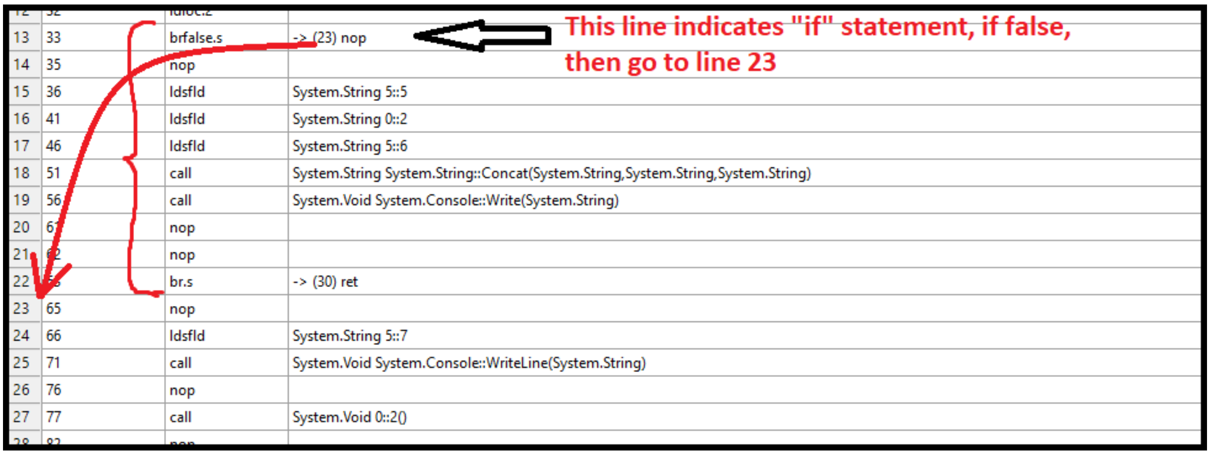
Now our program asks us to enter a secret key, so let’s continue changing the code.



```
// 0
using System;

public static void 2()
{
    string  = 5.3;
    Console.Write(5.4);
    string b = Console.ReadLine();
    if ( == b)
    {
        Console.Write(5.5 + global::0.2 + 5.6);
        return;
    }
    Console.WriteLine(5.7);
    2();
}
```

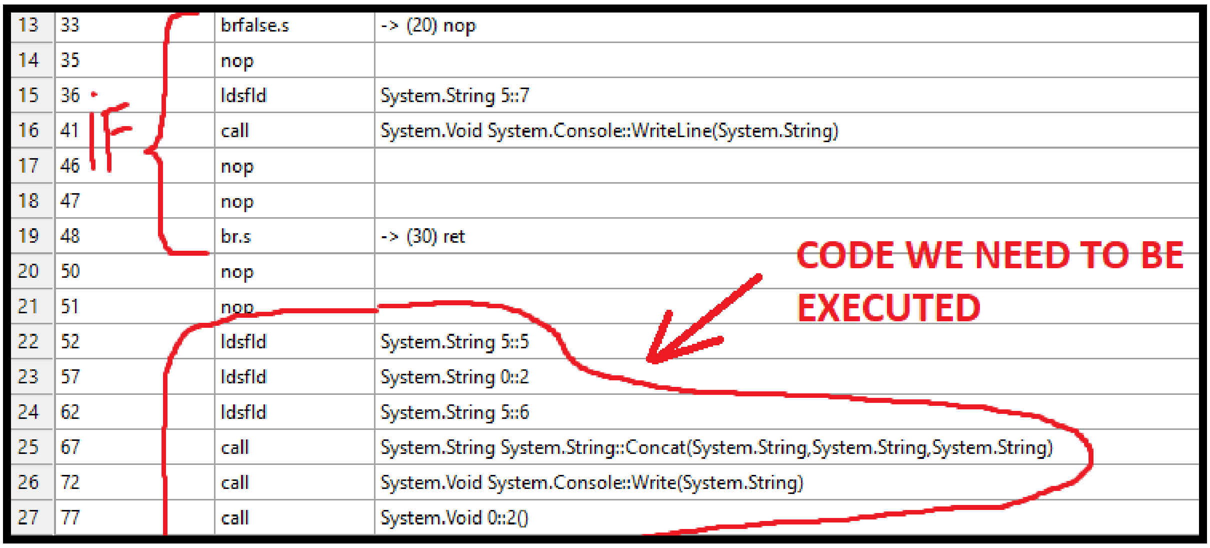
I’m sure there are different ways around, but here’s mine.
The code lines before change:



12	32	ldloc.2	
13	33	brfalse.s	-> (23) nop
14	35	nop	
15	36	ldsfld	System.String 5::5
16	41	ldsfld	System.String 0::2
17	46	ldsfld	System.String 5::6
18	51	call	System.String System.String::Concat(System.String,System.String,System.String)
19	56	call	System.Void System.Console::Write(System.String)
20	61	nop	
21	62	nop	
22	63	br.s	-> (30) ret
23	65	nop	
24	66	ldsfld	System.String 5::7
25	71	call	System.Void System.Console::WriteLine(System.String)
26	76	nop	
27	77	call	System.Void 0::2()
28	82	nop	

This line indicates "if" statement, if false, then go to line 23

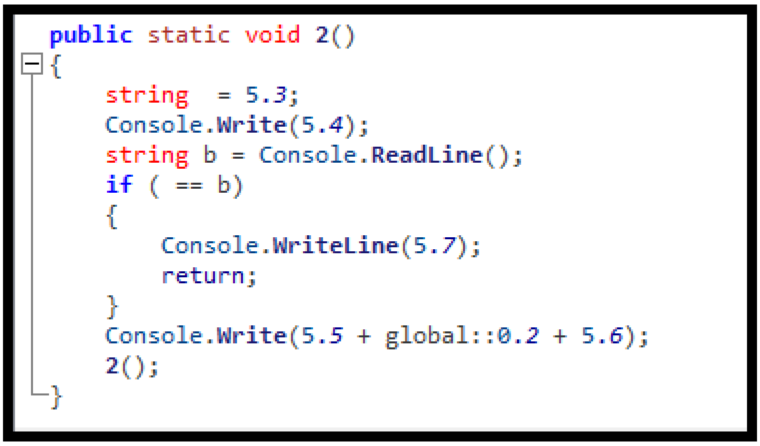
After the change:



13	33	brfalse.s	-> (20) nop
14	35	nop	
15	36	ldsfld	System.String 5::7
16	41	call	System.Void System.Console::WriteLine(System.String)
17	46	nop	
18	47	nop	
19	48	br.s	-> (30) ret
20	50	nop	
21	51	nop	
22	52	ldsfld	System.String 5::5
23	57	ldsfld	System.String 0::2
24	62	ldsfld	System.String 5::6
25	67	call	System.String System.String::Concat(System.String,System.String,System.String)
26	72	call	System.Void System.Console::Write(System.String)
27	77	call	System.Void 0::2()

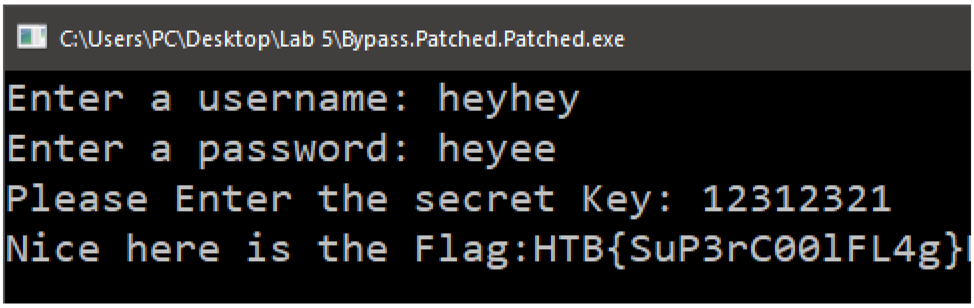
CODE WE NEED TO BE EXECUTED

Basically I moved our desired code out of the “if” statement and replaced it with the code we don’t need.
Updated code looks like this now.



```
public static void 2()
{
    string  = 5.3;
    Console.Write(5.4);
    string b = Console.ReadLine();
    if ( == b)
    {
        Console.WriteLine(5.7);
        return;
    }
    Console.Write(5.5 + global::0.2 + 5.6);
    2();
}
```

Now save the program and execute it.



```
Enter a username: heyhey
Enter a password: heyee
Please Enter the secret Key: 12312321
Nice here is the Flag:HTB{SuP3rC00lFL4g}
```

Challenge is resolved, flag is captured.

File link:
https://mega.nz/file/MloRgQSb#8-co_Aca8DAiatNGSpU_imVkFQktMrqb0BFkM0Kxi78