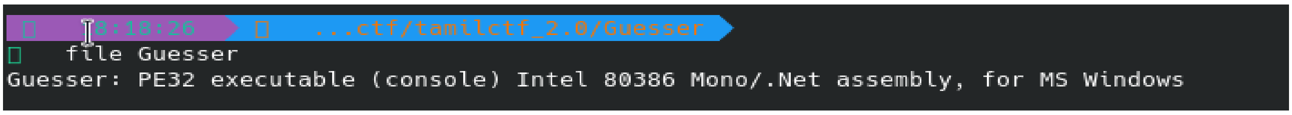
GUESSER

Description : My friend make a secure login app. It contain the secret message. Can you break the app and get the secret message for me :/ .
Author : 0xRakesh Kumar.

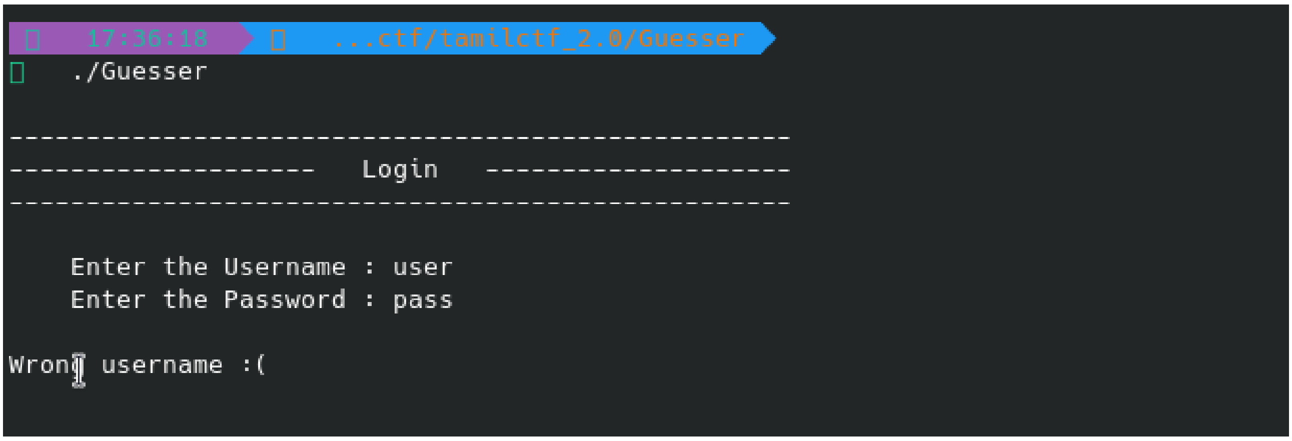
There are only one file . Guesser

Basic Info :
file Guesser



```
  18:18:26    ...ctf/tamilctf_2.0/Guesser
   file Guesser
Guesser: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
```

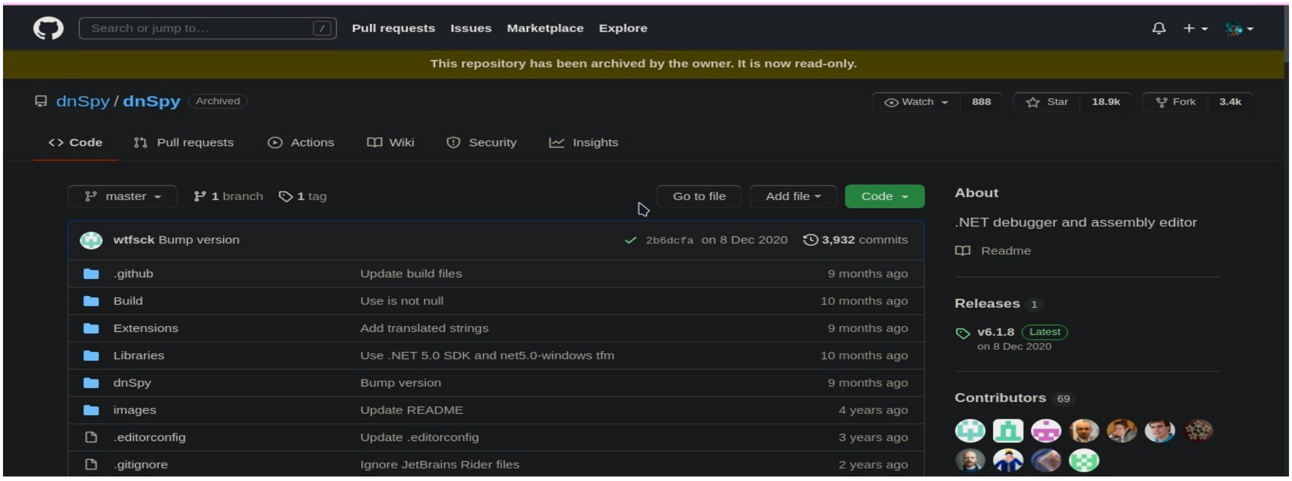
It is .Net assembly file. So we need dnspy for disassemble the file.
Run the binary :
mono Guesser



```
  17:36:18    ...ctf/tamilctf_2.0/Guesser
   ./Guesser

---------------------------------------------------
--------------------   Login   --------------------
---------------------------------------------------

    Enter the Username : user
    Enter the Password : pass

Wrong username :(
```

It ask for username and password. So we need to find it.

DNSPY :
dnSpy is a debugger and .NET assembly editor. You can use it to edit and debug assemblies even if you don't have any source code available.



This repository has been archived by the owner. It is now read-only.

About

.NET debugger and assembly editor

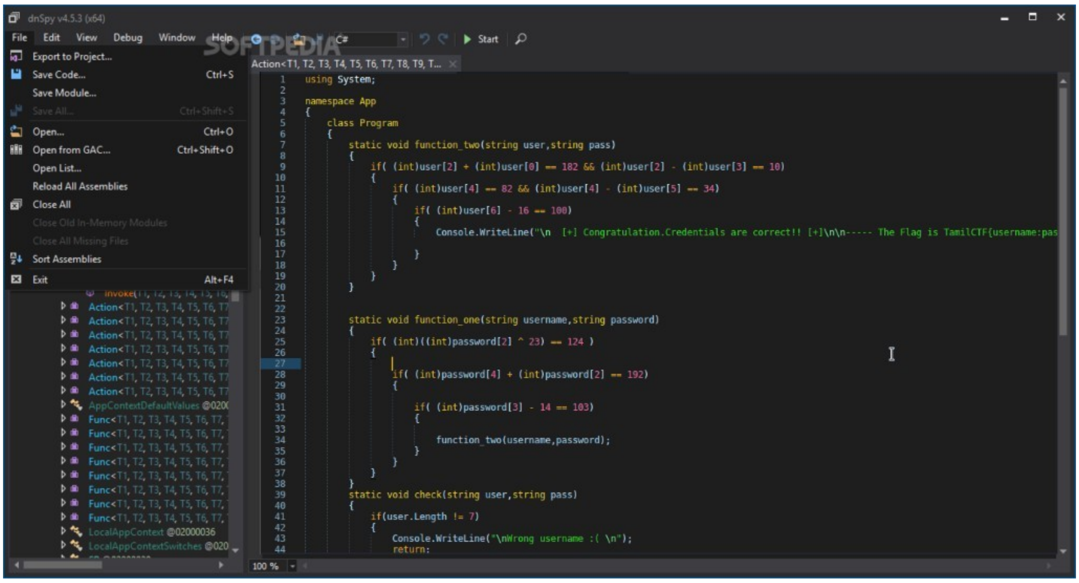
Releases 1

v6.1.8 Latest
on 8 Dec 2020

wtfsck Bump version ✓ 2b6dcfa on 8 Dec 2020 3,932 commits

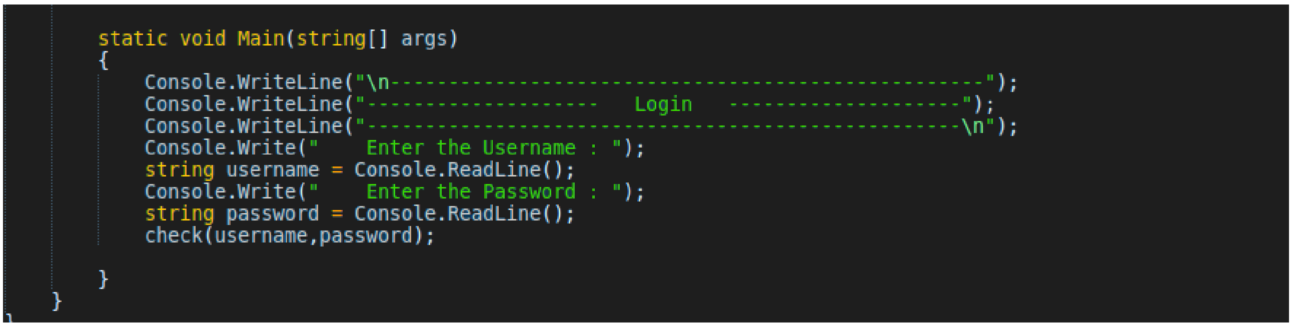
.github	Update build files	9 months ago
Build	Use is not null	10 months ago
Extensions	Add translated strings	9 months ago
Libraries	Use .NET 5.0 SDK and net5.0-windows tfm	10 months ago
dnSpy	Bump version	9 months ago
images	Update README	4 years ago
.editorconfig	Update .editorconfig	3 years ago
.gitignore	Ignore JetBrains Rider files	2 years ago

Load the binary in dnspy:



```
using System;

namespace App
{
    class Program
    {
        static void function_two(string user,string pass)
        {
            if( (int)user[2] + (int)user[0] == 182 && (int)user[2] - (int)user[3] == 10)
            {
                if( (int)user[4] == 82 && (int)user[4] - (int)user[5] == 34)
                {
                    if( (int)user[6] - 16 == 100)
                    {
                        Console.WriteLine("\n  [+] Congratulation.Credentials are correct!! [+]\n\n----- The Flag is TamilCTF{username:pas

                    }
                }
            }
        }


        static void function_one(string username,string password)
        {
            if( (int)((int)password[2] ^ 23) == 124 )
            {

                if( (int)password[4] + (int)password[2] == 192)
                {

                    if( (int)password[3] - 14 == 103)
                    {

                        function_two(username,password);
                    }
                }
            }
        }
        static void check(string user,string pass)
        {
            if(user.Length != 7)
            {
                Console.WriteLine("\nWrong username :( \n");
                return;
```

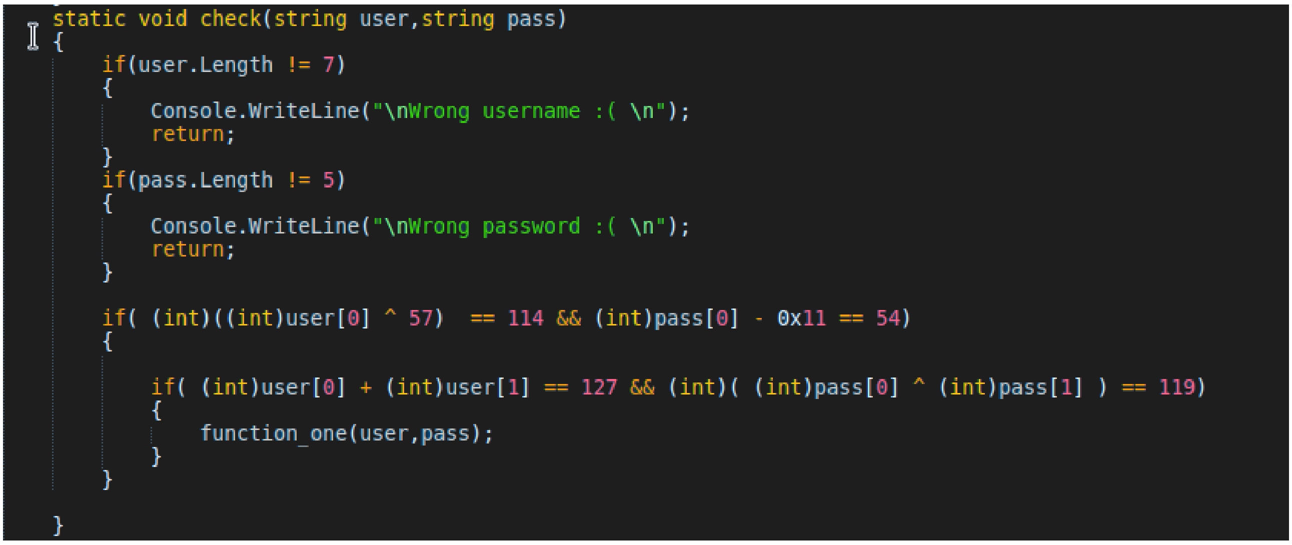
Every C# program start with main function, So look at the main function.



```
        static void Main(string[] args)
        {
            Console.WriteLine("\n--------------------------------------------------");
            Console.WriteLine("-------------------    Login    -------------------");
            Console.WriteLine("--------------------------------------------------\n");
            Console.Write("    Enter the Username : ");
            string username = Console.ReadLine();
            Console.Write("    Enter the Password : ");
            string password = Console.ReadLine();
            check(username,password);

        }
    }
```

Main Function

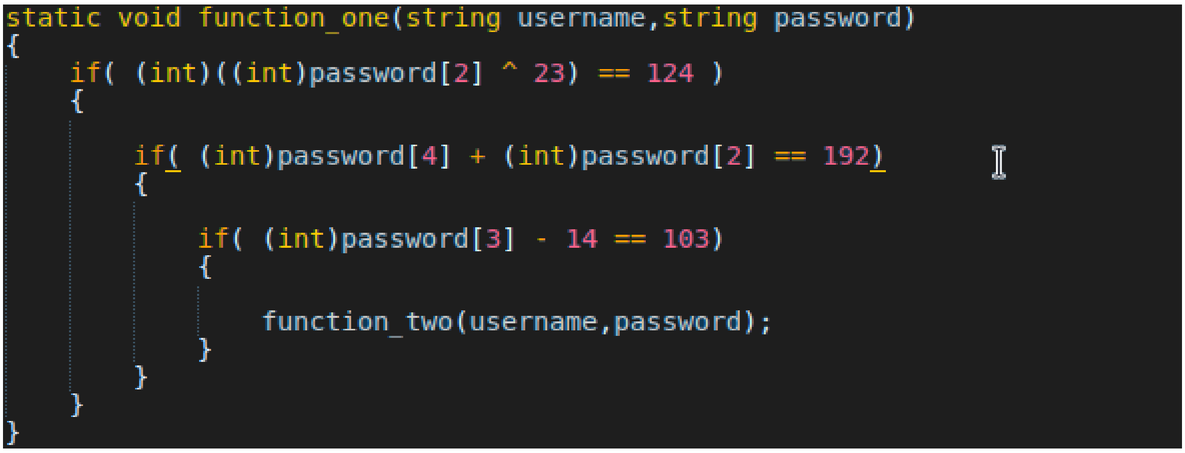
It get username and password , then call the check function with argument of username and password.



```
    static void check(string user,string pass)
    {
        if(user.Length != 7)
        {
            Console.WriteLine("\nWrong username :( \n");
            return;
        }
        if(pass.Length != 5)
        {
            Console.WriteLine("\nWrong password :( \n");
            return;
        }

        if( (int)((int)user[0] ^ 57)  == 114 && (int)pass[0] - 0x11 == 54)
        {

            if( (int)user[0] + (int)user[1] == 127 && (int)( (int)pass[0] ^ (int)pass[1] ) == 119)
            {
                function_one(user,pass);
            }
        }

    }
```

Check Function

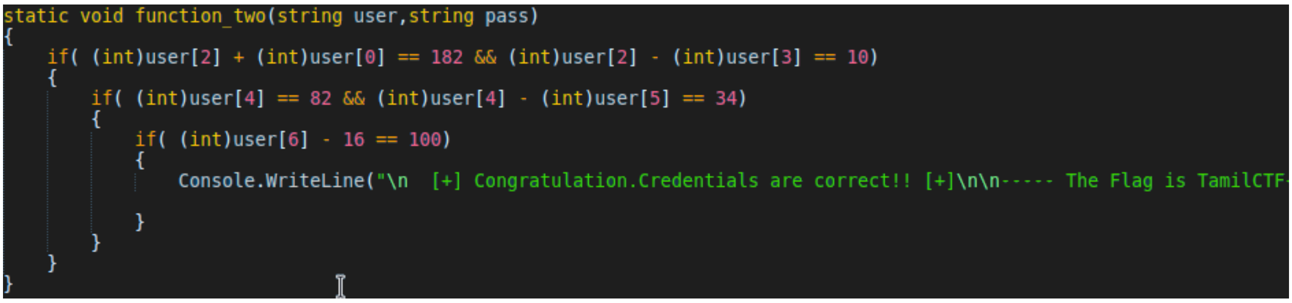
It check the length of username and password. The username’s length must be 7 and the password’s length must be 5. If it’s equal ,then it do some operation and check with some value. After the check function ,it call function_one with argument of user and pass.



```
static void function_one(string username,string password)
{
    if( (int)((int)password[2] ^ 23) == 124 )
    {

        if( (int)password[4] + (int)password[2] == 192)
        {

            if( (int)password[3] - 14 == 103)
            {

                function_two(username,password);
            }
        }
    }
}
```

Function_one

Same as check function ,it also do operation with password and check with some value. After the function_one, it call function_two with the argument of username and password.



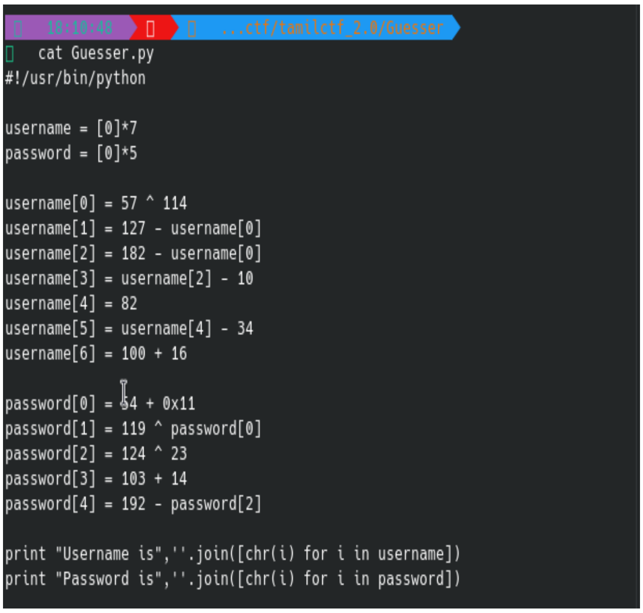
```
static void function_two(string user,string pass)
{
    if( (int)user[2] + (int)user[0] == 182 && (int)user[2] - (int)user[3] == 10)
    {
        if( (int)user[4] == 82 && (int)user[4] - (int)user[5] == 34)
        {
            if( (int)user[6] - 16 == 100)
            {
                Console.WriteLine("\n  [+] Congratulation.Credentials are correct!! [+]\n\n----- The Flag is TamilCTF

            }
        }
    }
}
```

Function_two

It check the username, it is equal , it print the congratulation message.

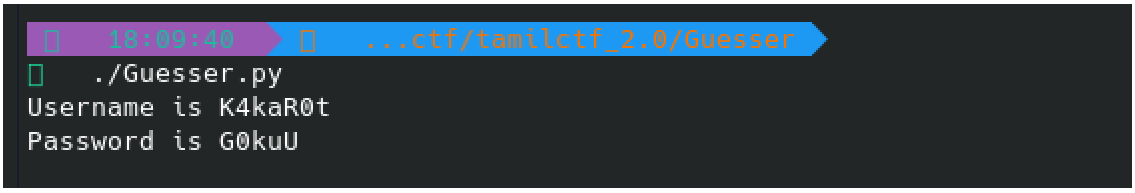
SCRIPT :

```
username = [0]*7
password = [0]*5
username[0] = 57 ^ 114
username[1] = 127 - username[0]
username[2] = 182 - username[0]
username[3] = username[2] - 10
username[4] = 82
username[5] = username[4] - 34
username[6] = 100 + 16
password[0] = 54 + 0x11
password[1] = 119 ^ password[0]
password[2] = 124 ^ 23
password[3] = 103 + 14
password[4] = 192 - password[2]

print "Username is",''.join([chr(i) for i in username])
print "Password is",''.join([chr(i) for i in password])
```

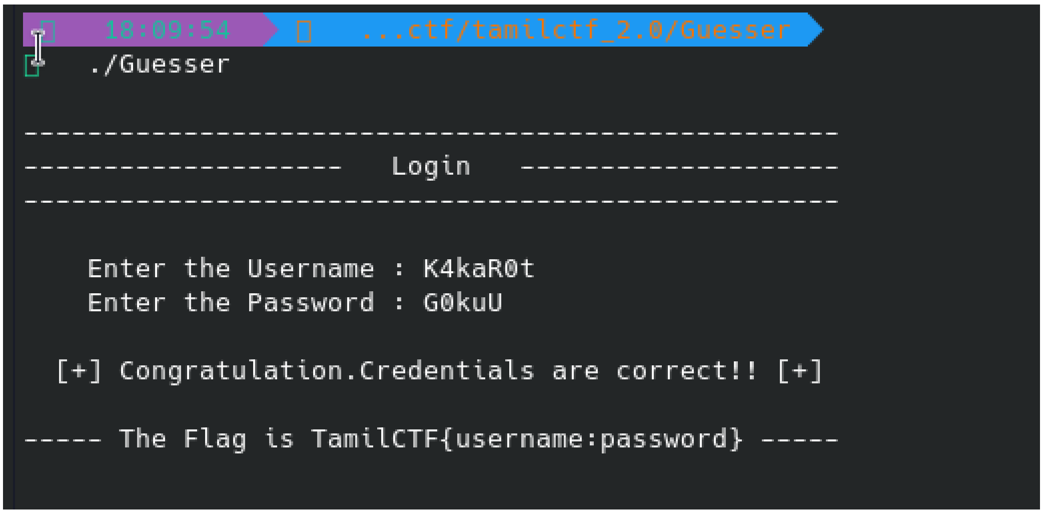


```
  18:10:48      ...ctf/tamilctf_2.0/Guesser
  cat Guesser.py
#!/usr/bin/python

username = [0]*7
password = [0]*5

username[0] = 57 ^ 114
username[1] = 127 - username[0]
username[2] = 182 - username[0]
username[3] = username[2] - 10
username[4] = 82
username[5] = username[4] - 34
username[6] = 100 + 16

password[0] = 54 + 0x11
password[1] = 119 ^ password[0]
password[2] = 124 ^ 23
password[3] = 103 + 14
password[4] = 192 - password[2]

print "Username is",''.join([chr(i) for i in username])
print "Password is",''.join([chr(i) for i in password])
```

Run the script:



```
  18:09:40    ...ctf/tamilctf_2.0/Guesser
   ./Guesser.py
Username is K4kaR0t
Password is G0kuU
```



```
  18:09:54    ...ctf/tamilctf_2.0/Guesser
    ./Guesser

---------------------------------------------------
--------------------   Login   --------------------
---------------------------------------------------

    Enter the Username : K4kaR0t
    Enter the Password : G0kuU

  [+] Congratulation.Credentials are correct!! [+]

----- The Flag is TamilCTF{username:password} -----
```

Yeah !!! The value are correct. We get the message.