

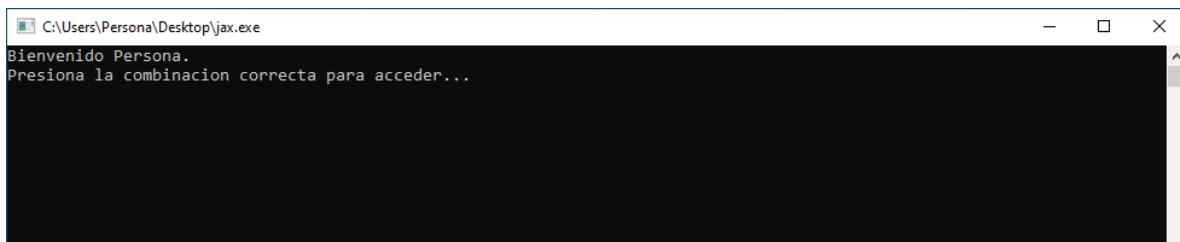
Descripción

Nos dijeron que si corres la bandera con el username correcto nos imprime la bandera, ¿puedes checarlo?

Importante: la bandera empieza con hackdef{

Procedimiento

Al ejecutar el archivo jax.exe nos ejecuta una ventana de consola en donde se nos pide ingresar una combinación correcta de teclas, al no ingresar correctamente esta combinación nos regresara el siguiente mensaje “WOP WOP! !! NoooOOOoooo!”.



Usando dnSpy encontramos una clase llamada programa, donde podemos encontrar la combinación de teclas necesarias para poder entrar al programa, la cual corresponde a F5, F3, F6.

```
using System;
using System.Globalization;
using System.Threading;

namespace jax
{
    // Token: 0x02000003 RID: 3
    internal class Program
    {
        // Token: 0x06000005 RID: 5 RVA: 0x000021C8 File Offset: 0x000003C8
        private static void Main(string[] args)
        {
            Thread.CurrentThread.CurrentUICulture = new CultureInfo("en-us");
            string userName = Environment.UserName;
            Console.WriteLine("Bienvenido {0}. \nPresiona la combinacion correcta para acceder...", userName);
            if (Console.ReadKey().Key == ConsoleKey.F5 && Console.ReadKey().Key == ConsoleKey.F3 && Console.ReadKey().Key == ConsoleKey.F6)
            {
                Console.WriteLine(new Flag(userName).print());
            }
            else
            {
                Console.WriteLine("WOP WOP WOP!!!! Noooooooo00000oooo!");
            }
            Console.ReadKey();
        }
    }
}
```

Una vez que introducimos la combinación nos manda el siguiente mensaje: “Nop, esa no es la excepción correcta”, por lo que procederemos a seguir revisando el ejecutable con dnSpy. Nos encontramos otra clase llamada flag, dentro de esta clase podemos observar que recibe como parámetro nuestro username y revisa si puede obtener el carácter en la posición 8, si esto se cumple manda el mensaje ya antes mencionado. Por lo que se puede deducir que el username debe ser menor a 8 caracteres para poder obtener la bandera.

```

using System;
using System.IO;

namespace jax
{
    // Token: 0x02000002 RID: 2
    internal class Flag
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
        public Flag(string _f)
        {
            try
            {
                File.ReadAllText(_f.ToCharArray()[8].ToString());
                this.s = "hackdf{NOP_ESTO_NO_ES_LO_QUE_BUSCAS!}";
            }
            catch (Exception e)
            {
                this.l(e, _f);
            }
        }
    }
}

```

Se probó primero con el siguiente nombre de usuario: "AAA", el cual nos regresó lo siguiente "S@Tt#?ÑEI?X6x@jwF:B8l", se probó con 7 A, para observar si cambiaba la salida y obtuvimos lo siguiente "[?²1?8?G=jD????#?Ñ??Fa△x@j,?A?Al". Observamos que si cambian las salidas y el objetivo del reto es encontrar el nombre de usuario correcto para obtener la bandera, por lo que procedemos a intentar con el nombre de usuario HackDef, haciendo la suposición de que sea el nombre de usuario correcto y obtenemos la siguiente salida "Pe?c?_aG&J"ltgb#?1h|CE xIJ?[Æu*I".

Al ver que no obtenemos la bandera correcta, lo siguiente es analizar el código de la excepción en la que estamos entrando y la cual es la encargada de devolver la bandera.

```
private void l(Exception e, string _f)
{
    string message = e.Message;
    this.s = "";
    Console.WriteLine(this.s);
    if (e.GetType() == typeof(IndexOutOfRangeException))
    {
        string text = this.f(_f);
        long num = 137438953472L;
        int[] array = new int[]
        {
            -47,
            -86,
            -107,
            -101,
            -83,
            -41,
            -80,
            -82,
            13,
            9,
            -22,
            -82,
            -68,
            -81,
            -91,
            -49,
            -80,
            -80,
            -71,
            -87,
            -30,
            0,
            -36,
            -97,
            -12,
            -61,
            -101,
            -67,
            -94,
            -75,
            -26,
            -15
        };
        char[] array2 = message.ToCharArray();
        char[] array3 = text.ToCharArray();
        while (((long)this.s.Length & num) == 0L)
        {
            byte b = Convert.ToByte(array2[this.s.Length]);
            b ^= (byte)((int)Convert.ToByte(array3[this.s.Length % 8]) + array[this.s.Length]);
            this.s += Convert.ToChar(b).ToString();
            num >>= 1;
        }
        return;
    }
    Console.WriteLine("Nop, esa no es la excepcion correcta");
}

// Token: 0x06000003 RID: 3 RVA: 0x0000219E File Offset: 0x0000039E
public string print()
{
    return this.s;
}

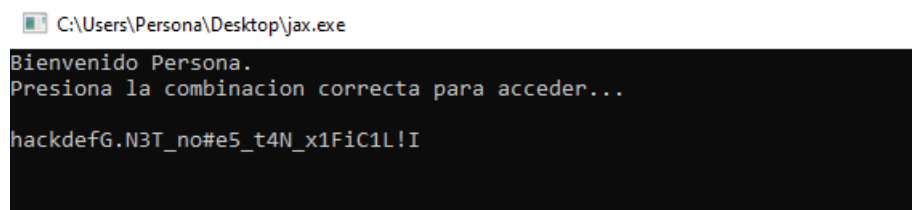
// Token: 0x06000004 RID: 4 RVA: 0x000021A6 File Offset: 0x000003A6
private string f(string inp)
{
    if ((inp.Length & 8) <= 0)
    {
        return this.f(inp + "x");
    }
    return inp;
}
```

Observamos lo siguiente, crea una variable **message** donde guarda el mensaje de la excepción, en la variable **s** guarda una cadena vacía, crea una variable **text** donde guarda nuestro nombre de usuario, las variables **message** y **text** las convierte en arrays, los cuales utiliza dentro del ciclo while que es donde se crea la bandera.

El primer paso que realiza es convertir en bytes el primer carácter del username y lo guarda en una variable b, después hace un XOR con la variable b y el primer elemento de la variable **message** convertida en bytes para después sumarla con el primer elemento del array de números, y una vez hecho esto lo va concatenando en **s**.

Sabemos que la bandera empieza con hackdef, por lo que podemos hacer el proceso inverso para obtener el username, usando el debugger, ponemos un breakpoint donde obtiene el mensaje de excepción el cual es "Index was outside the bounds of the array", esto nos sirve ya que es con lo que se realiza el XOR. Para obtener el username solo necesitaremos los primeros 7 caracteres del mensaje de excepción "Indexwa", y los primeros 7 elementos del array de números "47, 86, 107, 101, 83, 41, 80". Una vez que tenemos esto convertimos en binario las letras de hackdef y del mensaje de excepción, realizamos un XOR con la primera letra de hackdef y de Indexwa y así sucesivamente hasta tener las 7 letras, esto nos dará como resultado otro binario el cual pasaremos a decimal y se ira sumando con cada uno de los números del array y así obtenemos el siguiente username "Persona".

Procedemos a cambiar el nombre de usuario y nos regresa lo siguiente.



```
C:\Users\Persona\Desktop\jax.exe
Bienvenido Persona.
Presiona la combinacion correcta para acceder...
hackdefG.N3T_no#e5_t4N_x1FiC1L!I
```

Nos regresa la bandera, solo observamos que cada 8 caracteres no nos regresa el correcto, pero sabemos que donde va la G y la I van las llaves ({}), el # lo substituímos por un _ y la x por una d, quedando de la siguiente forma "hackdef{.N3T_no_e5_t4N_d1FiC1L!}".