

# Reporte de Vulnerabilidad

---

<b>Documento Creador</b>	Carlos Arizandy Rodriguez Preciado
<b>Revisión</b>	1
<b>Ultima actualización</b>	06-12-2023

# Contenido

<b>Recomendaciones</b>	3
<b>Vulnerabilidades de gravedad critica.</b>	3
<b>Use a dynamically-generated, random IV.</b>	3
Evidencia:	3
Recomendaciones	4
Solución:	4
<b>Vulnerabilidades de seguridad alta</b>	5
<b>Make 'key' 'readonly'.</b>	5
Evidencia:	5
Recomendaciones	6
Solución	6
<b>Vulnerabilidades de seguridad media</b>	7
<b>Denegación de servicio (DoS)</b>	7
Recomendaciones	7
Solución	8
<b>Vulnerabilidades de seguridad baja.</b>	9
Hotspots Reviewed	9
Evidencia:	9
Recomendaciones	10
Solución	10
<b>Code Smells</b>	11
Evidencia:	11
Recomendaciones	11
Solución	12
<b>Resumen</b>	13

# Recomendaciones

## Vulnerabilidades de gravedad critica.

### Use a dynamically-generated, random IV.

Esta vulnerabilidad consiste en el cifrado **Cipher Block** donde recomiendan utilizar un vector de inicialización (IV) para que el cifrado sea aleatorio.

No es necesario que el IV sea secreto, pero debe ser impredecible para evitar el "Chosen-Plaintext Attack".

Evidencia:

### Use a dynamically-generated, random IV.

Cipher Block Chaining IVs should be unpredictable [csharpsquid:S3329](#) 23 hours ago L42

**Vulnerability** Critical Open Carlos Arizandi Rodriguez Prec... 15min effort 0 comments cwe, owasp-a3, owasp-m5

Where is the issue? Why is this an issue?

CarlosRodriguezSecurityFinalProyect /Encriptacion.cs See all issues in this file

```
37 carlo... using (Aes aes = Aes.Create())
38 {
39     aes.Key = Encoding.ASCII.GetBytes(key);
40     aes.IV = iv;
41
42     ICryptoTransform encryptor = aes.CreateEncryptor(aes.Key, aes.IV);
43
44     using (MemoryStream memoryStream = new MemoryStream())
45     {
46         using (CryptoStream cryptoStream = new CryptoStream((Stream)memoryStream, encryptor,
47             CryptoStreamMode.Write))
48         {
49             using (StreamWriter streamWriter = new StreamWriter((Stream)cryptoStream))
50             {
51                 streamWriter.Write(plainText);
52             }
53         }
54     }
55 }
```

## Recomendaciones

- Se recomienda generar vectores de inicialización, "NIST" recomienda utilizar un generador de números aleatorios seguro.
- Definición de claves aleatorias.

```
namespace SecurityProyect2
{
    2 references
    internal class Encriptacion{
        private readonly byte[] key = new byte[32];
        private readonly byte[] iv = new byte[16];

        1 reference
        private static string hashinSHA256(string dato)
        {
            // Create a SHA256 hash from string
            using (SHA256 sha256Hash = SHA256.Create())
            {
                // Computing Hash - returns here byte array
                byte[] bytes = sha256Hash.ComputeHash(Encoding.UTF8.GetBytes(dato));

                // now convert byte array to a string
                StringBuilder stringBuilder = new StringBuilder();
            }
        }
    }
}
```

## Solución:

```
1 reference
private static byte[] Encrypt(string plaintext, byte[] key, byte[] iv)
{
    using (Aes aesAlg = Aes.Create())
    {
        aesAlg.Key = key;
        aesAlg.IV = iv;
        ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);
        byte[] encryptedBytes;
        using (var msEncrypt = new System.IO.MemoryStream())
        {
            using (var csEncrypt = new CryptoStream(msEncrypt, encryptor, CryptoStreamMode.Write))
            {
                byte[] plainBytes = Encoding.UTF8.GetBytes(plaintext);
                csEncrypt.Write(plainBytes, 0, plainBytes.Length);
            }
            encryptedBytes = msEncrypt.ToArray();
        }
        return encryptedBytes;
    }
}
```

# Vulnerabilidades de seguridad alta

En la revisión de las vulnerabilidades del proyecto, se detectó una vulnerabilidad de nivel alto, esta consiste en lo siguiente:

## Make 'key' 'readonly'.

Esta vulnerabilidad indica que la llave debe estar definida como solo de lectura para que su valor no sea modificado.

Evidencia:

**Make 'key' 'readonly'.**Get permalink  
Methods should not be empty [csharpsquid:S1186](#)24 hours ago L11  
Code Smell Major Open Carlos Arizandi Rodriguez Prec... 2min effort 0 comments confusing

Where is the issue?

Why is this an issue?

CarlosRodriguezSecurityFinalProyect

/Encriptacion.cs

See all issues in this file

```
6  carlo...  using System.Text;
7
8  namespace SecurityProyect2
9  {
10     internal class Encriptacion{
11         private String key;

12         public Encriptacion(String key) {
13             this.key = key;
14         }
15         private static string hashinSHA256(string dato)
16         {
17             // Create a SHA256 hash from string
18             using (SHA256 sha256Hash = SHA256.Create())
19             {
20                 // Computing Hash - returns here byte array
```

## Recomendaciones

- Se recomienda definir la variable como privada dentro de la clase con el atributo readonly, definir valor al iniciar la clase.

## Solución

```
7
8 namespace SecurityProyect2
9 {
10     2 references
11     internal class Encriptacion{
12         private readonly byte[] key = new byte[32];
13         private readonly byte[] iv = new byte[16];
14
15     1 reference
16     private static string hashinSHA256(string dato)
17     {
18         // Create a SHA256 hash from string
19         using (SHA256 sha256Hash = SHA256.Create())
20         {
21             // Computing Hash - returns here byte array
22             byte[] bytes = sha256Hash.ComputeHash(Encoding.UTF8.GetBytes(dato));
23
24             // now convert byte array to a string
25             StringBuilder stringBuilder = new StringBuilder();
26             for (int i = 0; i < bytes.Length; i++)
27             {
28             }
```

# Vulnerabilidades de seguridad media

## Denegación de servicio (DoS)

Se detectan 1 vulnerabilidades de este tipo, el cual nos están indicando una serie de expresiones reguladores, dichas expresiones regulares no están validando los datos de entrada de manera correcta, en algunos casos puede causar problemas de rendimiento y en el peor de los casos provocar una denegación de servicio de la aplicación.

### Evidencia

Where is the risk?	What's the risk?	Assess the risk	How can I fix it?
<div><div>/Form1.cs</div><div>Open in IDE</div><div>Get Permalink</div></div> <pre>16      } 17 18      private void label2_Click(object sender, EventArgs e) 19      { 20 21      } 22 23      //Metodo para validar número de tarjeta por medio de una regExp 24      private Boolean valida_tarjeta(String numTarjeta) { 25          String regex = @"^(d\s?){15,16}\$"; 26          return Regex.IsMatch(numTarjeta, regex); 27 28          Pass a timeout to limit the execution time. 29 30      } 31 32      // Método para enmascarar numero de tarjeta, visible solo los ultimos 4 digitos 33      private String mask_tarjeta(String numTarjeta) { 34          String mascara = ""; 35          for (int i = 0; i &lt; numTarjeta.Length -4;i++) { 36              mascara += "*"; 37          } 38          mascara += numTarjeta.Substring((numTarjeta.Length)-4); 39          return mascara; 40      }</pre>			

### Recomendaciones

- Se recomienda utilizar o definir "matchTimeout".
- Se recomienda revisar los patrones en busca de vulnerabilidades que puedan ocasionar una denegación de servicio

- Considerar utilizar un algoritmo sin retroceso especificando "RegexOptions.None".

## Solución

```
//Metodo para validar número de tarjeta por medio de una regExp
1 reference
private Boolean valida_tarjeta(String numTarjeta) {
    String regex = @"^\d\s?){15,16}$";
    return Regex.IsMatch(numTarjeta, regex, RegexOptions.None, TimeSpan.FromMilliseconds(100));
}
```



# Vulnerabilidades de seguridad baja.

## Hotspots Reviewed

En la revisión de las vulnerabilidades del proyecto, se encontraron 3 funciones definidas pero que no contienen código.

Evidencia:

Form1.cs

<input type="checkbox"/>	Add a nested comment explaining why this method is empty, throw a 'NotSupportedException' or complete the implementation.	1 day ago ▾ L17 🔗 🔍
🔗	Code Smell ▾ 🚨 Critical ▾ 🔵 Open ▾ Carlos Arizandi Rodriguez Prec... ▾ 5min effort Comment	🕒 suspicious ▾
<input type="checkbox"/>	Use a StringBuilder instead.	1 day ago ▾ L32 🔗 🔍
🔗	Code Smell ▾ 🟡 Minor ▾ 🔵 Open ▾ Carlos Arizandi Rodriguez Prec... ▾ 10min effort Comment	🕒 performance ▾
<input type="checkbox"/>	Add a nested comment explaining why this method is empty, throw a 'NotSupportedException' or complete the implementation.	1 day ago ▾ L74 🔗 🔍
🔗	Code Smell ▾ 🚨 Critical ▾ 🔵 Open ▾ Carlos Arizandi Rodriguez Prec... ▾ 5min effort Comment	🕒 suspicious ▾
<input type="checkbox"/>	Add a nested comment explaining why this method is empty, throw a 'NotSupportedException' or complete the implementation.	1 day ago ▾ L79 🔗 🔍
🔗	Code Smell ▾ 🚨 Critical ▾ 🔵 Open ▾ Carlos Arizandi Rodriguez Prec... ▾ 5min effort Comment	🕒 suspicious ▾

4 of 4 shown

Where is the issue? Why is this an issue?

CarlosRodriguezSecurityFinalProyect /Form1.cs 🔗

See all issues in this file 🔗

```
12 carlo... public Form1()
13 {
14     InitializeComponent();
15 }
16
17 private void label2_Click(object sender, EventArgs e)
18 {
19 }
20
21
22 //Metodo para validar número de tarjeta por medio de una regexp
23 private Boolean valida_tarjeta(String numTarjeta) {
24     String regex = @"^(\\d\\s?){15,16}$";
25 carlo... return Regex.IsMatch(numTarjeta, regex, RegexOptions.None, TimeSpan.FromMilliseconds(100));
26 carlo... }
```

🔗 Add a nested comment explaining why this method is empty, throw a 'NotSupportedException' or complete the implementation.

## Recomendaciones

- Eliminar funciones que no cuentan con código
- Agregue método "throw new NotSupportedException();"

## Solución

```
0 references
private void Label2_Click(object sender, EventArgs e)
{
    throw new NotSupportedException();
}
```

# Code Smells

Evidencia:

The screenshot shows a code editor window for a file named `/Form1.cs` in a project called `CarlosRodriguezSecurityFinalProyect`. The code is in C# and includes a method `mask_tarjeta` that concatenates strings in a loop. A red squiggly line under the `+=` operator in the loop indicates a code smell. A tooltip box is open, displaying the message "Use a StringBuilder instead." with a plus icon. The tooltip also includes a link to "See all issues in this file". The code in the background is as follows:

```
29 carlo...
30
31 // Método para enmascarar numero de tarjeta, visible solo los últimos 4 dígitos
32 private String mask_tarjeta(String numTarjeta) {
33     String mascara = "";
34     for (int i = 0; i < numTarjeta.Length -4; i++) {
35         mascara += "X";
36     }
37     mascara += numTarjeta.Substring((numTarjeta.Length)-4);
38     return mascara;
39 }
40
41 //Metodo para procesar información
42 private void button1_Click(object sender, EventArgs e)
43 {
44     //Declaramos clase de encriptación
```

Recomendaciones

- "StringBuilders" más eficiente que la concatenación de cadenas, especialmente cuando el operador se repite una y otra vez como en bucles.

## Solución

```
// Método para enmascarar numero de tarjeta, visible solo los ultimos 4 digitos
1 reference
private String mask_tarjeta(String numTarjeta) {
    StringBuilder bld = new StringBuilder();

    for (int i = 0; i < numTarjeta.Length - 4; i++) {
        bld.Append("*");
    }

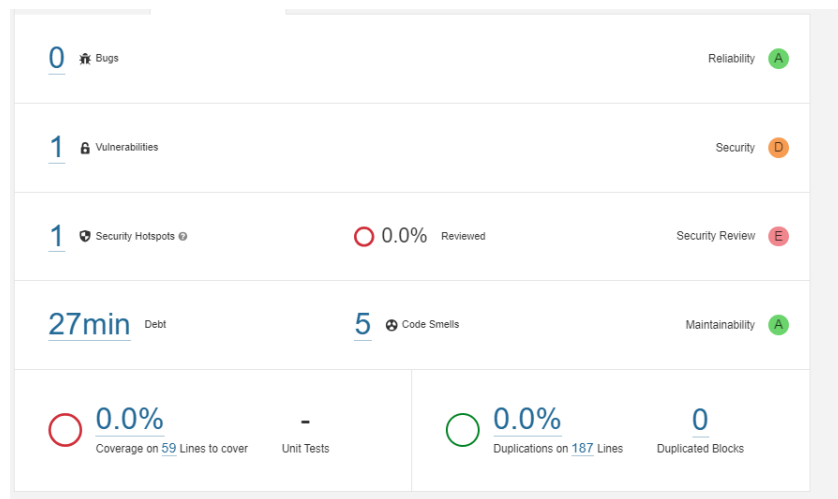
    bld.Append((numTarjeta.Length) - 4);

    return bld.ToString(); ;
}
```

# Resumen

Con ayuda de SonarQube se detectaron las vulnerabilidades del proyecto, con lo cual se ha podido solucionar de manera efectiva estas problemáticas, dando como resultado un proyecto seguro y con las mejores prácticas de desarrollo implementadas.

Antes de aplicar la solución.



Después de aplicar soluciones.

