

Ofuscación de código

Seguridad de aplicaciones Windows

Ariel Roymer Gabriel Ticona
@roymerariel



OWASP

The Open Web Application Security Project



About Me

- Ingeniero de Sistemas – U.T.O.
- Diplomado en Educación Superior y Software Libre GNU/Linux
- Developer en somosDAS
- Desarrollador de Software plataforma .NET
- Expositor en varios cursos de actualización en el área de .NET y UML
- Asesor en proyectos de tesis de grado
- y ex-docente facilitador de la U.T.O.



OWASP

The Open Web Application Security Project

¿Porque sólo preocuparse de las aplicaciones web?

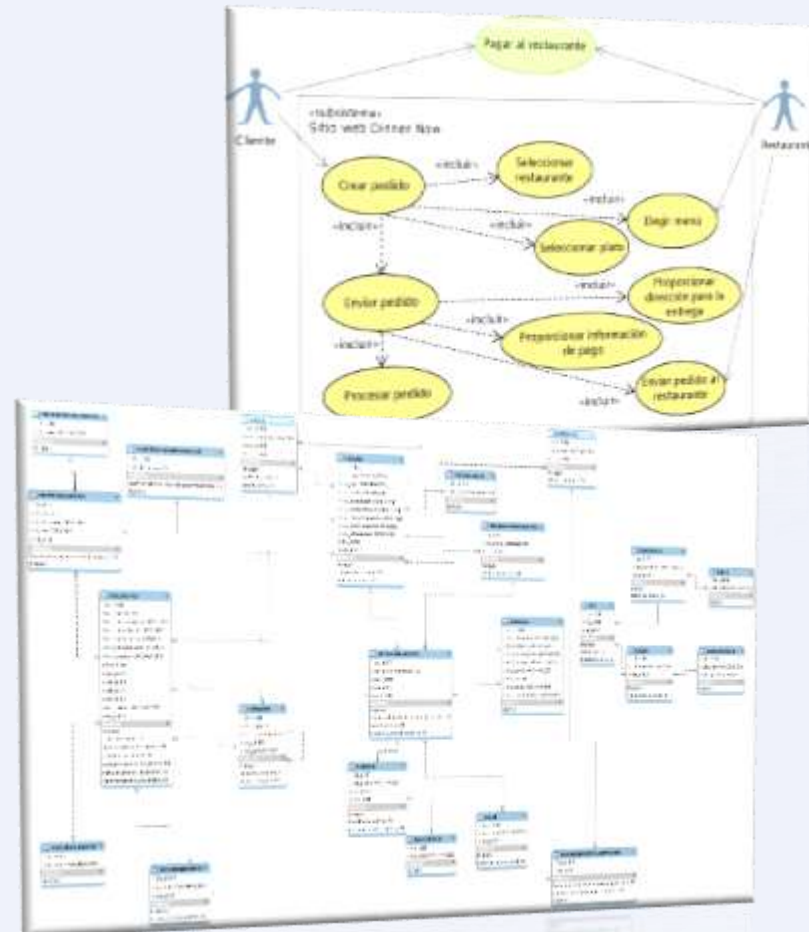
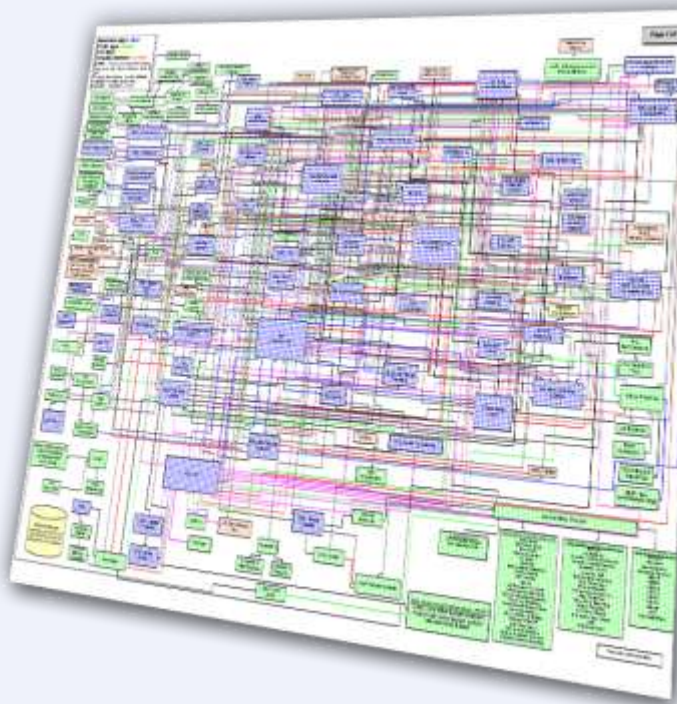




OWASP

The Open Web Application Security Project

El Software Hoy en Día ya no es como antes

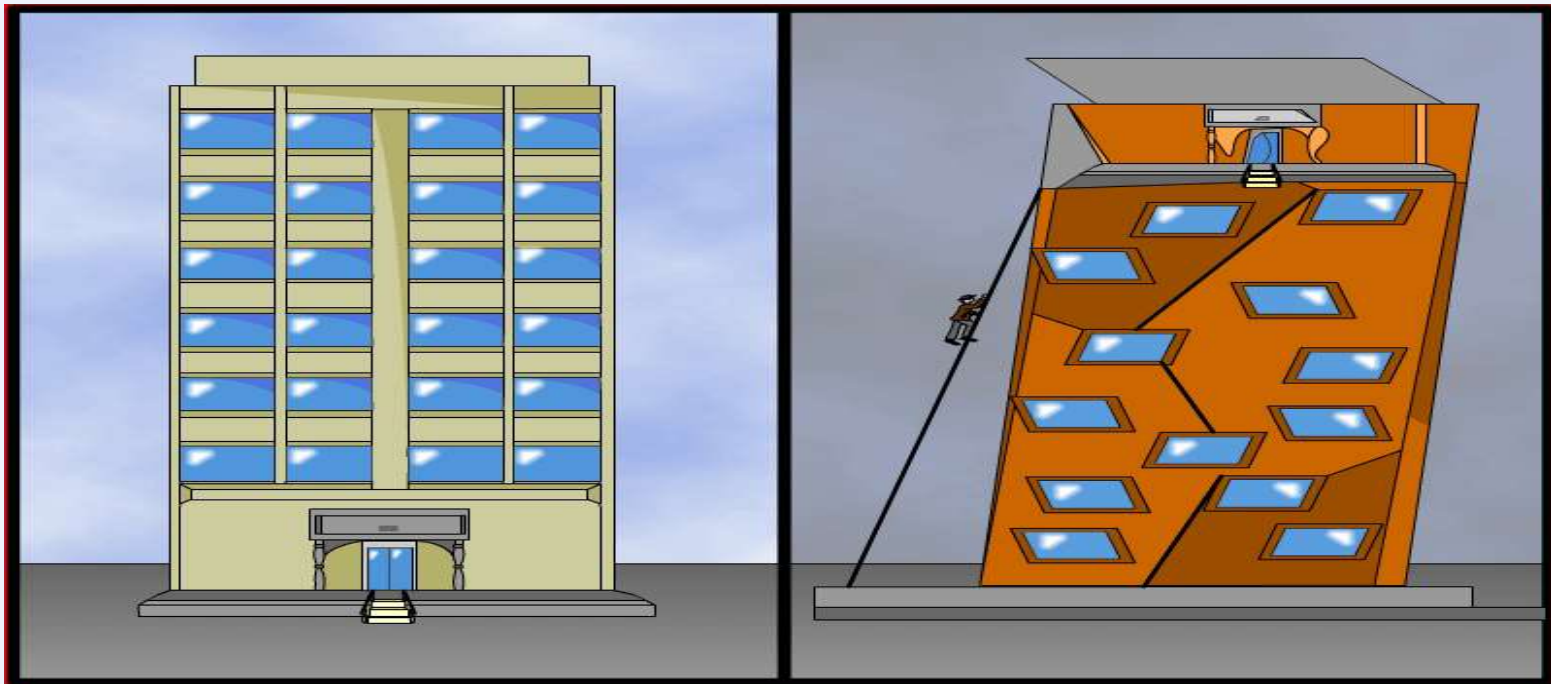




OWASP

The Open Web Application Security Project

¿A que se parece tu
Software?



¿Cuáles son las causas?

- Falta de planificación
- Malas prácticas de programación
- Falta de Diseño
- Documentación casi nula, etc. etc. etc.



¿Se te ocurre alguna otra causa?



OWASP

The Open Web Application Security Project

El Software Hoy en Día

- En el pasado las prioridades eran tener un código rápido, pequeño (ocupa poca memoria), optimizado, utilizando los algoritmos mas eficaces etc...
- Hoy en día el software es más complejo pero a la vez hay herramientas más poderosas, por lo que actualmente el enfoque es que este código tiene que **ser simple**.

Beneficios del Código Simple

- El código es mas fácil de cambiar o arreglar.
- Es más fácil desarrollar de un modo iterativo e incrementando.
- El código es más fácil de leer (entender).





OWASP

The Open Web Application Security Project

Buenas Prácticas de Programación (Sólo unas cuantas)

- DRY – Don't repeat yourself
- Don't make me think
- Open/Closed Principle
- Write Code for the Maintainer
- Single Responsibility Principle



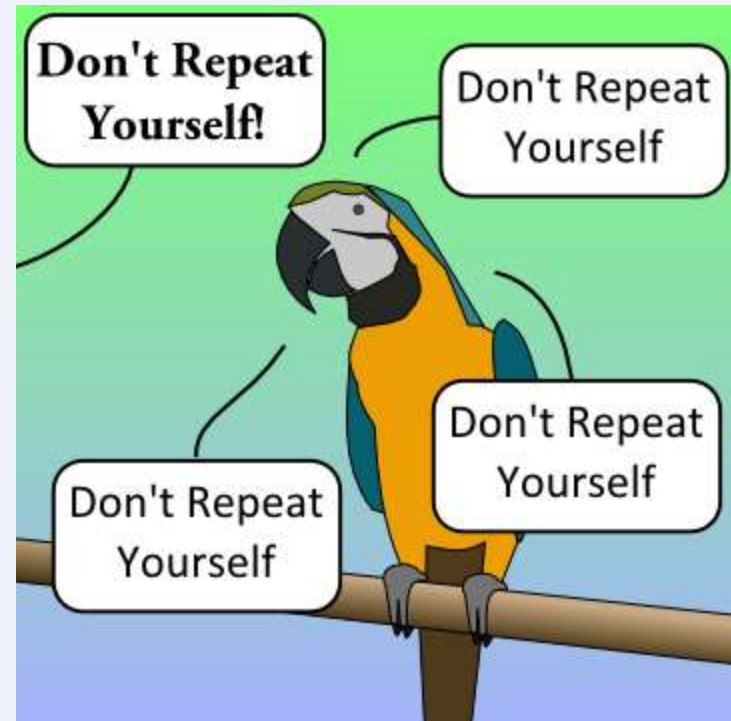
OWASP

The Open Web Application Security Project

DRY – Don't repeat yourself

(No repita código)

- Evita la repetición de código: como funciones, métodos, clases, etc.





OWASP

The Open Web Application Security Project

Algunos ejemplos...

```
private void toolStripBtnNuevo_Click(object sender, EventArgs e)
{
    frmNuevoMaterial v = new frmNuevoMaterial();
    v.ShowDialog();
    this.materialDisponibleTableAdapter.Fill( this.vistasProcedimientos.MaterialDisponible );
    materialDispTotalTableAdapter.Fill(vistasProcedimientos.MaterialDispTotal,txtBuscar.Text);
    this.materialTableAdapter.Fill(this.activoAlmacenDS.Material, txtBuscar.Text);
}
```

```
private void toolStripBtnEditar_Click(object sender, EventArgs e)
{
    if (materialDispTotalBindingSource.Count > 0)
    {
        frmNuevoMaterial v = new frmNuevoMaterial(dgvTotal.CurrentRow.Cells[0].Value.ToString());
        v.ShowDialog();
        this.materialDisponibleTableAdapter.Fill( this.vistasProcedimientos.MaterialDisponible );
        materialDispTotalTableAdapter.Fill(vistasProcedimientos.MaterialDispTotal,txtBuscar.Text);
        this.materialTableAdapter.Fill(this.activoAlmacenDS.Material, txtBuscar.Text);
    }
}
```



OWASP

The Open Web Application Security Project

Algunos ejemplos...

```
private void toolStripBtnNuevo_Click(object sender, EventArgs e)
{
    frmNuevoMaterial v = new frmNuevoMaterial();
    v.ShowDialog();
    Listar();
}

private void toolStripBtnEditar_Click(object sender, EventArgs e)
{
    if (materialDispTotalBindingSource.Count > 0)
    {
        frmNuevoMaterial v = new frmNuevoMaterial(dgvTotal.CurrentRow.Cells[0].Value.ToString());
        v.ShowDialog();
        Listar();
    }
}
```



OWASP

The Open Web Application Security Project

Don't make me think

(No me haga pensar)

- Declare claramente los nombres de las variables, métodos, etc., etc.





OWASP

The Open Web Application Security Project

```
public bool LisPNCB(string pBuscar)
{
    _taCuentaBancaria.FillByPK(_ds.CuentaBancaria, pBuscar);
    if (_ds.CuentaBancaria.Count > 0)
        return true;
    else
        return false;
}

public DataTable BusNCB(string pNroCuentaBancaria)
{
    _taCuentaBancaria.FillByPK(_ds.CuentaBancaria, pNroCuentaBancaria);
    try
    {
        var fila = _ds.CuentaBancaria[0];
        nroCuentaBancaria = fila.NroCuentaBancaria;
        nombreCuentaBancaria = fila.NombreCuentaBancaria;
        tipoMoneda = fila.TipoMoneda;
        estado = fila.Estado;
        fKBanco = fila.FKBanco;
    }
    catch (SqlException e) { Mensaje.error("Error de SQL :" + e.Message); }
    catch (Exception e) { Mensaje.error("Error :" + e.Message); }
    return _ds.CuentaBancaria;
}
```



OWASP

The Open Web Application Security Project

```
public bool ListarPorNombreCuentaBancaria(string pBuscar)
{
    _taCuentaBancaria.FillByPK(_ds.CuentaBancaria, pBuscar);
    if (_ds.CuentaBancaria.Count > 0)
        return true;
    else
        return false;
}

public DataTable BuscarPorNroCuentaBancaria(string pNroCuentaBancaria)
{
    _taCuentaBancaria.FillByPK(_ds.CuentaBancaria, pNroCuentaBancaria);
    try
    {
        var fila = _ds.CuentaBancaria[0];
        nroCuentaBancaria = fila.NroCuentaBancaria;
        nombreCuentaBancaria = fila.NombreCuentaBancaria;
        tipoMoneda = fila.TipoMoneda;
        estado = fila.Estado;
        fKBanco = fila.FKBanco;
    }
    catch (SqlException e) { Mensaje.error("Error de SQL :" + e.Message); }
    catch (Exception e) { Mensaje.error("Error :" + e.Message); }
    return _ds.CuentaBancaria;
}
```



OWASP

The Open Web Application Security Project

Open/Closed Principle

- Clases, módulos, funciones, etc., deben estar abiertos para que otros lo usen y extiendan, no para que lo modifiquen.





OWASP

The Open Web Application Security Project

```
/// <summary>
/// Lista iformación por Id de Comprobante
/// </summary>
/// <param name="pIdComprobante">Parámetro Id Comprobante</param>
/// <returns> Data Table </returns>
1 referencia
public DataTable BuscarPoridComprobante(int pIdComprobante)
{
    _taComprobante.FillByPK(_ds.comprobante, pIdComprobante);
    try
    {
        CargarDatosDataTable();
    }
    catch (SqlException e) { Alerta.error("Error de SQL :" + e.Message); }
    catch (Exception e) { Alerta.error("Error :" + e.Message); }
    return _ds.comprobante;
}
```



OWASP

The Open Web Application Security Project

Write Code for the Maintainer

- “Escriba el código como si el que tuviera que mantenerlo fuera un psicópata asesino que conoce donde vives”





OWASP

The Open Web Application Security Project

```
private void Guardar()
{
    if (EsValidoLosCampos() && SeCargoDatosAEmpresa())
    {
        if (_esNuevaEmpresa)
        {
            if (_objEmpresa.Insertar())
            {
                Mensaje.ok("Empresa guardada correctamente");
            }
        }
        else
        {
            if (_objEmpresa.Modificar(_nitEmpresa))
            {
                Mensaje.ok("Empresa modificada correctamente");
            }
        }
    }
}
```



OWASP

The Open Web Application Security Project

```
private bool EsValidoLosCampos ()
{
    bool esValido = false;
    esValido = Validacion.valor_requerido(
        nitEmpresatxtDasCrar, "Nit Empresa",
        nombreEmpresatxtDasCrar, "Nombre Empresa",
        telefonotxtDasCrar, "Telefono",
        direcciontxtDasCrar, "Direccion",
        ciudadtxtDasCrar, "Ciudad",
        aniotxtDasCrar, "Año"
    );
    if (!esValido)
        Mensaje.error(Validacion.error);
    return esValido;
}
```



OWASP

The Open Web Application Security Project

```
public bool SeCargoDatosAEmpresa ()
{
    try
    {
        _objEmpresa.NitEmpresa = nitEmpresatxtDasCrar.Text;
        _objEmpresa.NombreEmpresa = nombreEmpresatxtDasCrar.Text;
        _objEmpresa.Telefono = telefonotxtDasCrar.Text;
        _objEmpresa.Direccion = direcciontxtDasCrar.Text;
        _objEmpresa.Ciudad = ciudadtxtDasCrar.Text;
        _objEmpresa.FechaCreacion = DateTime.Now;
        return true;
    }
    catch (Exception ex)
    {
        Mensaje.error(ex.Message);
        return false;
    }
}
```



OWASP

The Open Web Application Security Project

```
private void btnAceptar_Click(object sender, EventArgs e)
{
    Guardar();
}
```

Mas entendible verdad?



OWASP

The Open Web Application Security Project

Single Responsibility Principle

- Un sector de código debe ejecutar una única y bien definida tarea.



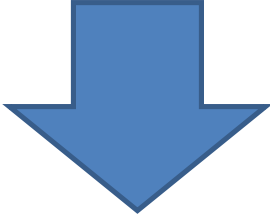


OWASP

The Open Web Application Security Project

1 referencia

```
public bool Modificar(int pIdComprobante)
{
    try
    {
        _taComprobante.Modificar(
            NroAsiento,
            TipoComprobante,
            FechaComprobante,
            FechaProcesado,
            Glosa,
            RecibidoPagadoDe,
            EstadoComprobante,
            (float)Total,
            FkUsuario,
            pIdComprobante
        );
        Eliminar(pIdComprobante);
        return true;
    }
    catch (SqlException e) { Alerta.error("Error de SQL :" + e.Message); }
    catch (Exception e) { Alerta.error("Error :" + e.Message); }
    return false;
}
```





OWASP

The Open Web Application Security Project

1 referencia

```
public bool Modificar(int pIdComprobante)
{
    try
    {
        _taComprobante.Modificar(
            NroAsiento,
            TipoComprobante,
            FechaComprobante,
            FechaProcesado,
            Glosa,
            RecibidoPagadoDe,
            EstadoComprobante,
            (float)Total,
            FkUsuario,
            pIdComprobante
        );
        //Alerta.ok("Comprobante Modificado Correctamente");
        return true;
    }
    catch (SqlException e) { Alerta.error("Error de SQL :" + e.Message); }
    catch (Exception e) { Alerta.error("Error :" + e.Message); }
    return false;
}
```



OWASP

The Open Web Application Security Project

¿Hasta aquí, todo bien verdad?

Tenemos

- Código entendible
- Código reutilizable
- Y... bueno, todo eso...
pero? ? ?



¿Nuestro código fuente está seguro?

Los archivos ejecutables pueden ser desensamblados obteniendo su código fuente en ensamblador.

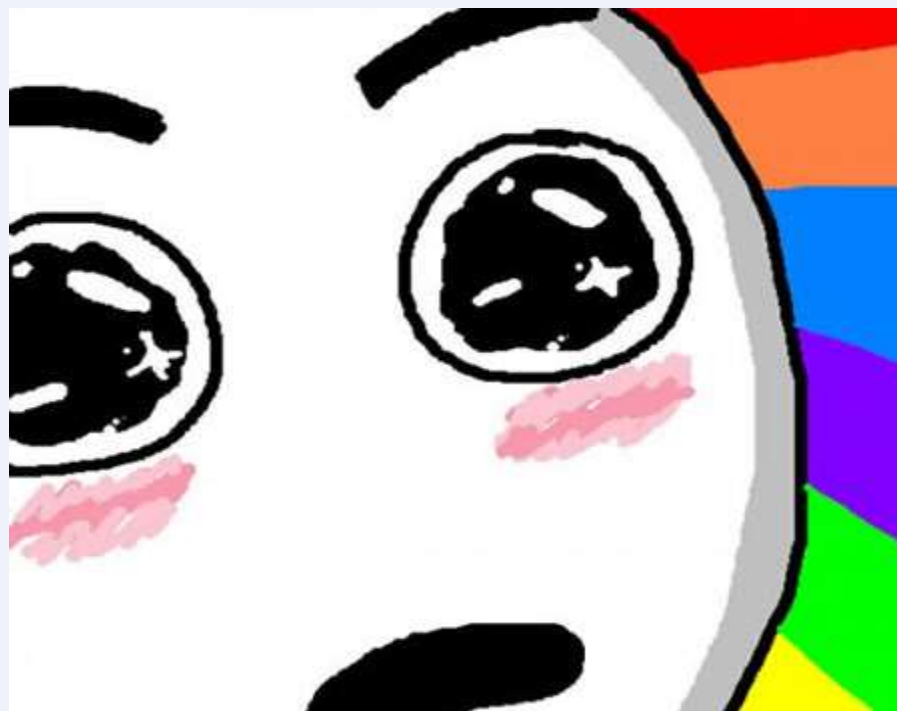




OWASP

The Open Web Application Security Project

Tu cara cuando vez un .exe que no está ofuscado





OWASP

The Open Web Application Security Project

¿Y qué hacer entonces?

Existen varias formas de proteger nuestro código, entre ellas tenemos:

- El cifrado de archivos
- **La ofuscación de código**



OWASP

The Open Web Application Security Project

¿Qué es la ofuscación?

- La ofuscación es una técnica que permite cambiar sin problema el nombre de los símbolos de los ensamblados así como otros trucos para frustrar la acción de los descompiladores.



OWASP

The Open Web Application Security Project

¿Ofuscación de código?

Es importante comprender que la ofuscación es un **proceso que se aplica a código MSIL compilado**, no a código fuente.

El **entorno de desarrollo y las herramientas no se modifican** para ajustarse al cambio de nombre.

El **código fuente nunca se modifica de ninguna manera**, ni siquiera se lee. El código MSIL ofuscado es funcionalmente equivalente al código MSIL tradicional y se ejecutará en Common Language Runtime (CLR) con idéntico resultado.



OWASP

The Open Web Application Security Project

¿Herramientas de descompilación?

He aquí algunas herramientas útiles

- Dotfuscator (Visual Studio 2010)
- Aldaray
- Agile.net Code Protection
- Eazfuscator.NET
- **Crypto Obfuscator**



OWASP

The Open Web Application Security Project

Veamos los ejemplos...



OWASP

The Open Web Application Security Project

Gracias mil!!!...