

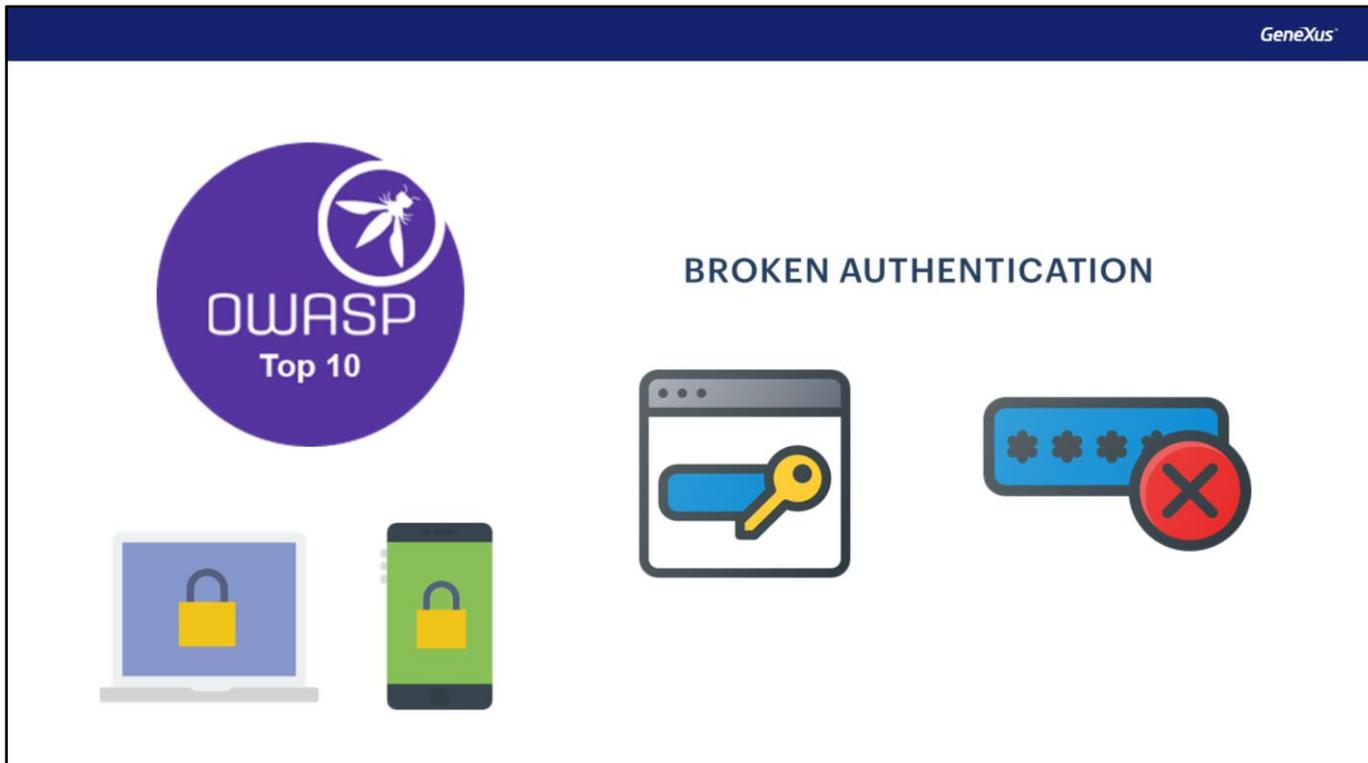
Introducción a GeneXus Access Manager

GeneXus 16



En el desarrollo de nuestras aplicaciones existen diversos lineamientos de seguridad que hay que tomar en cuenta. Los más importantes se encuentran descritos en el Open Web Application Security Project (OWASP).

La Fundación OWASP que gestiona este proyecto, es una comunidad abierta que define y provee información, además de herramientas para el desarrollo y la verificación de sistemas informáticos desde una perspectiva de seguridad.



Dentro del OWASP existen varios proyectos. Uno de los más destacados y con mayor relevancia es el **OWASP Top 10**, un documento que trata sobre los riesgos de seguridad más críticos en las aplicaciones web y móviles.

En uno de los puntos del proyecto habla sobre la **Broken authentication** donde resalta la importancia de tener un buen factor de autenticación.



GeneXus ofrece un módulo denominado Genexus Access Manager (GAM) que resuelve la Autenticación en forma automática. Además de esta tarea, el GAM también permite solucionar problemas de Autorización, es decir restringir el acceso a distintas partes de la aplicación, dependiendo de los roles o permisos de cada usuario.

El GAM también nos proporciona diversos objetos para administrar todos los problemas de seguridad relacionados con una aplicación web o para dispositivos móviles. Por ejemplo objetos para agregar usuarios, asignar roles, otorgar permisos, etc.

Enabled Integrated Security

The image shows two windows from the GeneXus application. On the left is the 'Preferences' window, which has a tree view. The 'Travel_Agency' folder is expanded, and the 'Travel_Agency' sub-folder is selected. A red arrow points from this selection to the 'Properties' window on the right. The 'Properties' window shows a table of settings for the selected version. The 'Enable Integrated Security' property is highlighted with a red box and is currently set to 'False'.

Version: Travel_Agency	
Significant attribute name length	30
Significant table name length	30
Significant object name length	128
Preserve Table Casing	True
Generate prompt programs	Yes
LIKE escape character	None
Enable Integrated Security	False
External Storage	
Compatibility	
User interface	
Defaults	
Images	
Team Development	
Workflow	
Patterns	

La activación de los controles de seguridad se realiza automáticamente mediante la configuración de la propiedad [Enable Integrated Security](#), que podemos encontrar en la ventana de Preferences, seleccionando la versión activa de nuestra KB.

Importación de objetos GAM

The image shows two windows from the GeneXus application. On the left is the 'Enable Integrated Security' dialog box. It contains the following text: 'Enabling Integrated Security imports GeneXus Access Manager (GAM) components to the Knowledge Base, providing authentication and security to your applications. You will be able to manage users, roles and permissions to control access to your application (authentication), and to grant access permissions to your programs (authorization). Please select the additional objects you want to import and how to manage their future upgrades.' Under 'Additional Components', there are two checkboxes: 'Web backend panels and Web security objects. If you select this option, a new theme will be imported also.' (checked) and 'Smart Devices security panels' (unchecked). Below this is a dropdown menu for 'Select how to manage the future upgrades:' with 'Prompt me to update' selected. At the bottom, it asks 'Do you want to Enable Integrated Security?' with 'Yes' and 'No' buttons. A red arrow points from the 'Yes' button to the 'KB Explorer' window on the right. The 'KB Explorer' window shows a tree view of the Knowledge Base structure. Under the 'Root Module' folder, two folders are highlighted with a red box: 'GAM_Examples' and 'GAM_Library'. Other folders visible include 'Travel_Agency', 'Main Programs', 'GeneXus', 'Scheduler', and 'SmartDevicesApi'.

Al cambiar la propiedad Enabled integrated Security a True se importarán los componentes del GeneXus Access Manager a nuestra KB. Bajo el Root Module, veremos carpetas que contendrán varios objetos encargados de proveer las funciones del GAM.

Integrated Security Level

Version: Travel_Agency	
Significant attribute name length	30
Significant table name length	30
Significant object name length	128
Preserve Table Casing	True
Generate prompt programs	Yes
LIKE escape character	None
Enable Integrated Security	True
Integrated Security	
Integrated Security Level	Authentication
Application ID	None
> Web specific	Authentication
> SmartDevices specific	Authorization
> External Usage	
> Compatibility	

Una vez habilitada la seguridad se puede seleccionar el nivel de la misma utilizando la propiedad Integrated Security Level, que podemos encontrar a nivel de la versión de la KB o de cada objeto. El valor por defecto de esta propiedad es Authentication.

Algunas opciones para el nivel de seguridad de nuestra aplicación son:

Ninguna, es decir no aplica ningún mecanismo de seguridad.

Autenticación, donde el usuario necesita solo estar logueado para acceder

Autorización, donde el usuario necesita además de estar logueado, tener los permisos necesarios para acceder a cada parte de la aplicación

The image shows a screenshot of the GeneXus software interface. On the left, there is a 'KB' icon representing a knowledge base, consisting of three server racks with a checkmark in a yellow circle. Below this is the GeneXus logo with 'ACCESS MANAGER' underneath. At the bottom, there is a plus sign and the text 'Rebuild All'. On the right, a 'Preferences' window is open, showing a tree view of settings. The 'Data Stores' folder is expanded, and 'GAM (SQL Server)' is selected and highlighted with a red box. Other options in the tree include 'Default (SQL Server)', 'Deployment Units', 'Team Development', 'GeneXus Cloud', 'Patterns', and 'Workflow'.

Una vez aplicada la seguridad y el tipo de nivel que utilizará nuestra aplicación, necesitamos dar un **Rebuild all** a nuestra KB para que se cree la base de datos que utilizará el GAM.

• User must be authenticated. (GAM104)

LOGIN

DON'T HAVE AN ACCOUNT? REGISTER

 Keep me logged in
 Remember Me

[FORGOT YOUR PASSWORD?](#)

User Name: admin
Password: admin123

Después de que activamos la seguridad, al ejecutar nuestra aplicación se desplegará una pantalla de login tanto en la parte web como smart devices.
Como aún no hemos configurado usuarios, podemos utilizar un usuario local con las siguientes credenciales: usuario: admin y contraseña: admin123.

Acceso al panel GAM HOME

The screenshot displays the 'Users' management interface in the GeneXus Access Manager. The header includes 'GENEXUS ACCESS MANAGER', navigation tabs for 'USERS', 'ROLES', and 'SETTINGS', and a user profile for 'Administrator'. Below the header, there is a search bar with the text 'Try a Search' and a '+ ADD' button. The main content area features a table with the following data:

User Name	First Name	Last Name	Authentication	
<u>admin</u>	Administrator	User	local	EDIT

At the bottom of the table, there are navigation controls: 'FIRST', 'PREV', and 'NEXT'.

Para poder acceder a la consola de administración del GAM, debemos acceder al panel GAM HOME que estará listado en el Developer Menu. Este panel es el objeto backend principal del GAM donde podemos configurar los usuarios y los permisos de nuestra aplicación.

DEMO

Veamos una pequeña demostración.

GET
READY
TO EXPLORE

The new age of EXPLORATION

CONTACT US TODAY →

At Travel Agency, we have consultants with an average of 20 years experience and a passion for travel available who will work out the details and create unforgettable vacations.

We will work with you to plan a worry free adventure that meets your travel needs,

[DEMO: <https://youtu.be/hhgWSZu1nkc>]

Tipo de autenticación



Local



Social Media



Web Service



Hasta ahora solo hemos utilizado la autenticación de los usuarios locales pero podemos utilizar otro tipo de autenticación como Facebook, Twitter, Google o de algún servicio externo. Cabe destacar que la versión 16 de GeneXus puede realizar la autenticación con cualquier proveedor que utilice Oauth 2.0.

OAuth es un estándar para otorgar acceso a los sitios web o aplicaciones desde otro sitio web pero sin otorgar las contraseñas.

Una de las ventajas del Oauth 2.0 es que se verifica la identidad del usuario y emite un token a la aplicación para otorgar acceso, lo cual hace mucho más segura la autenticación en nuestra aplicación.



<https://wiki.genexus.com/commwiki/servlet/wiki?24746>

Para saber más sobre el GeneXus Access Manager, visite el siguiente link del Wiki:
<https://wiki.genexus.com/commwiki/servlet/wiki?24746>

GeneXus[™]

The power of doing.

Videos

training.genexus.com

Documentation

wiki.genexus.com

Certifications

training.genexus.com/certifications