The User contributions web parts use the following properties to configure their security options:

- **Check permissions** – if you select this option, appropriate permissions to read/modify/create/delete pages using the User contributions web parts need to be granted to the users. See Configuring permissions for more details on page permissions.
- **Insert requires page type permission** – indicates if page type permissions are required to create a new page.
- **Allow insert/edit/delete** – indicates if the web part displays the corresponding buttons.
- **Allow editing by users** – you can choose between:
  - **All –** any user who comes to a page that contains the web part can use it to edit the pages.
  - **Authenticated** – any authenticated user (site member) can edit the pages. You can use this value in combination with the *NodeOwner = {%CurrentUser.UserID%}* value in the *WHERE condition* property to display only pages created by the current user (to allow editing of these pages only for this user).
  - **Page owner** – only the owner of the parent page under which the user contribution pages are stored can edit them.

**Note**

When rendering data that users input through user contributions (for example in Transformations), be sure to properly escape or encode the values to protect against XSS attacks. See Cross site scripting (XSS) to learn more.

**Security for file attachments**

The system does not allow public unauthenticated users to upload file attachments.

If your user contribution page types have attachment fields, we recommend setting the **Allow editing by users** property of your web parts to *Authenticated*, or securing the entire page to require authentication. Otherwise an error will occur if a public visitor attempts to upload a file.