

Stored Cross Site Scripting (XSS)

Download Link: <https://www.campcodes.com/downloads/school-management-software-in-php-mysql-full-source-code/>

Software Name: School Management Software

Login inside admin account and traverse to the Photo Gallery “/photo-gallery” section. Enter a Javascript or HTML payload inside the “Description” field of the form. Upload any normal image and add the image to the gallery.

The screenshot shows the admin interface of the School Management Software. On the left is a sidebar with a 'Frontend CMS' menu. The main area is titled 'Photo Gallery'. It contains a form with a 'NAME' field (filled with 'Cross Site Scripting - Stored') and a 'DESCRIPTION' field (filled with the payload ''). Below the description field is a 'FEATURE IMAGE' section with a 'BROWSE' button and a small image. At the bottom of the form is an 'ADD' button. To the right is a 'Photo Gallery List' table with 6 entries. Each entry has a 'SELECT' button.

SL	Name	Description	Image	Action
1	Pre-Primary	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
2	Kindergarden	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
3	Celebration	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
4	Recreation Centre	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
5	Facilities	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
6	Activities	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT

This screenshot shows the same interface as the previous one, but after the payload has been successfully added to the gallery. The 'DESCRIPTION' field is now empty. The 'FEATURE IMAGE' section now shows a small image of a person. The 'ADD' button is now labeled 'ADD'. The 'Photo Gallery List' table now has 7 entries, with the 7th entry being 'Cross Site Scripting - Stored' with the payload ''. A green success message 'Success Operation successful!' is displayed at the top right. The footer shows 'Copyright © 2025 All rights reserved | This application is made with by Codethemes'.

SL	Name	Description	Image	Action
1	Pre-Primary	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
2	Kindergarden	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
3	Celebration	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
4	Recreation Centre	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
5	Facilities	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
6	Activities	Fusce semper, nibh eu sollicitudin imperdiet, dolo		SELECT
7	Cross Site Scripting - Stored			SELECT

Once the file gets uploaded with the Javascript payloads, go to the main website and traverse to “/gallery” as shown in the below screenshot. It can be observed that the entered Javascript payload gets executed and an alert/popup gets generated as a result.

