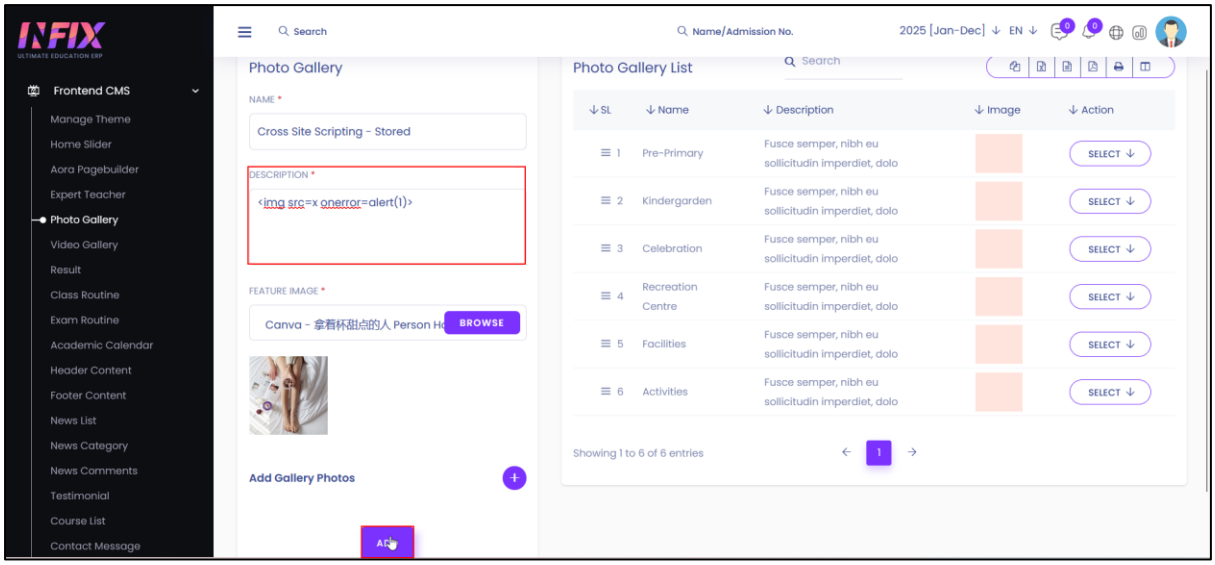
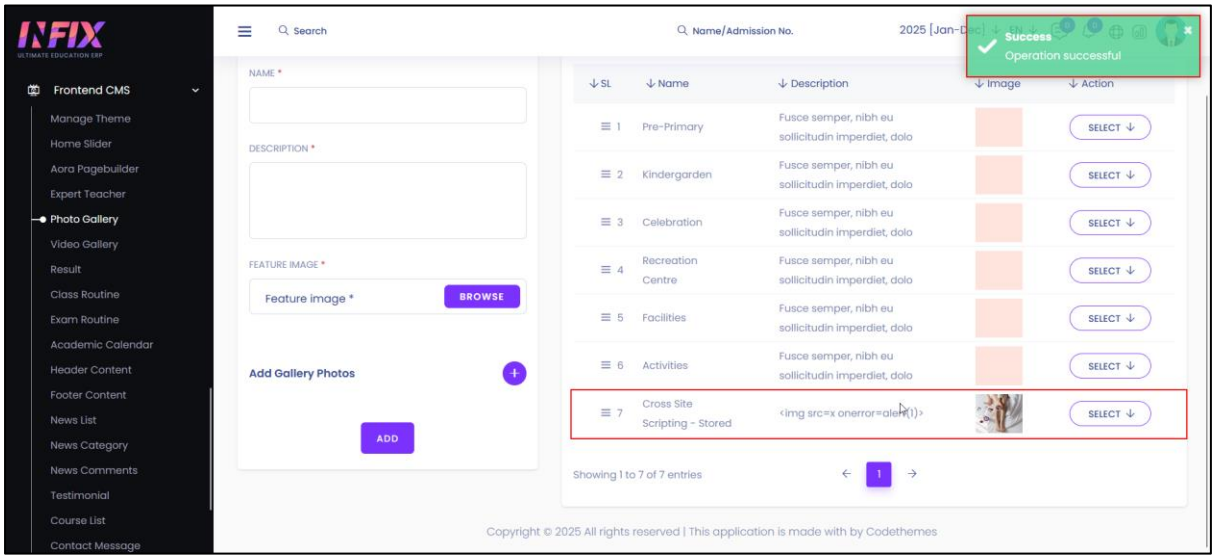
Stored Cross Site Scripting (XSS)

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.





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.