

Security Assessment Report for Opencart

Vulnerability : Stored Cross Site Scripting (XSS)

Severity : High

Vulnerable option : Image Manager's Folder Creation

Payload Used : Demo">

Steps to reproduce :

Step 1 : Login in any **Seller** account and go to **Product** option and here edit/add any product's image. Open Image viewer and try to create one new folder. Here in input box, add **XSS payload** and click on **+** icon to save this folder.

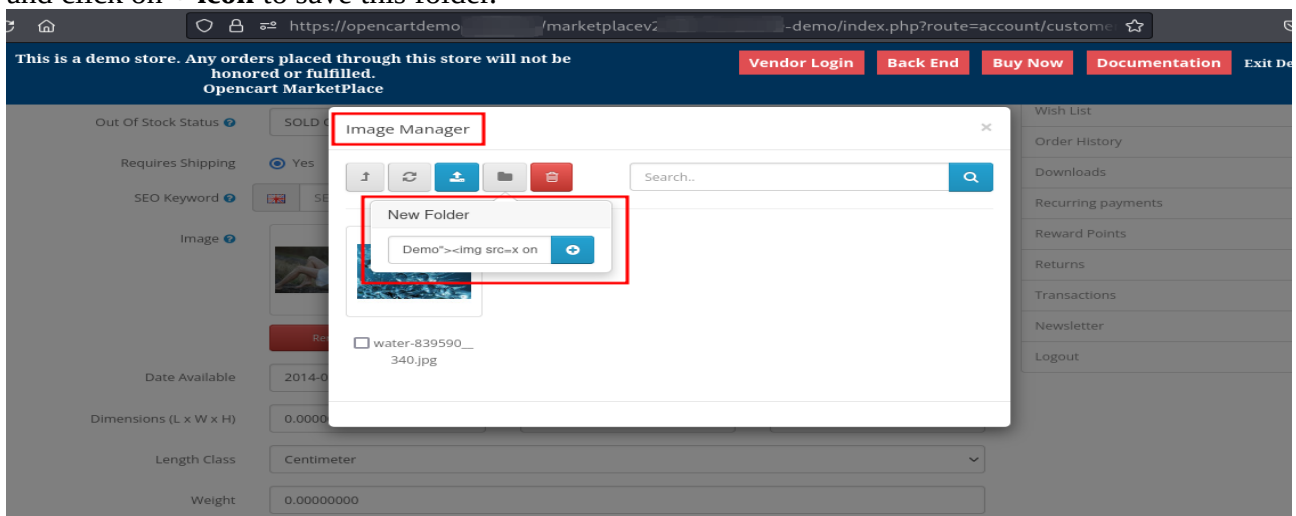


Fig-1

Step 2 : As we save this folder name, Our XSS payload has been executed and we can see a popup is displayed on the screen as shown in the screenshot below;

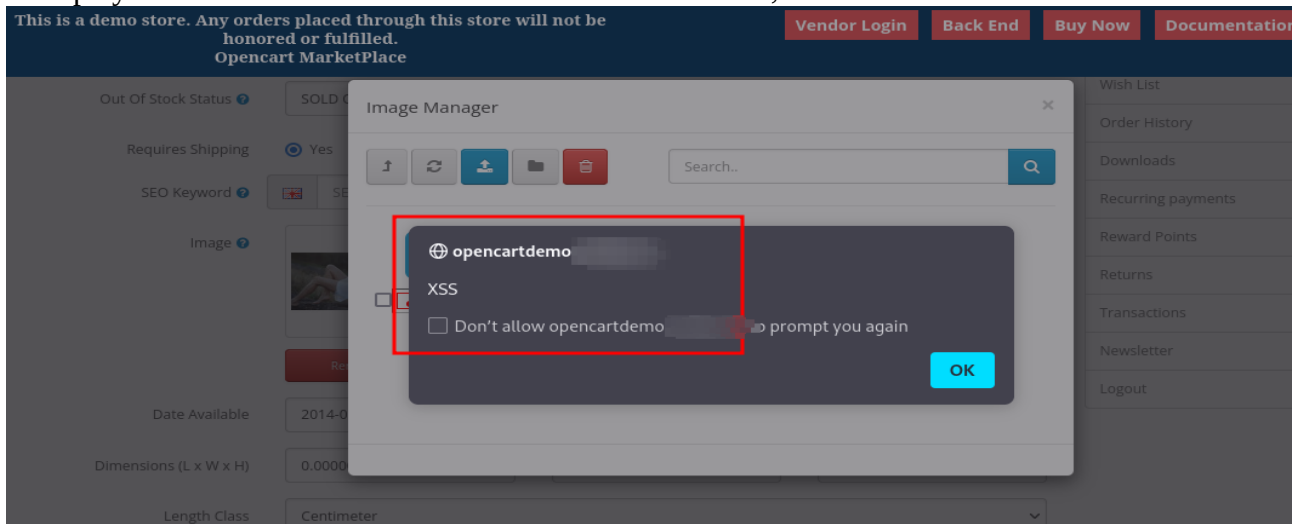


Fig-2

Step 3 : We can see that folder name with XSS payload in the screenshot below;

This document contains sensitive information

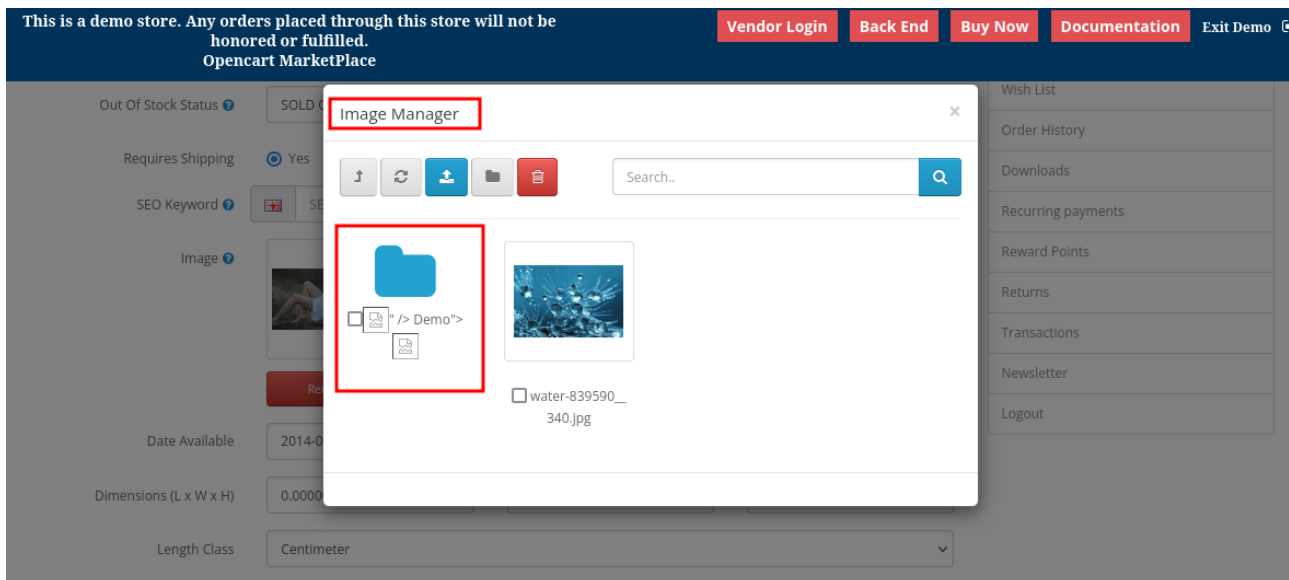


Fig-3

So It verifies the existence of Stored XSS Vulnerability here.

NOTE : This payload is stored in this image manager, whenever this image manager will be open, this payload will be executed at the same time. This issue is exist everywhere where Image Manager is used to upload and view images and folder.

Impact :

- Attacker can steal the cookies of the logged in user.
- Attacker can perform any malicious action using this vulnerability.
- This vulnerability can impact the complete functionality of the website.

Recommendation :

- Encode text at Client side.
- Encode text on the arrival of output also.
- Encode text before sending mail as it can be executed in mail also.
- Use Web Application firewall to prevent application from attack.
- Use Whitelisting approach instead of Blacklisting.
- Do not directly display the same name as folder name.

Prevention Cheat Sheet for developer :

- https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html

END OF THE REPORT