PrestaShop / **PrestaShop** Public

Code Issues 2.4k Pull requests 197 Actions Projects 8 ···

New issue

Jump to bottom

Cross Site Scripting Issue in PrestaShop Using File Upload Functionality #20306

Closed **p1nk15amak** opened this issue on Jul 23, 2020 · 3 comments

Labels **No change required**

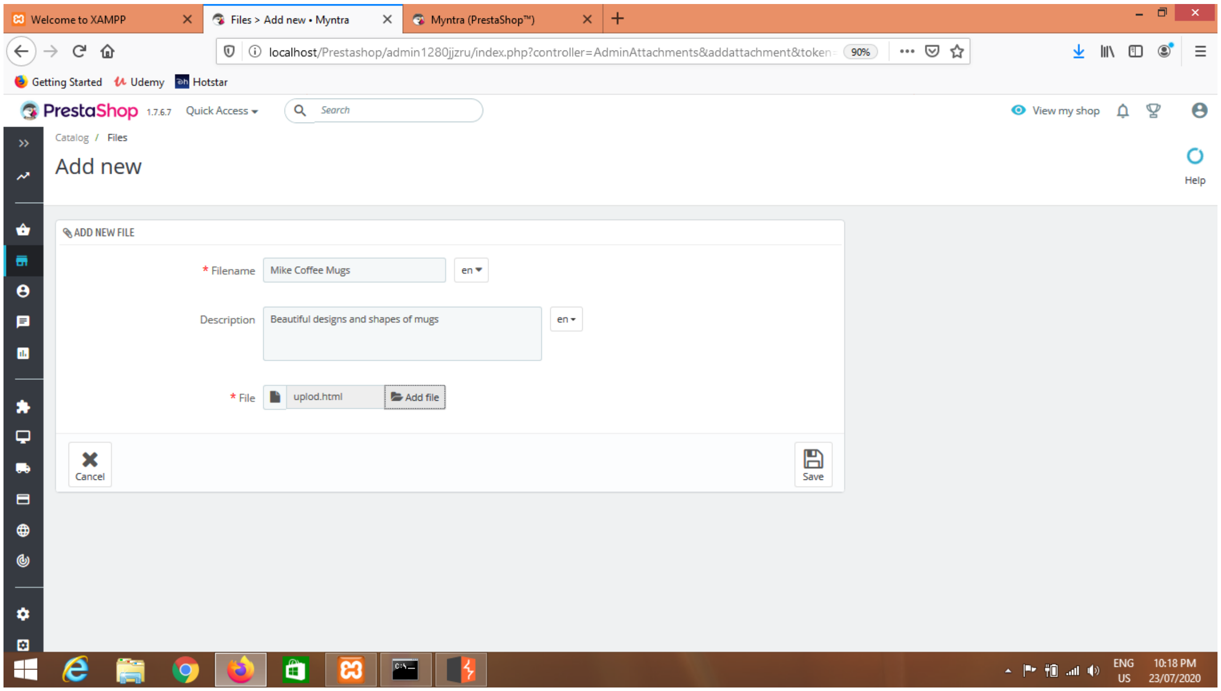
p1nk15amak commented on Jul 23, 2020

An issue is discovered in PrestaShop version 1.7.6.7 under the Catelog feature when using the file-upload functionality for uploading the Files for various products. This issue exists because it fails to implement file content checks and improperly handles the output, resulting in cross-site scripting attack that leads to cookie stealing or malicious actions.

Steps to Reproduce

1. Go to Catelog feature
2. Click on File component and add the details accordingly.
3. Create a file with .html extension and enter the payload <script>alert('XSS!!');</script>within it. (Here its, uplod.html)
4. Upload the file
5. Login as customer and click on the file uploaded for the particular product.
6. You can see the XSS payload gets executed.

CVSS Score:
CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:N

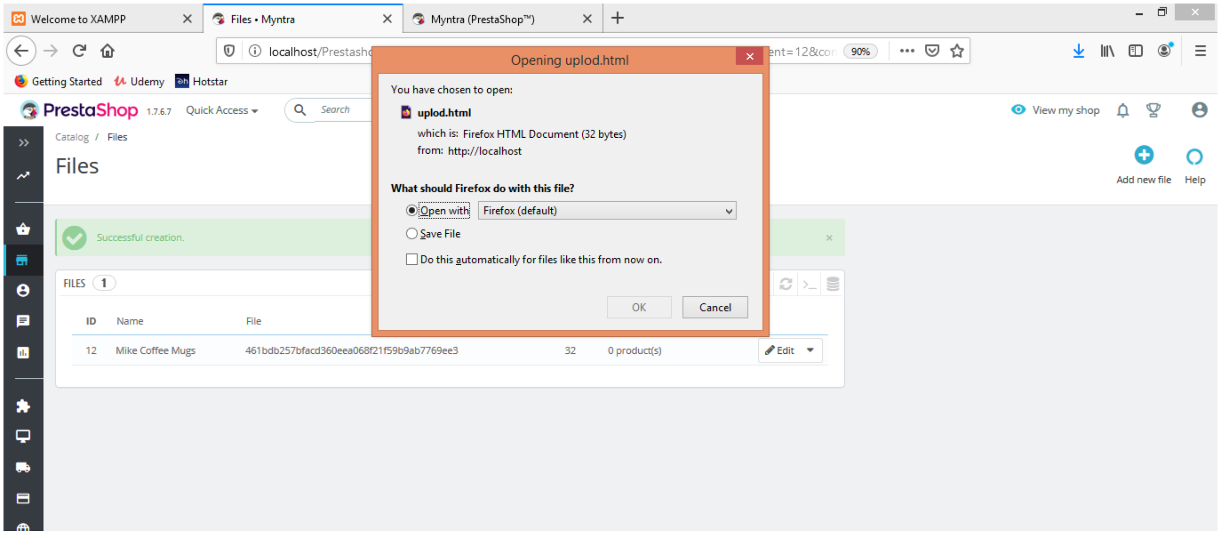

localhost/Prestashop/admin1280jjzru/index.php?controller=AdminAttachments&addattachment&token

Catalog / Files

Add new

ADD NEW FILE

- * Filename: Mike Coffee Mugs
- Description: Beautiful designs and shapes of mugs
- * File: uplod.html


Opening uplod.html

You have chosen to open:

uplod.html

which is: Firefox HTML Document (32 bytes)
from: http://localhost

What should Firefox do with this file?

● Open with: Firefox (default)
○ Save File
□ Do this automatically for files like this from now on.

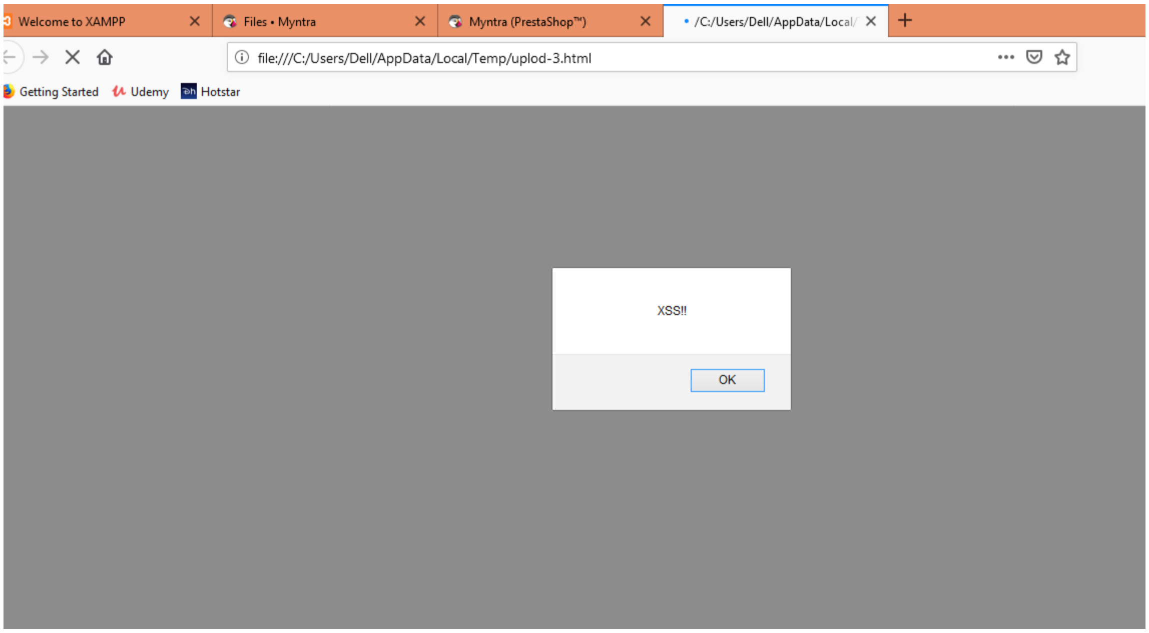
OK Cancel

Files

Successful creation.

FILES 1

ID	Name	File			
12	Mike Coffee Mugs	461bdb257bfacd360eea068f21f59b9ab7769ee3	32	0 product(s)	Edit


file:///C:/Users/Dell/AppData/Local/Temp/uplod-3.html

XSS!!

OK

prestashop-issue-... bot commented on Jul 23, 2020

Thanks for opening this issue! We will help you to keep its state consistent

matks commented on Jul 24, 2020 Contributor

Hi **@p1nk15amak** ! thank you for the report

Am I wrong if I guess that you had a look at our newly opened bug bounty and that you found this while bug hunting, but since the CVS score is low, you reported it here ?

PierreRambaud commented on Jul 24, 2020 Contributor

Hi,

This is something we already received on the Bug Bounty program.
Unfortunately, this is not a security issue, as we allow to upload any files we wanted, (it's the same for SVG files), any users with admin employee can upload this kind of file, like he's able to upload a module or a theme with comprised data.

Kind regards

👍 1

PierreRambaud closed this as completed on Jul 24, 2020

florine2623 added the **No change required** label on Jul 24, 2020

Assignees

No one assigned

Labels

No change required

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants