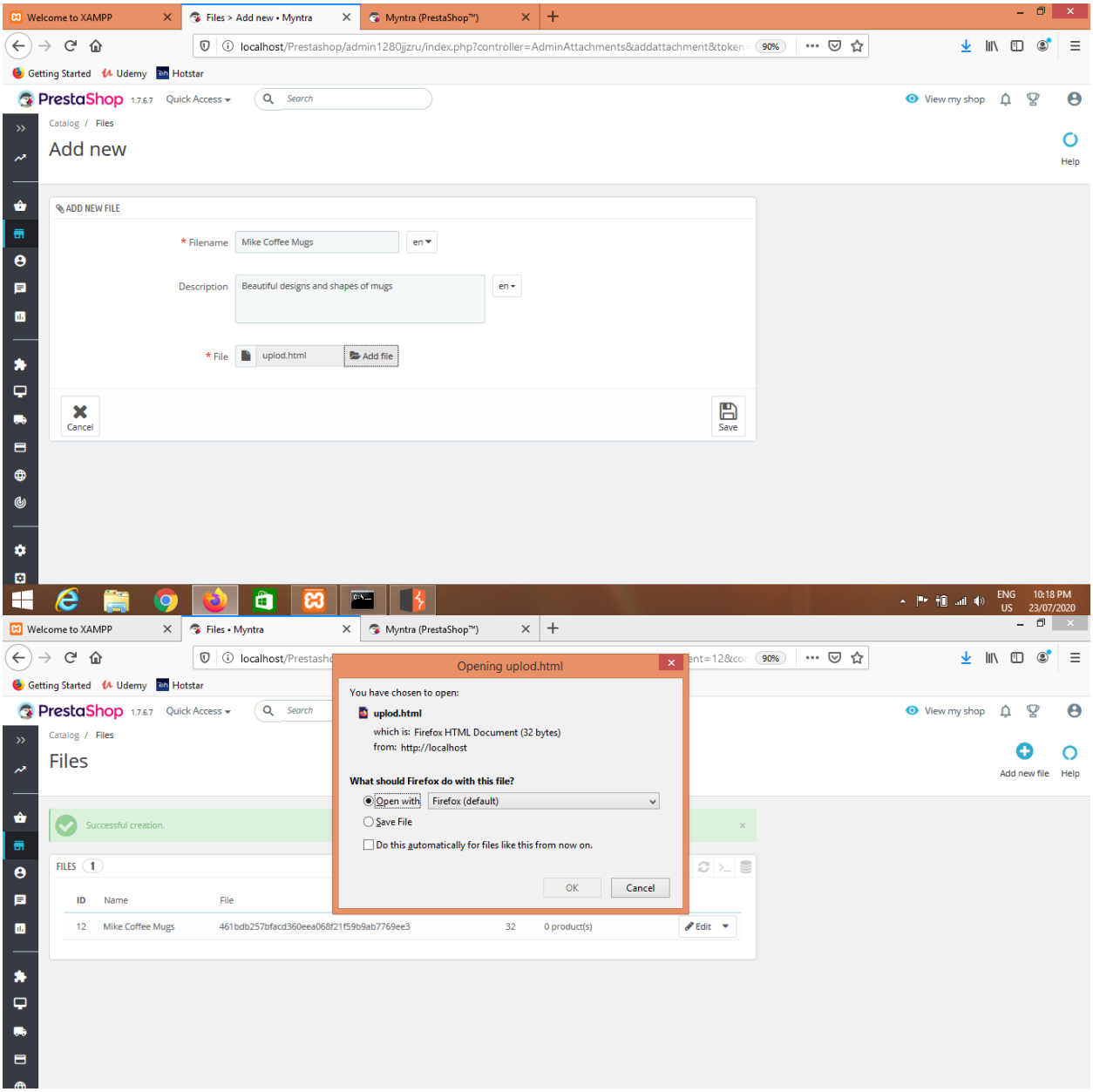
An issue is discovered in PrestaShop version 1.7.6.7 under the Catelog feature when using the file-upload functionality for uploading the Files for various products. This issue exists because it fails to implement file content checks and improperly handles the output, resulting in cross-site scripting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

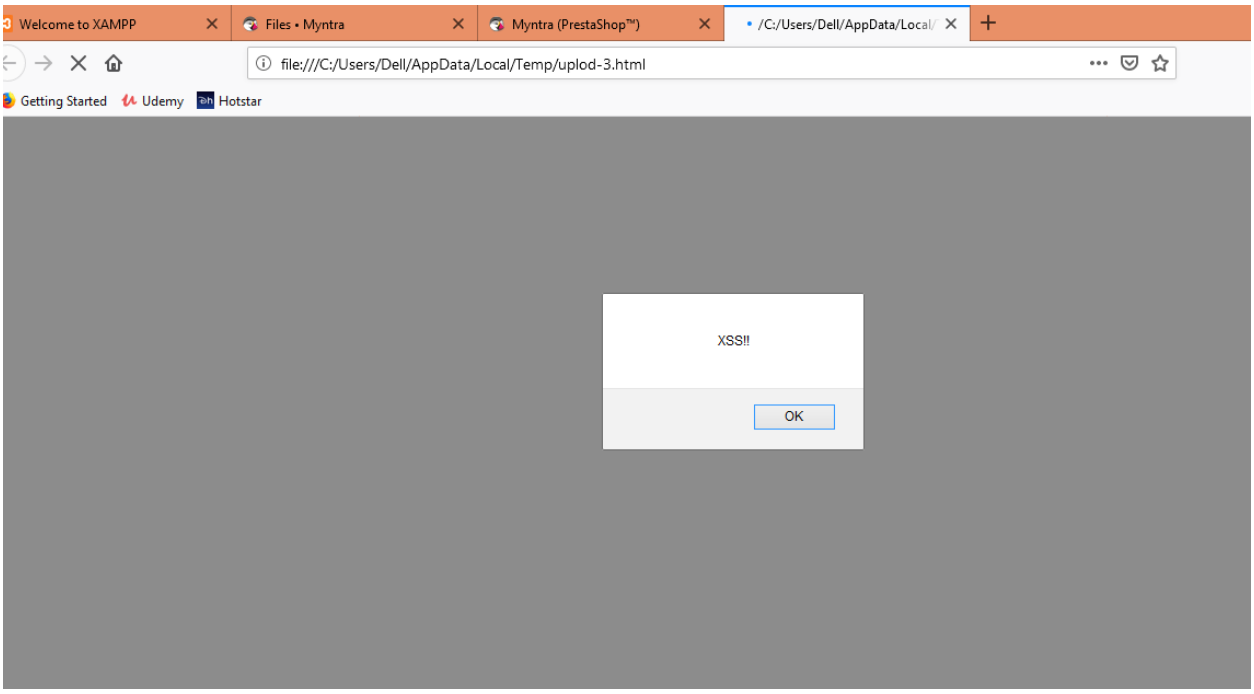
**Steps to Reproduce**

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

I have got ***CVE-2020-21967*** assigned to the issue.


Welcome to XAMPP
Files > Add new • Myntra
Myntra (PrestaShop™)
localhost/Prestashop/admin1280jjzru/index.php?controller=AdminAttachments&addattachment&token
Getting Started
Udemy
Hotstar
PrestaShop 1.7.6.7
Quick Access
Search
View my shop
Catalog / Files
Add new
Help
ADD NEW FILE
* Filename
Mike Coffee Mugs
en
Description
Beautiful designs and shapes of mugs
* File
uplod.html
Add file
Cancel
Save
ENG US
10:18 PM 23/07/2020
Files • Myntra
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
Add new file
Successful creation.
FILES 1
ID
Name
File
12
Mike Coffee Mugs
461bdb257bfacd360eea068f21f59b9ab7769ee3
32
0 product(s)
Edit


Welcome to XAMPP
Files • Myntra
Myntra (PrestaShop™)
• /C:/Users/Dell/AppData/Local/
file:///C:/Users/Dell/AppData/Local/Temp/uplod-3.html
Getting Started
Udemy
Hotstar
XSS!!
OK