New issue

# Vulnerability Arbitrary Image Upload + XSS Via Image Name #151

**Open**

jeagercoder opened on Nov 30, 2021

https://github.com/pylixm/django-mdeditor/blob/master/mdeditor/views.py

1.no authentication check so anyone can upload image file
2.Name of uploaded file is not cleaned so it is vulnerable to XSS attack, one can upload file with name like: "><script>alert(1)</script>

pylixm on Dec 1, 2021 Owner

**@zonefteam** Thank you for your reminder, I will fix it later.

Before releasing the new version, I hope everyone can check whether the problem will bring security risks to their services.

**pylixm** pinned this issue on Dec 1, 2021

jeagercoder on Feb 16, 2022 Author

of course because it is a security vulnerability.

1. arbitrary file upload
   2, XSS stored

in our community there are some people who use django mdeditor, after I told them they immediately disabled the vulnerable upload feature

**lenoctambule** mentioned this on Oct 30, 2024

Added file format check and option to require authentication to upload files #185

**nixpkgs-security-tracker** mentioned this 2 days ago

All versions of the package django-mdeditor are vulnerable to Missing … NixOS/nixpkgs#515462

**augustebaum** added 2 commits that reference this issue 2 days ago

`django-mdeditor: drop ···` `f46d5b1`

`python3.pkgs.django-mdeditor: drop ···` `2f12c1e`

**augustebaum** mentioned this 2 days ago

python3.pkgs.django-mdeditor: drop NixOS/nixpkgs#515503

**augustebaum** added 3 commits that reference this issue 19 hours ago

`python3.pkgs.django-mdeditor: drop ···` `70e9d6b`

`python3.pkgs.django-mdeditor: drop ···` `e753d7e`

`python3.pkgs.django-mdeditor: drop ···` `03dac7c`



## Metadata

**Assignees**

No one assigned

**Labels**

No labels

**Projects**

No projects

**Milestone**

No milestone

**Relationships**

None yet

**Development**

No branches or pull requests

**Participants**