

pylixm / django-mdeditor Public[Code](#) [Issues 20](#) [Pull requests 5](#) [Discussions](#) [Actions](#) [Projects](#)[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](#)

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants



