

New issue

[Jump to bottom](#)

Stored-Cross-Site-Scripting (XSS)-vulnerabilities(authenticated)--1 #484

✓ Closed

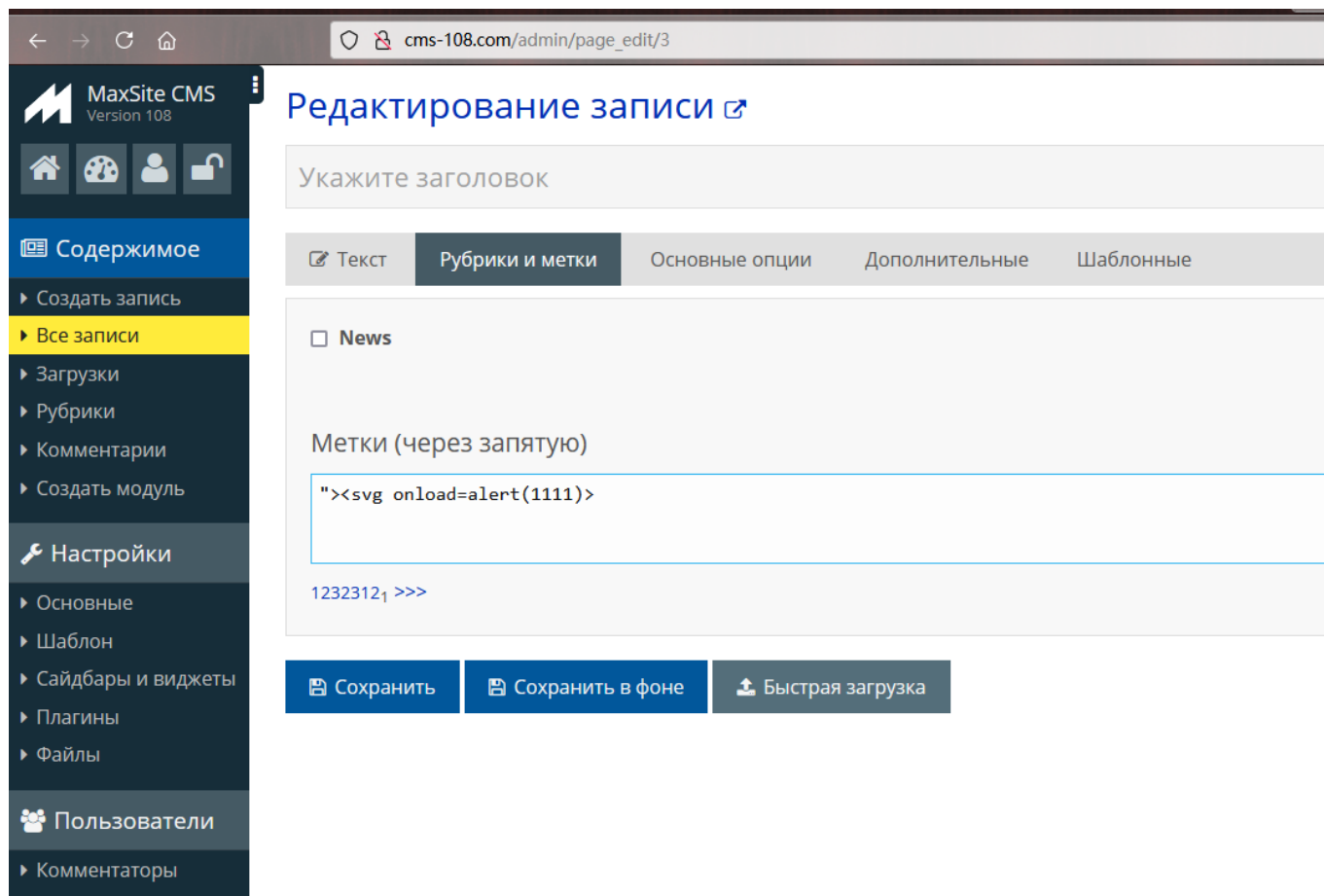
fuzzyap1 opened this issue on Feb 17 · 1 comment

fuzzyap1 commented on Feb 17 • edited ▼

Stored-Cross-Site-Scripting (XSS)(authenticated)

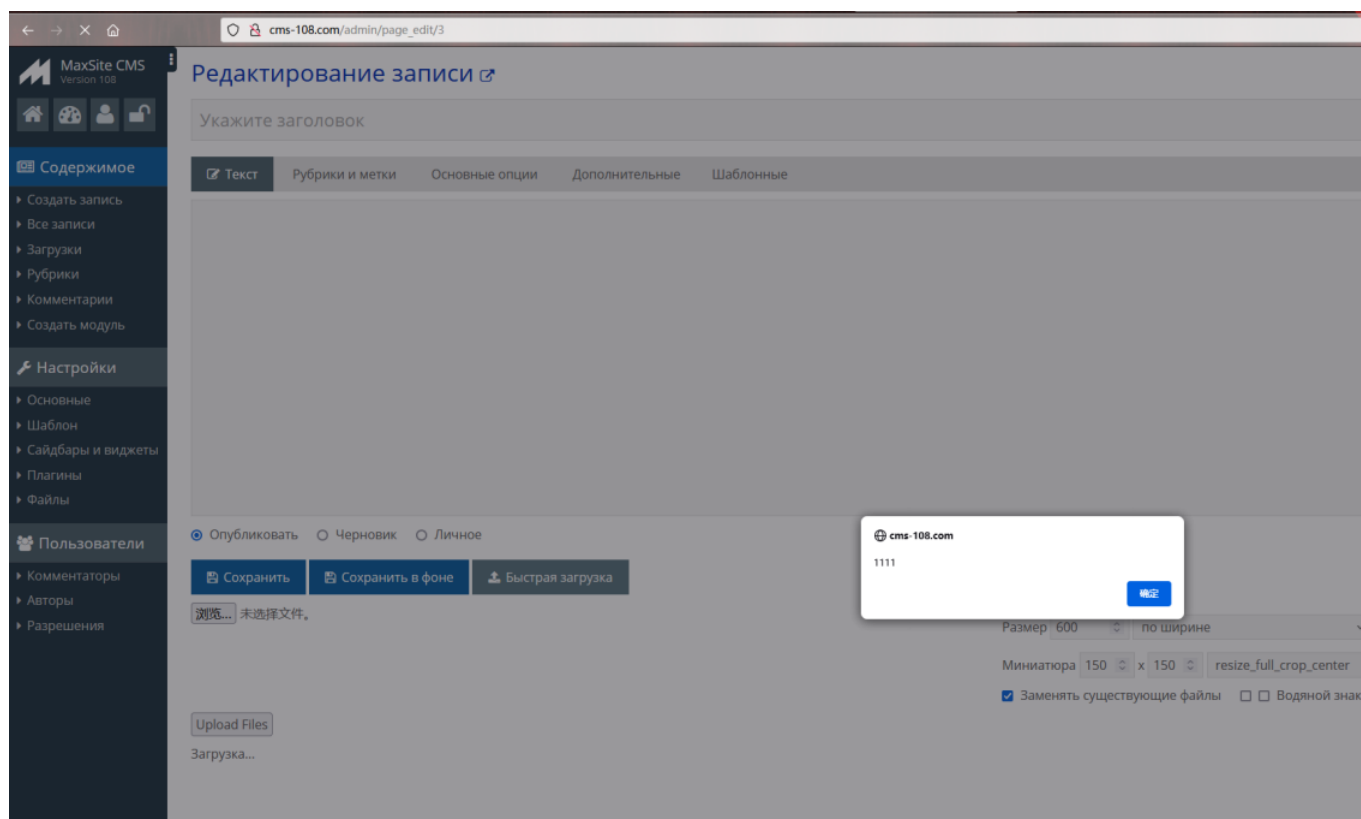
a stored cross-site scripting (XSS) in maxsite cms version 108 targeted towards web admin through ~/admin/page_edit/3 at via the parameter f_tags.

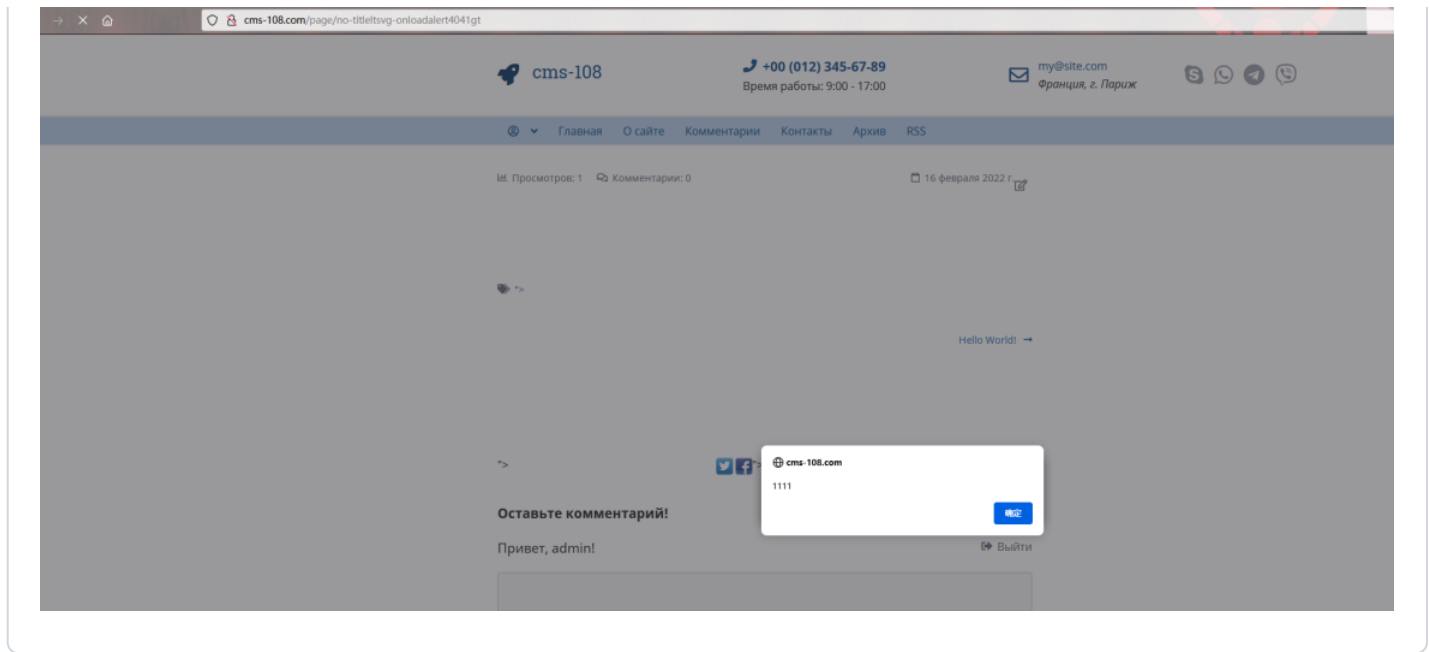
1. Navigate to admin page, ~/admin/page_edit/ and make a new page
2. click in "Рубрики и метки">"Метки (через запятую)"
3. insert xss payload "><svg onload=alert(1111)>" in the parameter f_tags



4. click save

You will observe that the payload successfully got stored into the database and when you are triggering the same functionality at that time JavaScript payload gets executed successfully and we'll get a pop-up.





 maxsite closed this as completed in [82ee32b](#) on Feb 17

fuzzyap1 commented on Feb 17

Author

update version

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant



