New issue

Jump to bottom

Stored-Cross-Site-Scripting (XSS)(authenticated) --2 #485

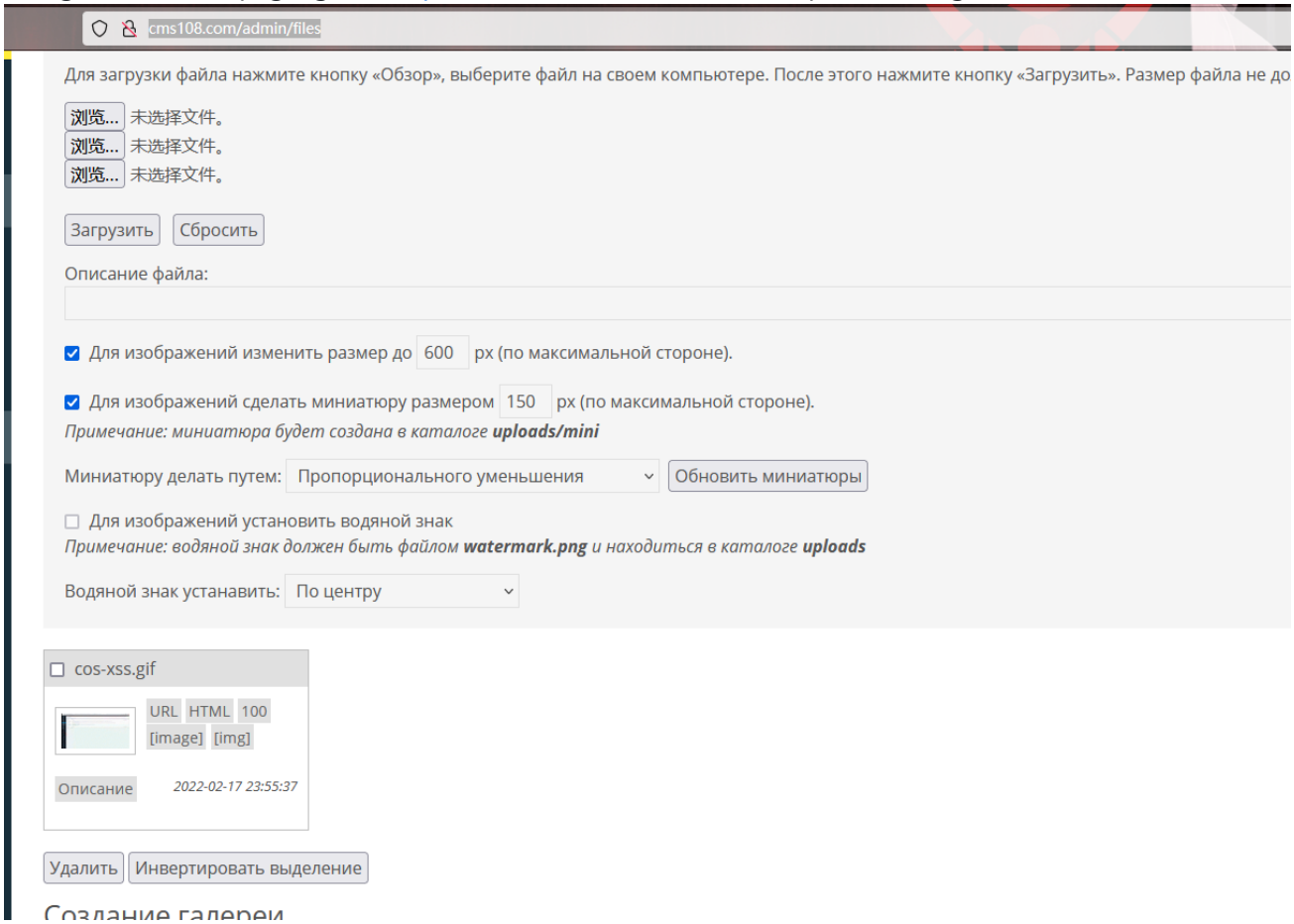
Closed **fuzzyap1** opened this issue on Feb 17 · 1 comment

fuzzyap1 commented on Feb 17

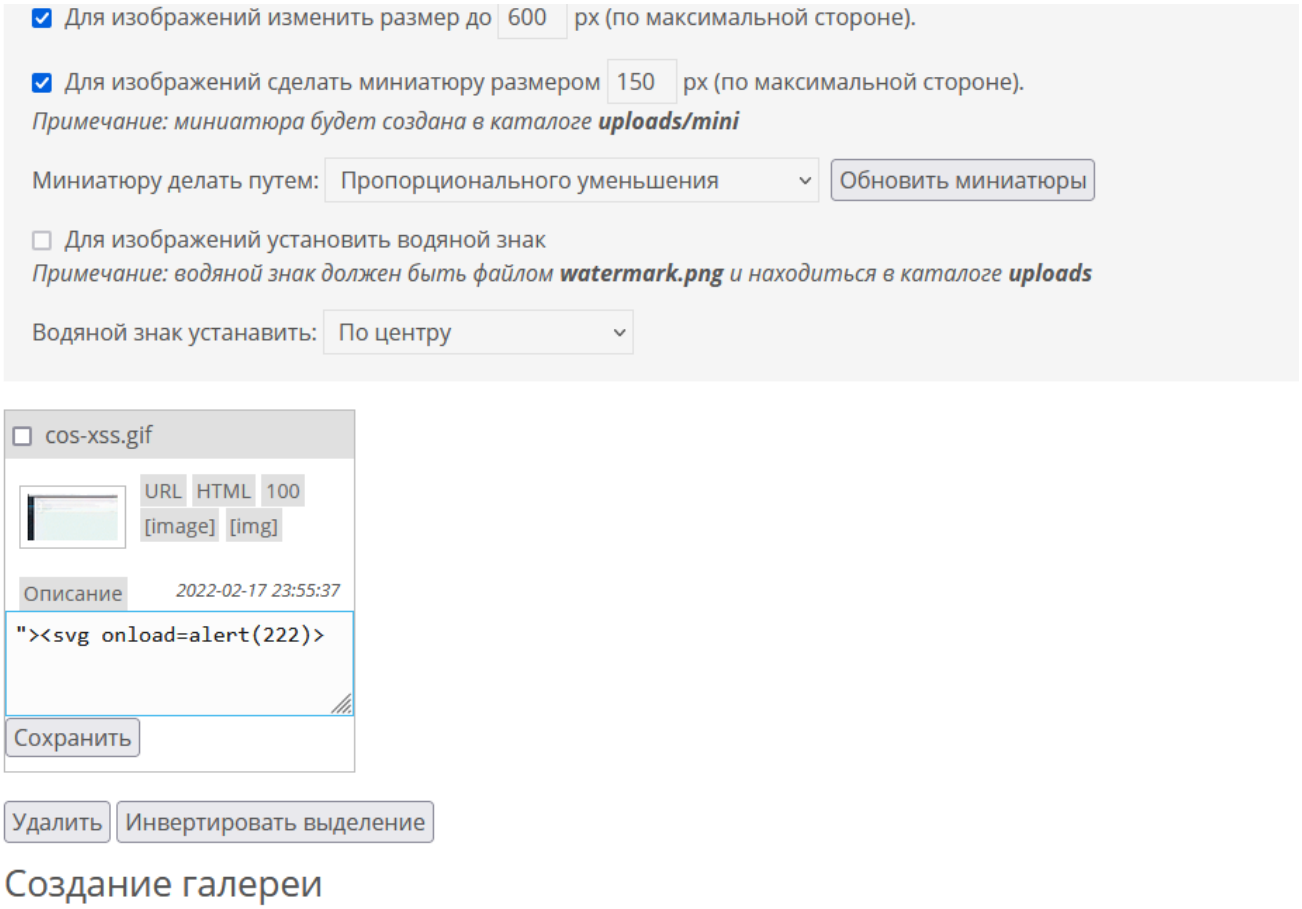
Stored-Cross-Site-Scripting (XSS) -2

a stored cross-site scripting (XSS) in maxsite cms targeted towards web admin through ~/admin/files at via the parameter f_file_description .

1. Navigate to admin page, go to http://localhost/admin/files,then update a xss.gif file

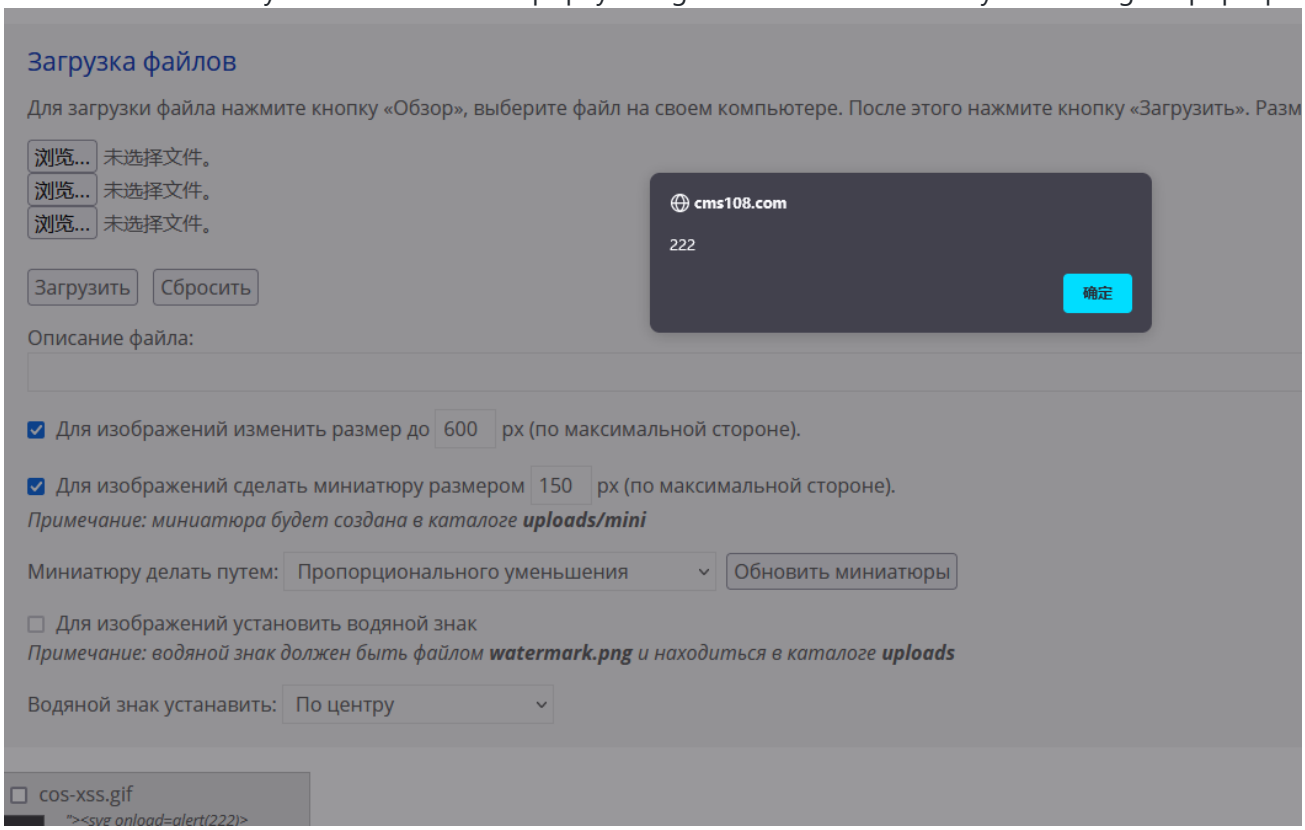


2. insert xss payload `"><svg onload=alert(222)>` in the parameter f_file_description



3. 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 `949d49b` on Feb 17

---

maxsite commented on Feb 17 — Owner

Thank you for your work!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants