New issue

Jump to bottom

Stored Cross Site Scripting Vulnerability Bypass filter on "Files" feature in webtareas 2.4p5 #8

Open **anhdq201** opened this issue on Nov 2 · 0 comments

anhdq201 commented on Nov 2 Owner

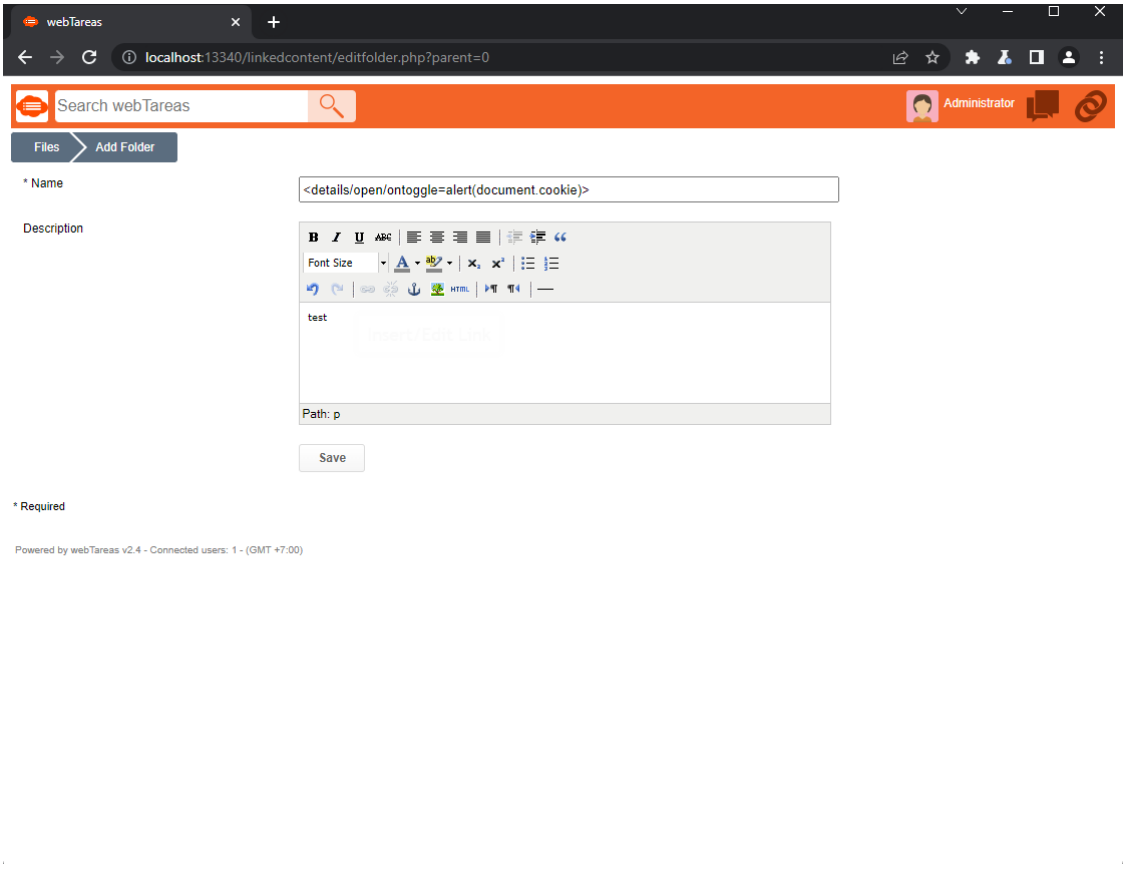
Version: 2.4p5

Description

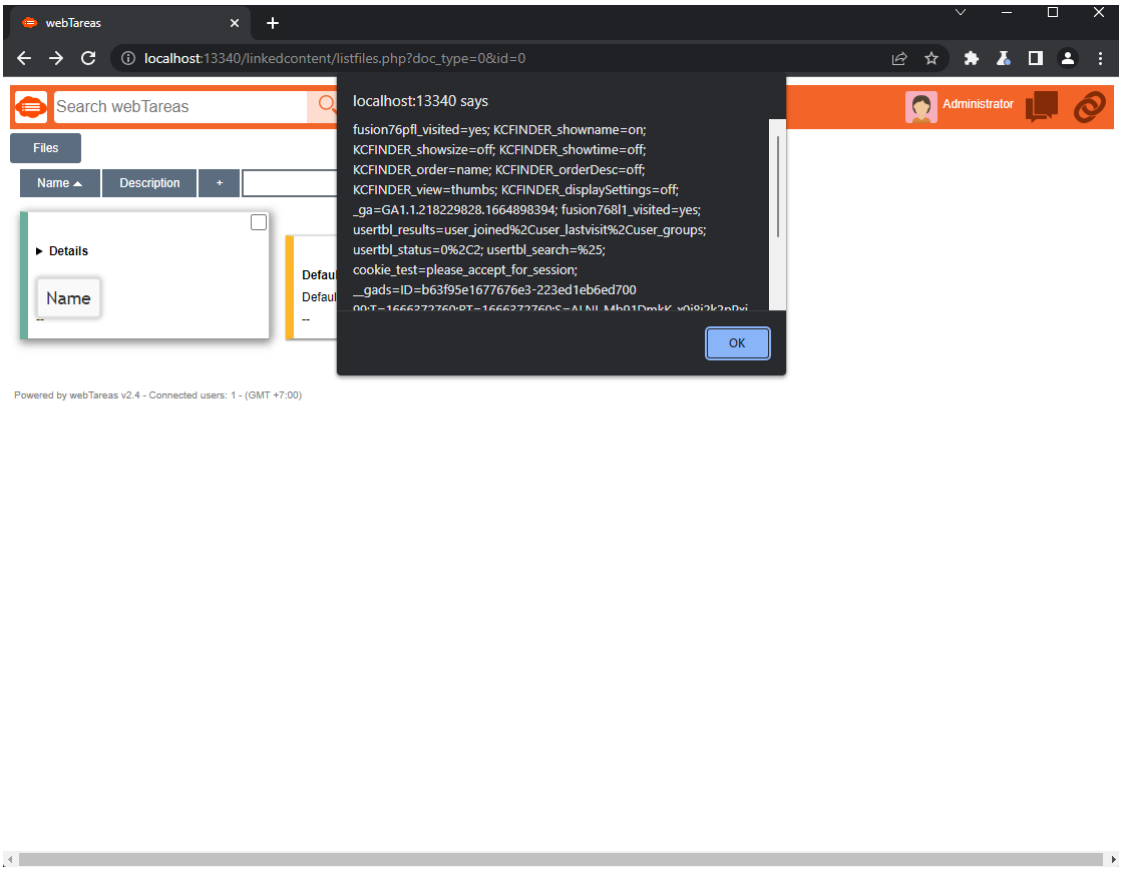
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Files" feature.

Proof of Concept

Step 1: Go to "/linkedcontent/listfiles.php?doc_type=0&id=0", click "Add" and insert payload " `<details/open/ontoggle=alert(document.cookie)>` " in "Name" field.



Step 2: Alert XSS Message



Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant