New issue

Jump to bottom

Reflect Cross Site Scripting Vulnerability Bypass filter on "Search" feature in webtareas 2.4p5 #4

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

anhdq201 commented on Nov 2 Owner

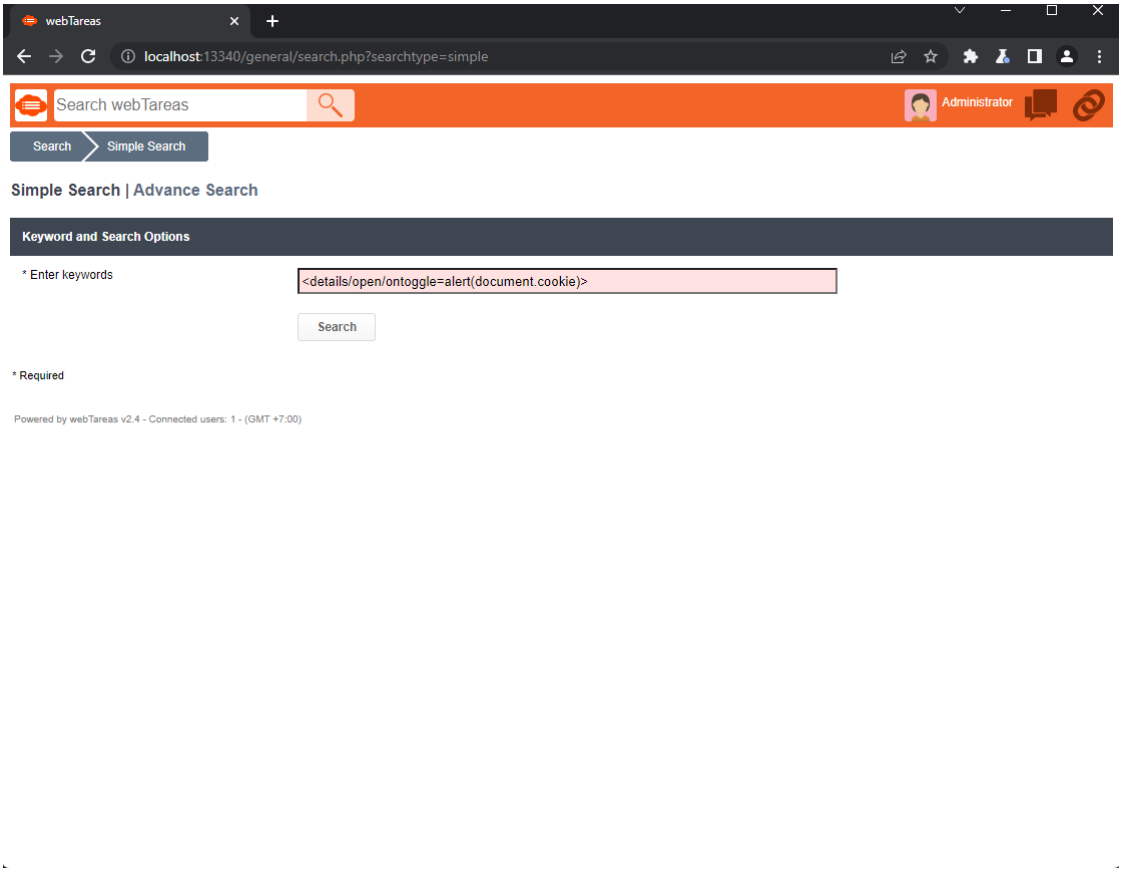
Version: 2.4p5

Description

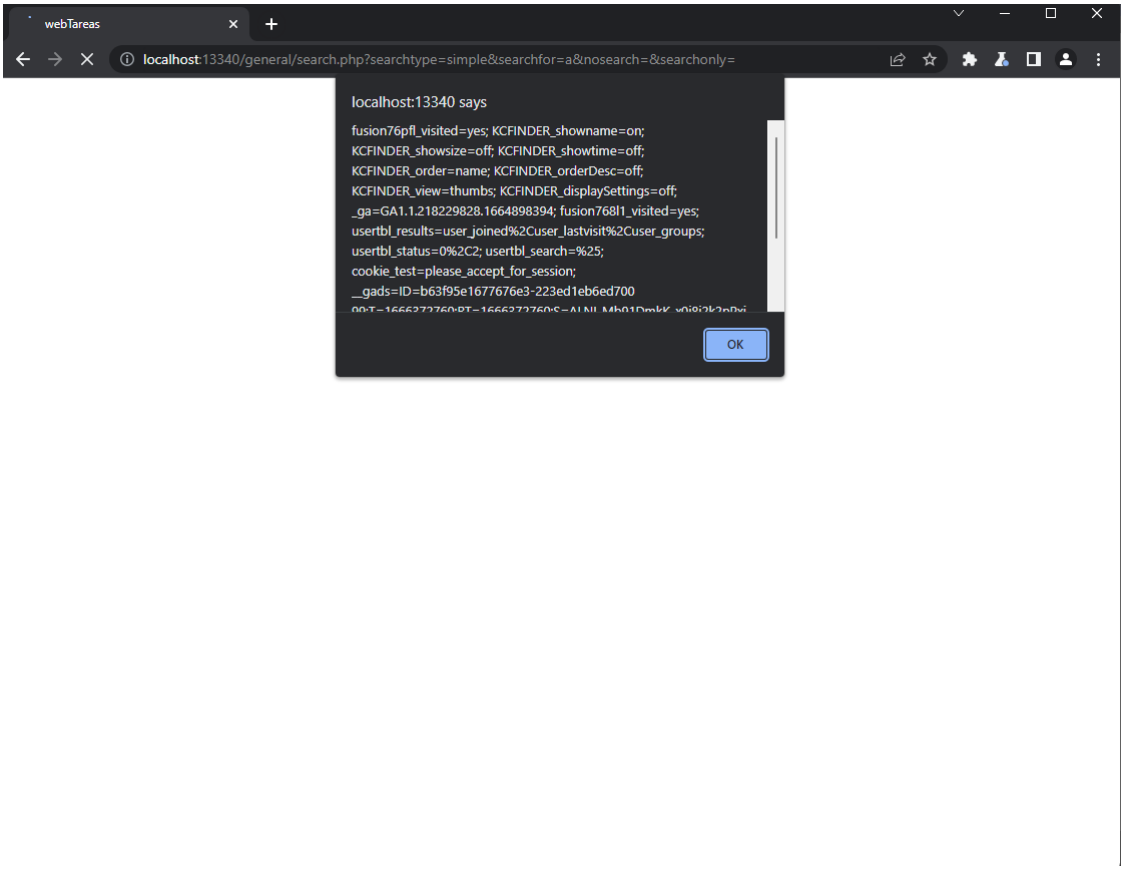
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Search" feature.

Proof of Concept

Step 1: Go to "/general/search.php?searchtype=simple", click "Search" and insert payload "`<details/open/ontoggle=alert(document.cookie)>`".



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.

anhdq201 changed the title ~~Bypass Reflect Cross Site Scripting Vulnerability on "Search" feature in webtareas 2.4p5~~ **Reflect Cross Site Scripting Vulnerability Bypass filter on "Search" feature in webtareas 2.4p5** on Nov 2

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant