

New issue

[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability Bypass filter on "Projects" feature in webtareas 2.4p5 #3

Open anhdq201 opened this issue on Nov 2 · 0 comments

anhdq201 commented on Nov 2 · edited Owner

Version: 2.4p5

Description

An authenticated malicious user can take advantage of a Stored XSS vulnerability in "Add projects" function in the "Projects" feature.

Proof of Concept

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

webTareas

localhost:13340/projects/editproject.php

Search webTareas

Administrator

ProjectsAdd Project

* Name
Priority
Description
Path: p
Owner
Type
Client Organization

ils/open?ontoggle=alert(document.cookie)>

Medium

B I U ABC [list icons] [link icon]

Font Size [dropdown] [color picker] [text color] [background color] [bold] [italic] [underline]

[undo] [redo] [find] [replace] [insert link] [insert image] [HTML] [source code]

Enable Phases
Status
Currency
Cost Method
Permission Set
Workcalendar
Project Form Templates Add

None
Initiation
USD
☒ Use the cost rate of member only
☐ Use the hourly rate of service first and use the cost rate of member if no service specified
☐ Use the hourly rate of service only
Custom (System Default)
default

Save

Attach Documents

Drop file here
or
Choose

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 ~~Stored Cross Site Scripting Vulnerability on "Projects" feature in webtareas 2.4p5~~ Stored Cross Site Scripting Vulnerability Bypass filter on "Projects" 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

