

New issue

Jump to bottom

Stored Cross Site Scripting Vulnerability Bypass filter on "Meetings" feature in webtareas 2.4p5 #6

🔗 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 "Meetings" feature.

Proof of Concept

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

The screenshot displays the 'Edit Meeting' form in the webTareas application. The form is structured as follows:

- Name:** A text input field containing the placeholder text: `<details/open/ontoggle=alert(document.cookie)>`.
- Agenda:** A rich text editor with a toolbar (bold, italic, underline, text color, background color, link, unlink, list, indent, outdent, undo, redo) and the text "test". Below the editor is a "Path:" label and a text input field containing "p".
- Location:** A rich text editor with a toolbar (bold, italic, underline, text color, background color, link, unlink, list, indent, outdent, undo, redo) and a text input field containing "p".
- Status:** A dropdown menu with the selected value "Scheduling". A tooltip is visible over this field with the text: "Rich Text Area Press ALT-F10 for toolbar. Press ALT-0 for help".
- Priority:** A dropdown menu with the selected value "Medium".
- Date/Time:** Two input fields for date and time, both showing "11/03/2022" and "00:00" respectively, followed by an "Add" button.
- Duration:** A dropdown menu showing "1" and a label "Hours".

The application interface includes an orange header bar with a search bar and a user profile icon labeled "Administrator". The left sidebar is dark and contains navigation links for "Meetings" and "Add Meeting".

### Step 2: Alert XSS Message

The screenshot shows a web browser window with the address bar displaying `localhost:13340/meetings/viewmeeting.php?id=1&msg=addMeeting#emDAnchor`. The page layout includes a top navigation bar with a search bar, a sidebar with 'Meetings' and 'Details' tabs, and a main content area. A modal dialog box is open in the center, displaying a list of cookies and an 'OK' button. The cookies listed are:

```

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; fusion768f1_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
00T-1666377760DT-1666377760S-A1N1 Mh01DmkV wh012b2nDvi
  
```

The background application interface shows a sidebar with 'Meetings' and 'Details' tabs. The 'Details' tab is active, showing a table with columns for Name, Meeting ID, Agenda, Location, Priority, Status, and Duration. The table contains one row with the following data:

Name	Meeting ID	Agenda	Location	Priority	Status	Duration
	1	test		Medium	Scheduling	1.0 Hours

Below the table is a section titled 'Proposed Start Dates/Times' with a single entry for '11/03/2022 00:00' and a 'Confirm' button.

# 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

