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

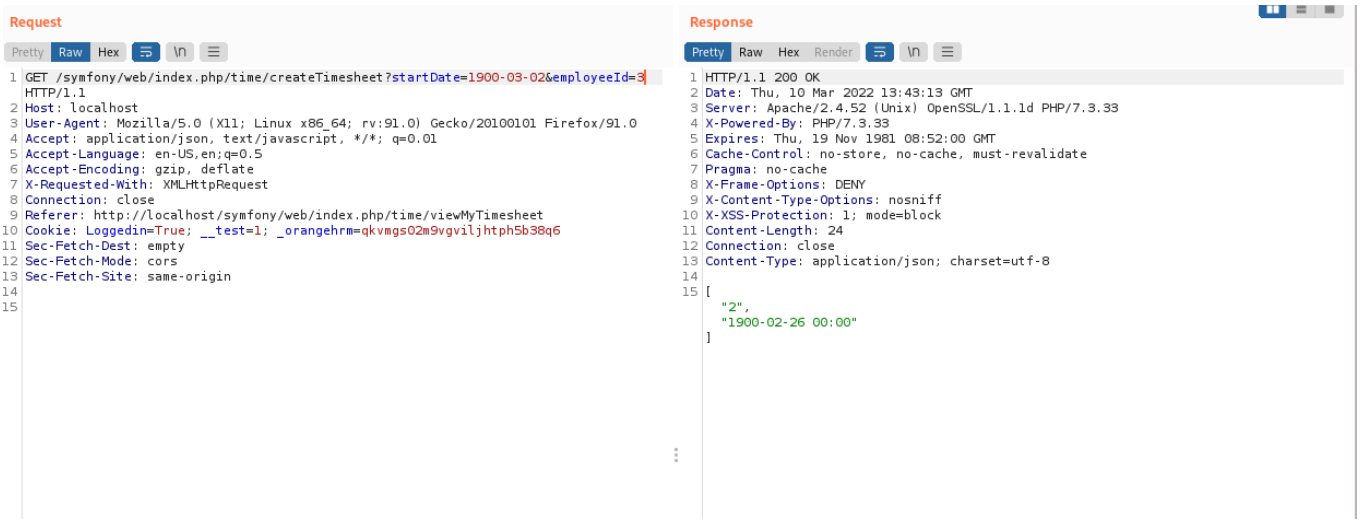
1. Login to the OrangeHRM application as user A with `employeeId` as `2`
2. Navigate to "Dashboard" > "My Timesheet"
3. Click on "Add Timesheet"
4. Turn on Intercept in Burp Suite (or any other web proxy)

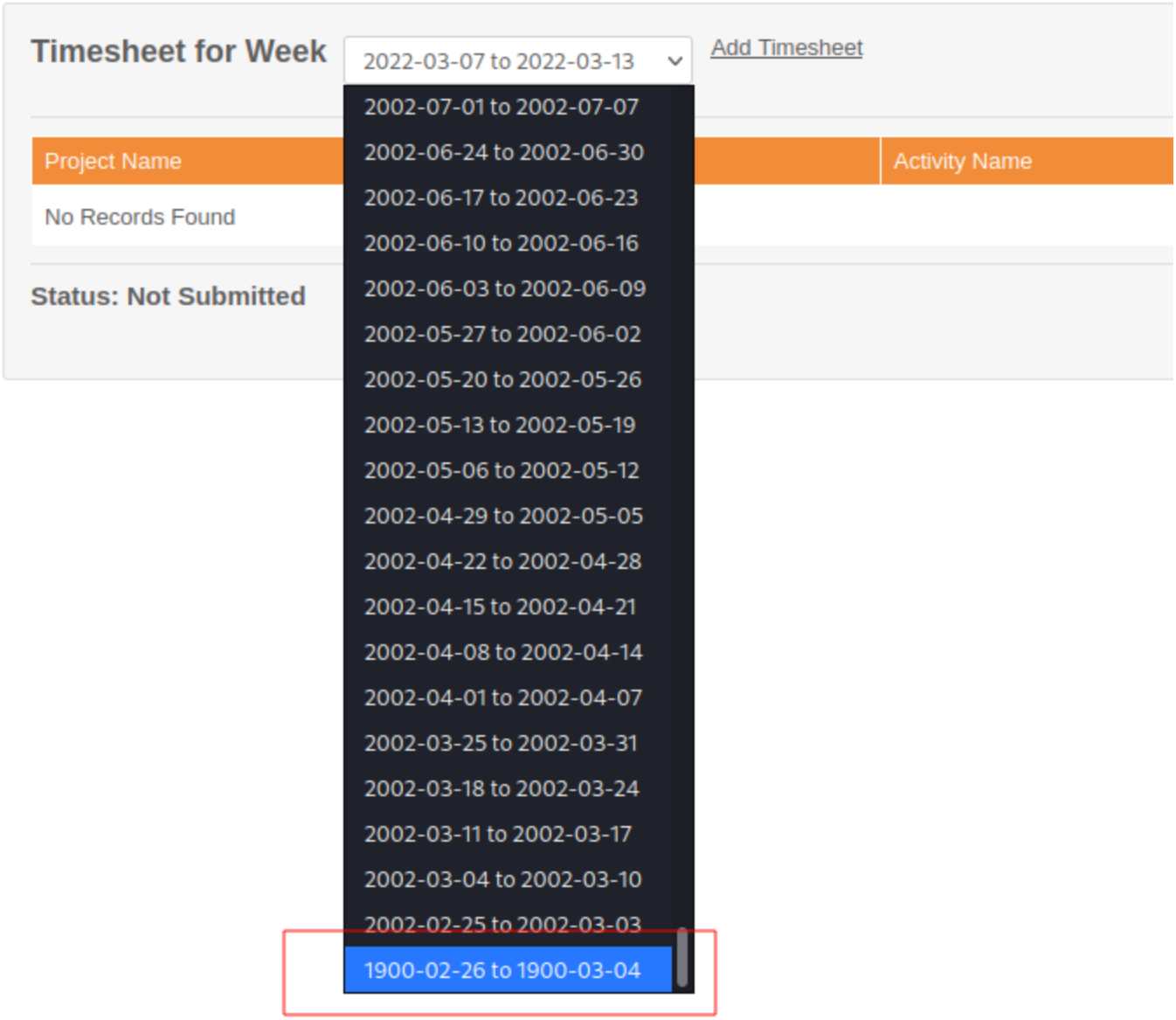
5. Click on the textbox and select any date, say 1900-03-02
6. Click on "Ok"
7. Go to the Burp Intercept tab and you will notice a GET request being made to the `/symfony/web/index.php/time/createTimesheet` endpoint
8. Modify the value of `employeeId` parameter to a user B's `employeeId`, `4`
9. Click 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





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