

jorani / jorani Public

- <> Code
- Issues 13
- Pull requests 5
- Discussions
- Actions
- Projects

Commit c5c42e2



Benjamin BALET committed on Jun 6, 2022

BF:Prevent SQL injection fix #369

master · v1.0.4 v1.0.2

1 parent [299b5a3](#) commit c5c42e2

1 file changed

+2 -2

↑ Top ⚙️

🔍 Filter files...

application/controllers

Leaves.php

🔍 Search within code ⚙️

application/controllers/Leaves.php

```

@@ -820,14 +820,14 @@ public function validate() {
820 820     header("Content-Type: application/json");
821 821     $id = $this->input->post('id', TRUE);
822 822     $type = $this->input->post('type', TRUE);
823 - //The above parameters could cause an SQL injection vulnerability due
      to the non standard
824 - //SQL query in leave_model::detectOverlappingLeaves
825 823     $date = $this->input->post('startdate', TRUE);
826 824     $d = DateTime::createFromFormat('Y-m-d', $date);
827 825     $startdate = ($d && $d->format('Y-m-d') === $date)?$date:'1970-01-01';
826 +     $startdate = preg_replace("([^\0-9-])", "", $startdate);
828 827     $date = $this->input->post('enddate', TRUE);

```

```
829 828      $d = DateTime::createFromFormat('Y-m-d', $date);
830 829      $enddate = ($d && $d->format('Y-m-d') === $date)?$date:'1970-01-01';
830 +      $enddate = preg_replace("[^0-9-]", "", $enddate);
831 831      $startdatetype = $this->input->post('startdatetype', TRUE);
      //Mandatory field checked by frontend
832 832      $enddatetype = $this->input->post('enddatetype', TRUE);
      //Mandatory field checked by frontend
833 833      $leave_id = $this->input->post('leave_id', TRUE);
```



Comments 0



Please [sign in](#) to comment.