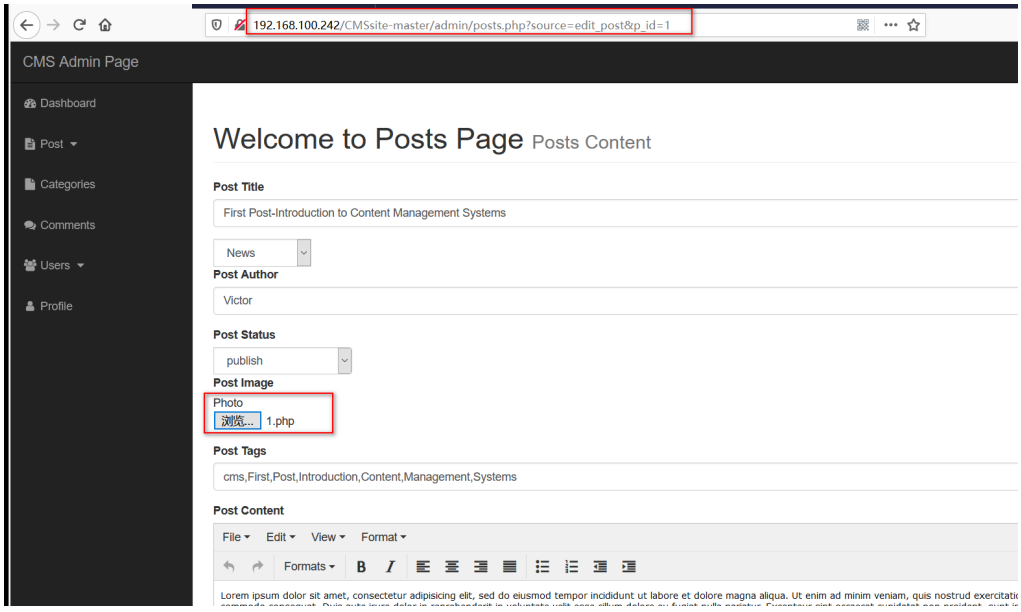
Victor-CMS

Exploit Title：Victor-CMS 1.0 —— Arbitrary file upload vulnerability
Vendor Homepage:https://github.com/VictorAlagwu/CMSsite
Vulnerability Type：
File upload
Vulnerability Version ：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the \CMSsite-master\admin\includes\admin_add_post.php file

```php

if (isset($_POST['create_post'])) {

    //--VARIABLES--
    $post_category_id = $_POST['post_category'];
    $post_title = $_POST['post_title'];
    $post_author = $_POST['post_author'];

    $post_date = date('d-m-y');

    $post_image = $_FILES['post_image']['name'];
    $post_image_temp = $_FILES['post_image']['tmp_name'];

    $post_content = $_POST['post_content'];
    $post_tags = $_POST['post_tags'];
    $post_comment_count = 4;
    $post_status = $_POST['post_status'];

    move_uploaded_file($post_image_temp, "../img/$post_image");

    //-------QUERY TO RELOAD IMAGE IN EDIT AND UPDATE PAGE
    if (empty($post_image)) {
        $query = "SELECT * FROM posts WHERE post_id=$id";
        $image_query = mysqli_query($con, $query);
        while ($row = mysqli_fetch_array($image_query)) {
            $post_image = $row['post_image'];
        }
    }
```



You can access our Webshell in the root directory