New issue

Jump to bottom

Unauthorized Sql Injection in admin/ajax/avatar.php #257

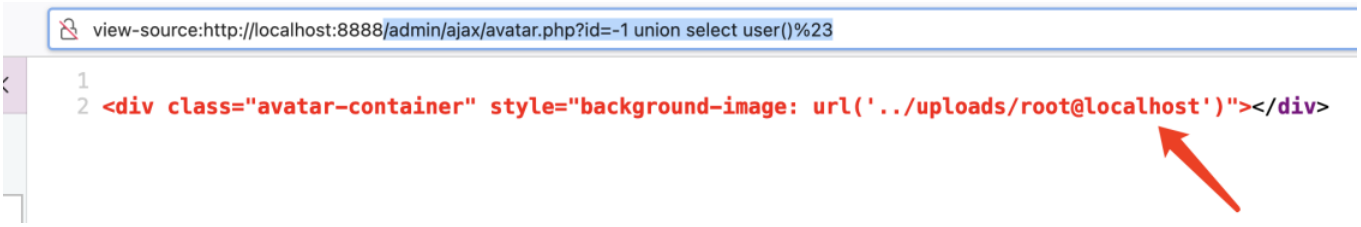
Open **bkfish** opened this issue on Feb 16 · 1 comment

bkfish commented on Feb 16

poc

```
/admin/ajax/avatar.php?id=-1 union select user()%23
```

the user() output can be found in html source



analysis

file /admin/ajax/avatar.php line 7 without any filter to protect

repair suggestion

add some filter about id

bkfish changed the title ~~Unauthorized Sql Injection in /admin/login.php admin/ajax/avatar.php~~ **Unauthorized Sql Injection in admin/ajax/avatar.php** on Feb 16

creptor commented on Feb 17 • edited Contributor

Thank you for taking the time to write this Issue for the project. It's very helpful for new users to understand some of the common problems they can face while developing a website on any platform.

SQL injections are a common problem in the series and is present to a great extent in the code itself, which is very dangerous. If a website fails to stop these kinds of attacks it could end on lost information from the database or even compromise the website for malicious use.

For this and many other problems I always mention that Atom.CMS is **not** meant to be used in production, and it should be used solely for learning PHP in a controlled environment.

That said, an option to avoid the above issue was already discuss in #255, but to remove many of those SQL injections you could try PDO or a function that filters all the user inputs (which you could easily find on the web).

I'm not the author or maintainer of this project, just someone who learned a lot from the YouTube series and is willing to help.

This was referenced on Apr 12

SQL Injection vulnerability on Atom.CMS_admin_uploads.php #259
Open

SQL Injection vulnerability on Atom.CMS_admin_ajax_blur-save.php #260
Open

SQL Injection vulnerability on Atom.CMS_admin_ajax_list-sort.php #261
Open

SQL Injection vulnerability on Atom.CMS_admin_ajax_navigation.php #262
Open

SQL Injection vulnerability on Atom.CMS_admin_ajax_pages.php #263
Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants