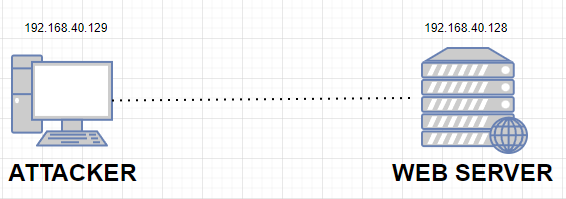
HUỲNH THANH TÂM – 2033210951

1. MÔ HÌNH MẠNG

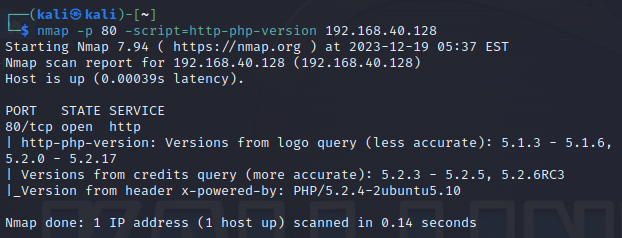


1. THỰC HIỆN

* BƯỚC 1: Thực hiện scan WEBSERVER

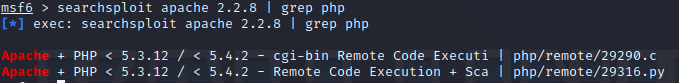
Sử dụng lệnh : *nmap –p 80 –script=http-php-version 192.168.40.128*

*KẾT QUẢ :*



* BƯỚC 2: Kiểm tra lỗ hổng cgi có trên php là từ phiên bản bao nhiêu.

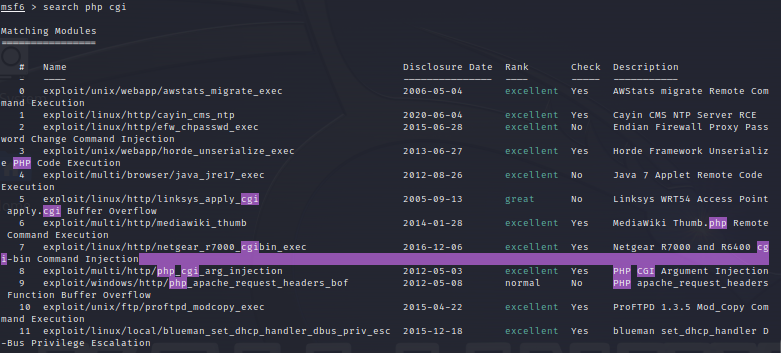
*KẾT QUẢ:*



*Lỗ hổng này từ 5.4.2 trở xuống . php web chuẩn bị khai thác 5.2.4.*

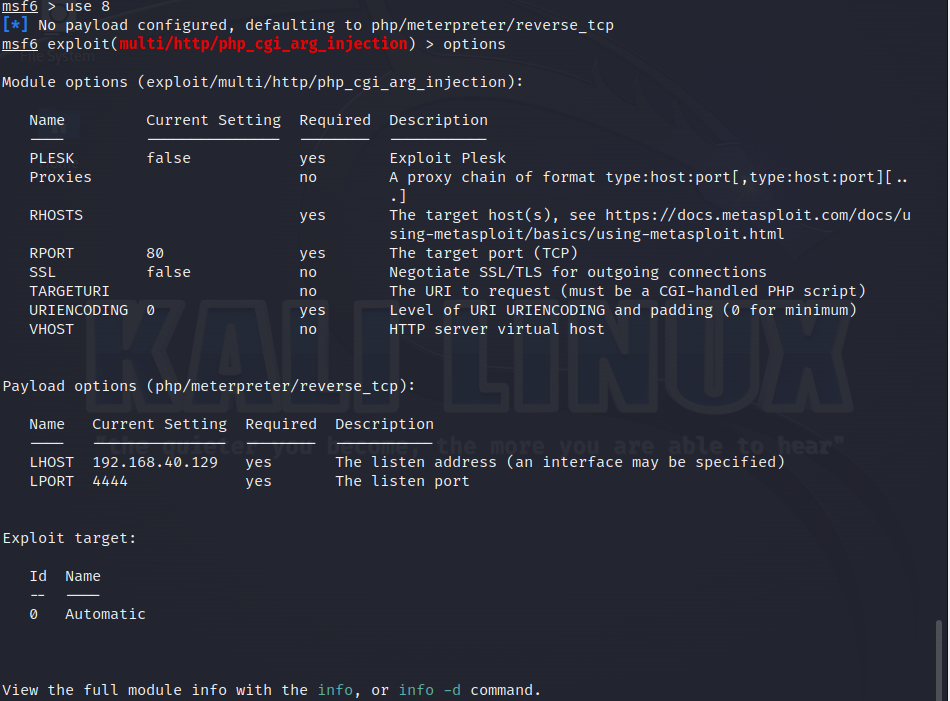
*Tại msf6 > search php cgi => ra lỗ hổng php\_cgi*

*KẾT QUẢ:*



*Use id hoặc tên lỗ hổng.*

*KẾT QUẢ :*



*Model thiếu rhosts = ip của máy webserver.*

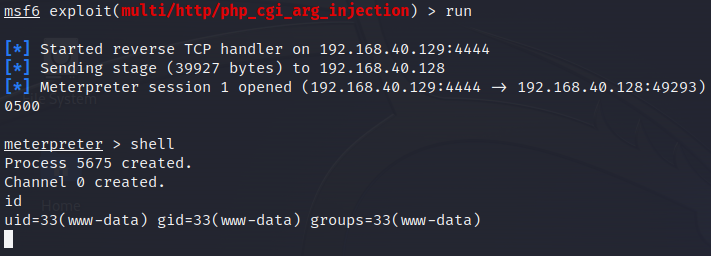
*Tiến hành set ip cho rhosts*

*KẾT QUẢ :*



*Gõ run để bắt đầu chạy model , thực hiện vào shell của máy webserver với quyền user là www-data.*

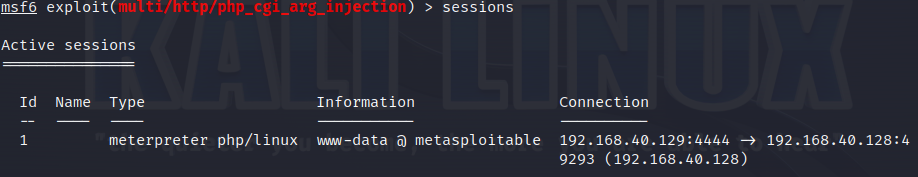
*KẾT QUẢ :*



* Bước 3: Nâng cấp lên meterpreter session

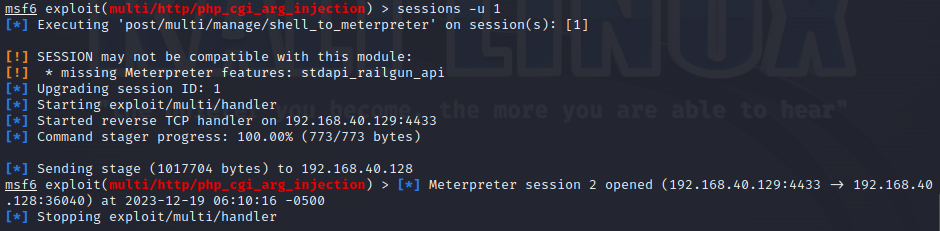
*Sử dụng lệnh > session để xem có kiểm tra session ở bước trước có chạy không, có 1 session đang chạy.*

*KẾT QUẢ:*



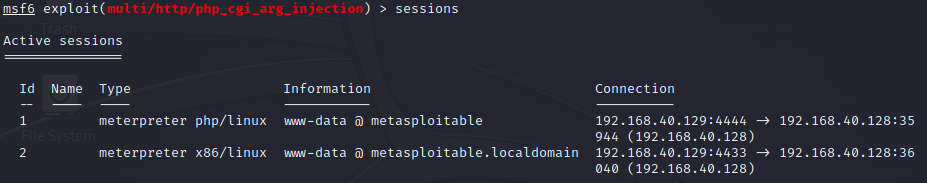
*Cách để nâng là sử dụng câu lệnh ‘session –u + số session nâng cấp’*

*KẾT QUẢ :*



*Kiểm tra lại session :*

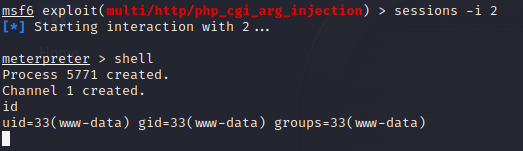
*KẾT QUẢ :*



*Thực hiện session*

*Sử dụng lệnh sessions –i 2 .Kết nối tới session có ID là 2.*

*KẾT QUẢ :*



* BƯỚC 3:

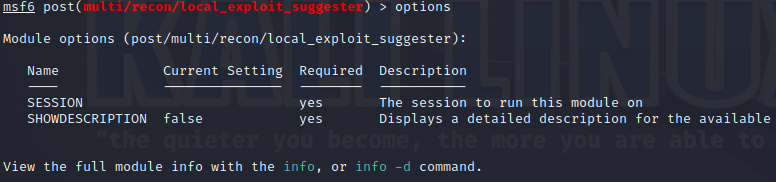
Model *post/multi/recon/local\_exploit\_suggester* trong Metasploit được dùng để kiểm tra hệ thống đang bị tấn công (được kết nối qua session) nhằm tìm kiếm các lỗ hổng có thể khai thác bằng các exploit có sẵn trong framework. Nó thực hiện việc này bằng cách chạy một loạt các kiểm tra dựa trên các mô-đun exploit cục bộ (local exploit) có trong Metasploit.

Tìm lỗ hổng tiềm ẩn: Thay vì thủ công thử từng exploit, mô-đun này thực hiện các kiểm tra nhanh chóng giúp xác định các exploit có khả năng thành công cao dựa trên thông tin thu thập được từ hệ thống.

Cú pháp lệnh :

use post/multi/recon/local\_exploit\_suggester [options]

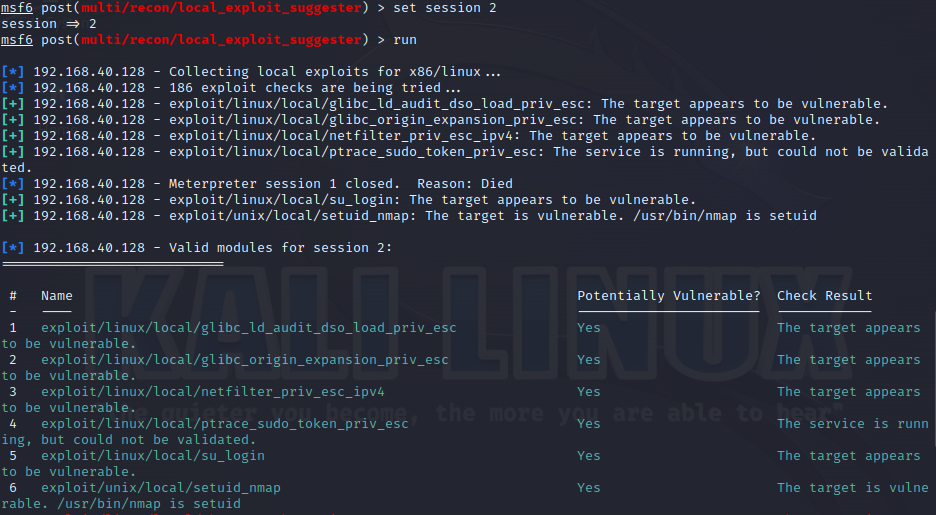
*KẾT QUẢ :*



Các options phổ biến :

* SESSION: ID của session dùng để kết nối với hệ thống mục tiêu.
* VERBOSE: Hiển thị chi tiết quá trình kiểm tra.
* LIMIT: Số lượng exploit tối đa để kiểm tra.

KẾT QUẢ SỬ DỤNG ‘session’:



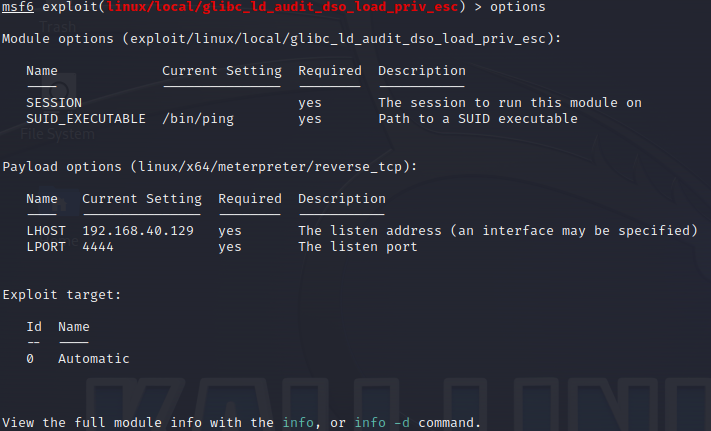
* BƯỚC 4: Thực hiện leo thang đặc quyền lên root.

Model *exploit/linux/local/glibc\_ld\_audit\_dso\_load\_priv\_esc* này sử dụng LD\_AUDIT để tải đối tượng chia sẻ libpcprofile.so, được phân phối với một số phiên bản của glibc và tận dụng chức năng tạo tệp tùy ý trong hàm tạo thư viện để ghi một tệp có thể ghi trên toàn thế giới thuộc sở hữu gốc vào đường dẫn tìm kiếm đáng tin cậy của hệ thống (thường là /lib). Sau đó, tệp sẽ được ghi đè bằng một đối tượng dùng chung rồi được tải bằng LD\_AUDIT dẫn đến việc thực thi mã tùy ý.

Cú pháp lệnh :

use exploit/linux/local/glibc\_ld\_audit\_dso\_load\_priv\_esc [option]

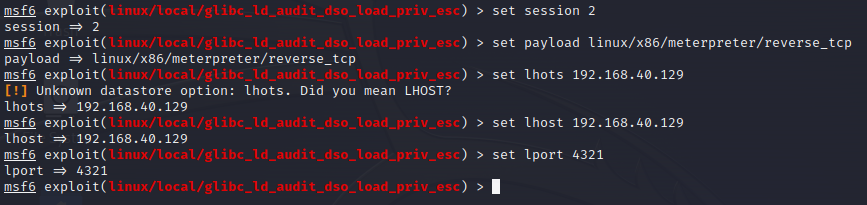
KẾT QUẢ :



Các options phổ biến :

* SESSION: ID của session dùng để kết nối với hệ thống mục tiêu.
* LHOST: Địa chỉ IP của máy tính của bạn, nơi payload sẽ tạo một kết nối ngược.
* LPORT: Cổng trên máy tính của bạn mà payload sẽ tạo một kết nối ngược.
* PAYLOAD: Loại payload, chẳng hạn như windows/meterpreter/reverse\_tcp hoặc linux/x64/shell/reverse\_tcp.
* RHOST: Địa chỉ IP của hệ thống mục tiêu mà bạn muốn khai thác.
* RPORT: Cổng trên hệ thống mục tiêu mà bạn muốn khai thác.

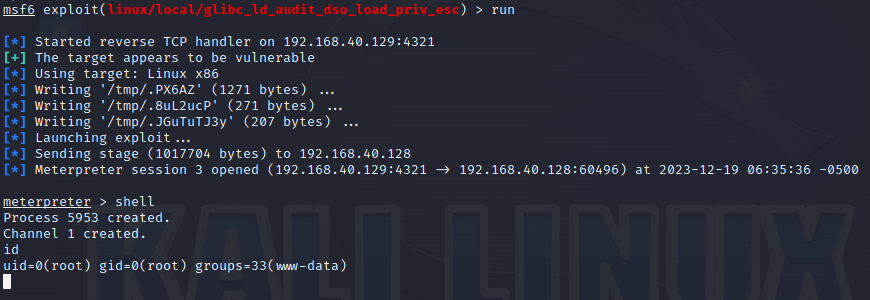
KẾT QUẢ :



Cuối cùng, run để khai thác.

Vào shell kiểm tra id, người dùng là root.

KẾT QUẢ :

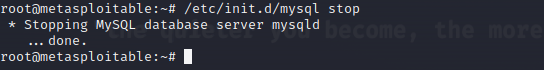


* BƯỚC 5: Sau khi có quyền root , tiếp tục xâm nhập vào database lấy username và password của website.

Chạy câu lệnh khởi động MySQL không cần mật khẩu

Tại root> ***/etc/init.d/mysql stop***

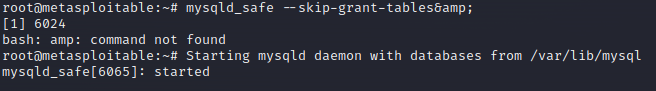
KẾT QUẢ : tắt mysql



Tiến hành chạy câu lệnh khởi động MySQL không cần mật khẩu

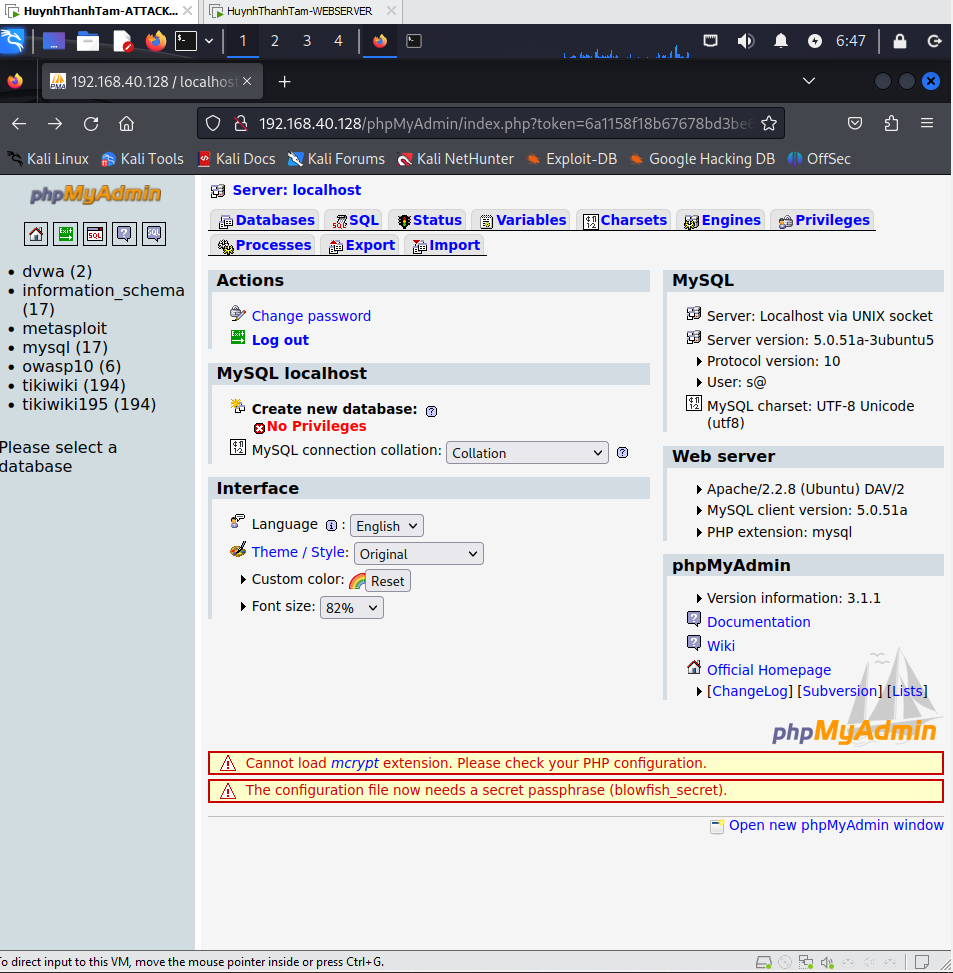
Tại root > ***mysqld\_safe --skip-grant-tables &amp;***

KẾT QUẢ :



Vào trang phpMyAdmin đăng nhập(hoặc có thể chỉ sửa trên terminal của root)

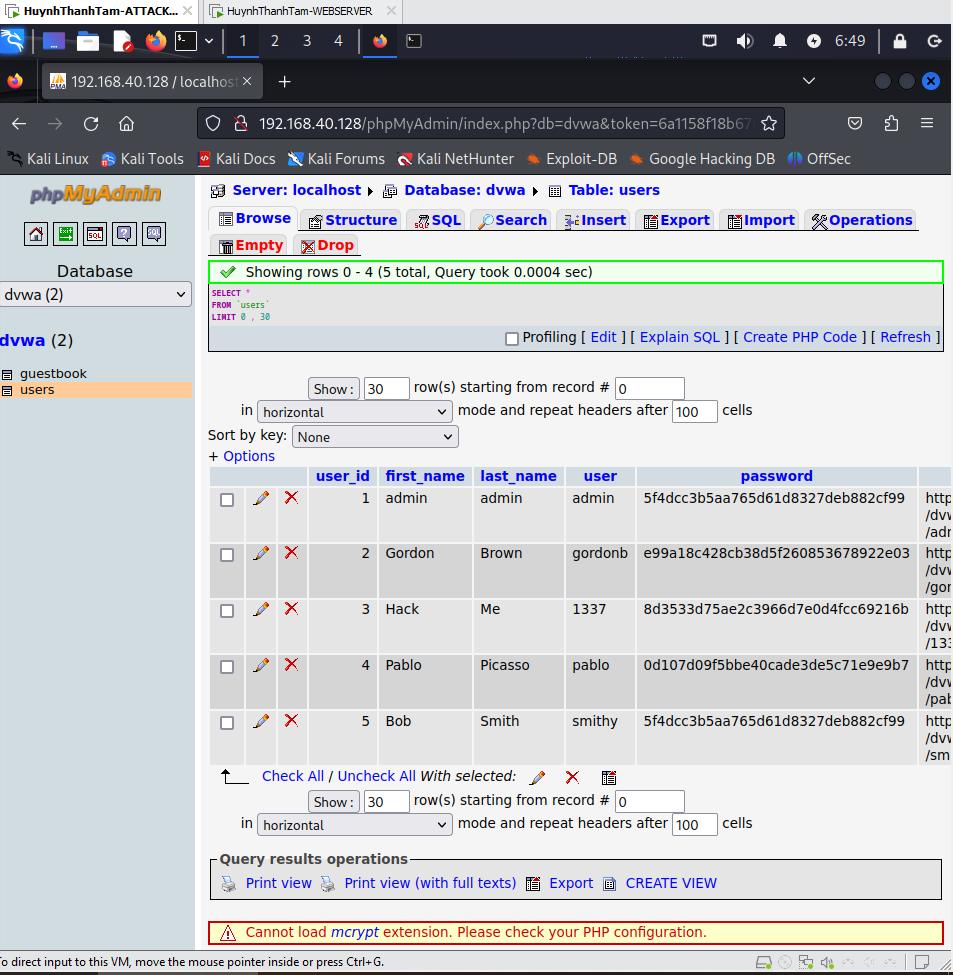
KẾT QUẢ:



Ta có toàn quyền thêm,xóa,sửa database

Tại database > dvwa , tables>users . Ta lấy được username và password

KẾT QUẢ:



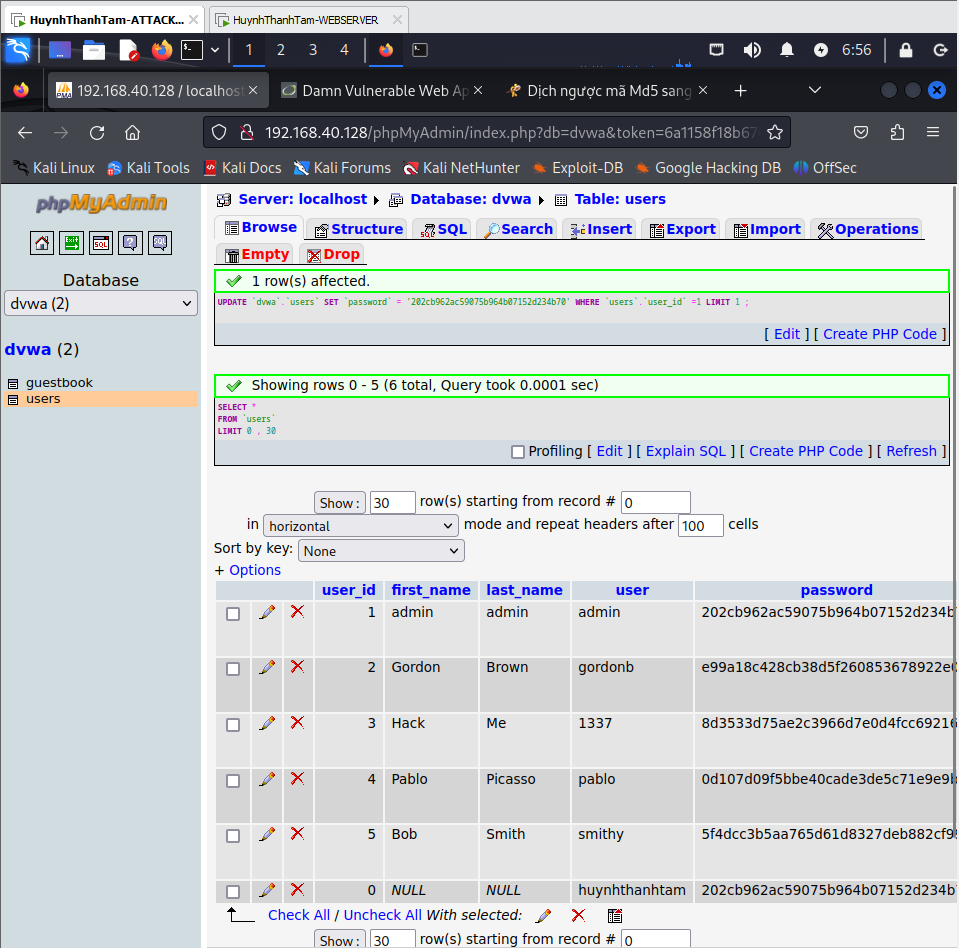
Giải mã các mật khẩu, đổi mật khẩu, thêm user mới.

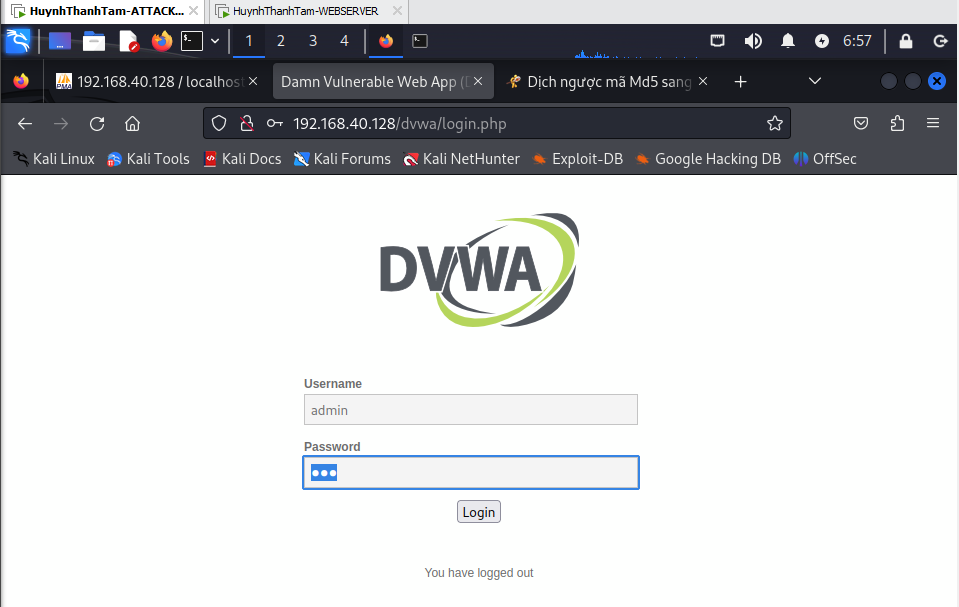
Để thay đổi mật khẩu thì mật khẩu cần đổi phải được mã hóa ví dụ :

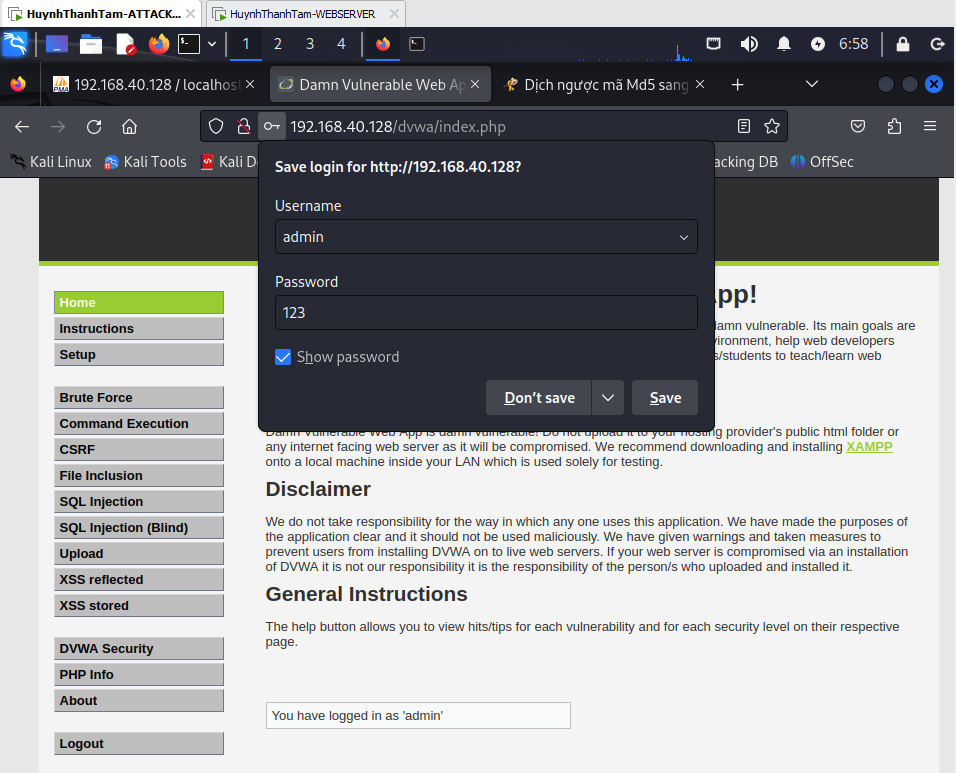
Mật khẩu muốn đổi là 123 thì mã hóa thành 202cb962ac59075b964b07152d234b70

Rồi thay vào cột password là có thể đăng nhập với mật khẩu 123

KẾT QUẢ :







Có thể làm mọi thứ mình muốn khi có quyền root.