**LAB 4**

**Web Attack and Defense**

| Họ tên và MSSV:……Đào Ngọc Hòa……..  Lớp: ……1050080050………..  Link youtube:………………..  Link Github:……………….. |
| --- |

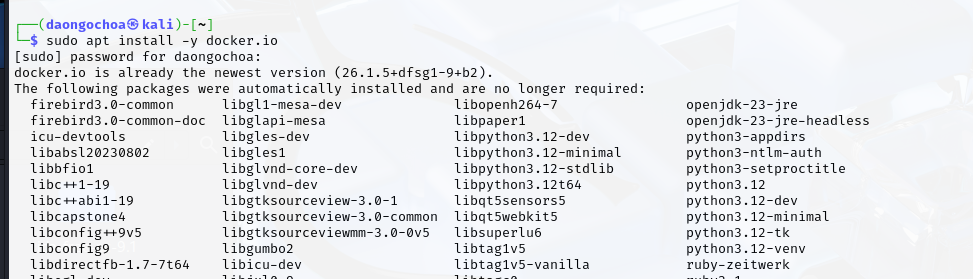
* *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*
* *Trình bày chi tiết từng bước thực hành*
* *Bài nộp phải ở dạng ,docx, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
* *Quay lại quá trình làm bài, quay luôn faces của mình, đang làm, đẩy lên youtube, gửi link vào đây.*
* *Link youtube tham khảo full của Thanh Hơn 09\_CNPM3:* [Lab4 2-5-2024 - YouTube](https://www.youtube.com/playlist?list=PLkhsQ56XEcBItZjjvZ2Lz9JCKKUfDsnZo)

**Câu 1: Cài đặt Damn Vulnerable Web Application (DVWA) trên Kali Linux**

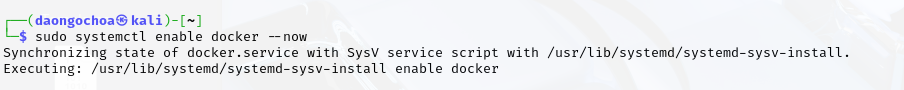
- Cài đặt docker

sudo apt update

sudo apt install -y docker.io

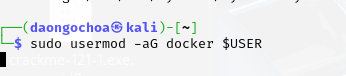


sudo systemctl enable docker --now



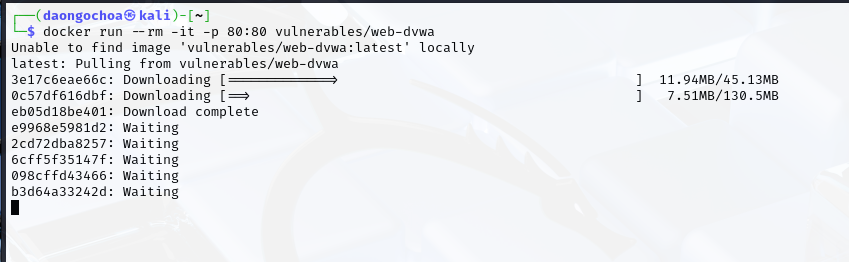
- Thêm người dùng vào nhóm docker; log out và log in lại vào kali

sudo usermod -aG docker $USER

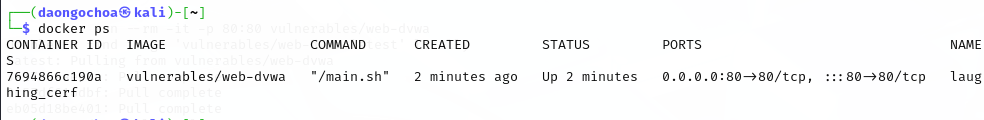


- Tải và thực thi image của DVWA từ Docker Hub

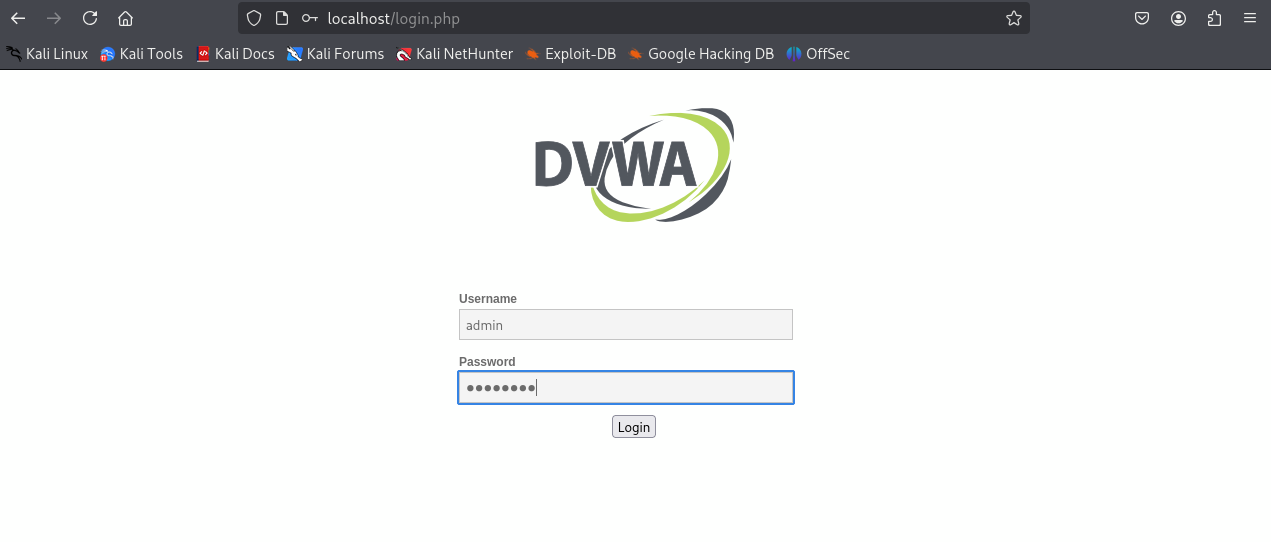
docker run --rm -it -p 80:80 vulnerables/web-dvwa

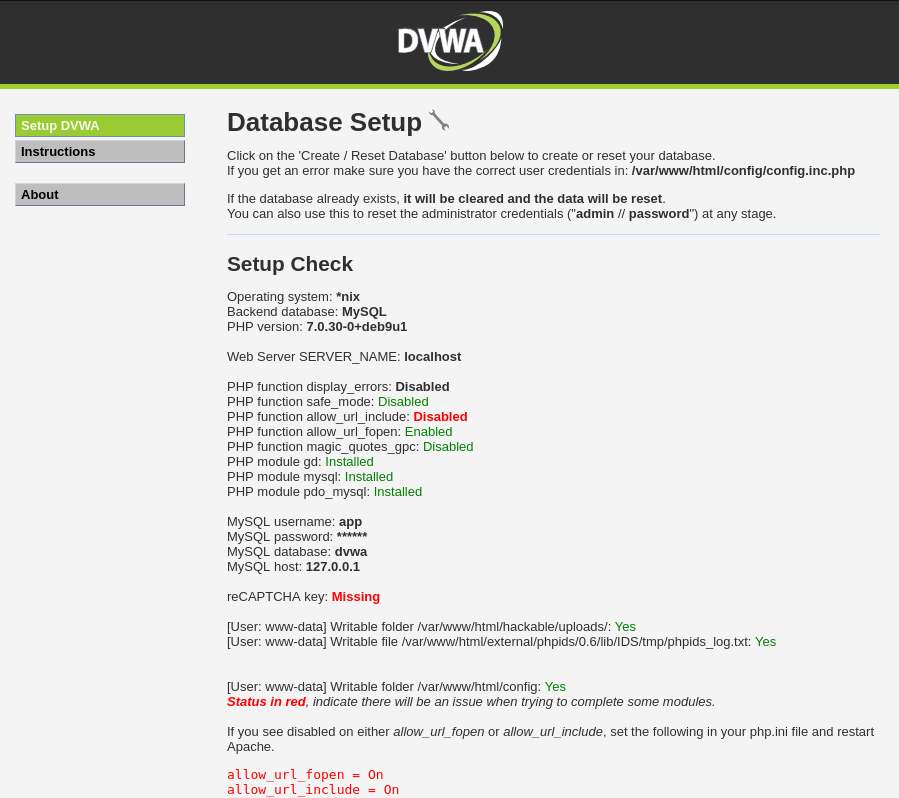


* Kiểm tra bằng docker ps

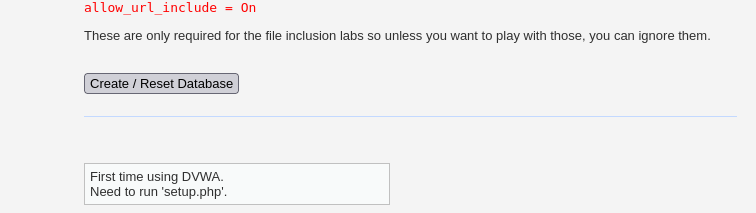


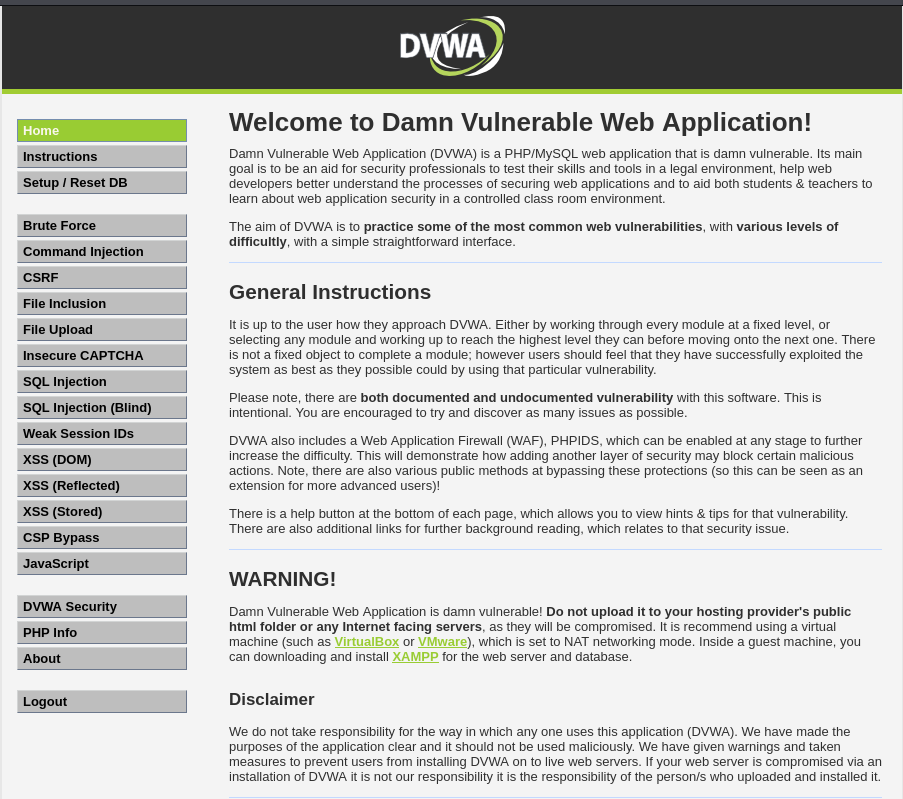
- Truy cập vào DVWA ở địa chỉ <http://localhost>; đăng nhập với tài khoản ***admin/password***

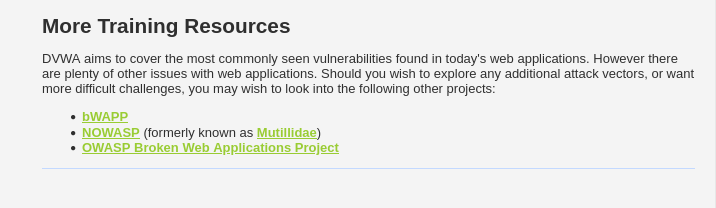
******

******

- Chọn “Create/Reset Database”; sau đó đăng nhập lại vào DVWA



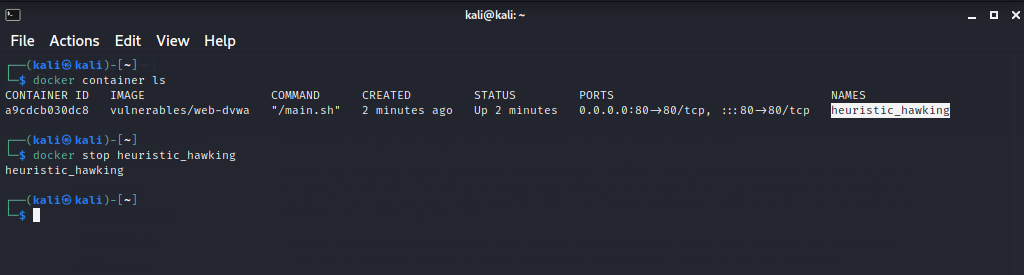




- Sau khi hoàn thành bài thực hành dừng container DVWA

docker container ls

docker stop <container name>



(Chụp hình minh họa quá trình thực hiện)

**Câu 2: Tấn công dò mật khẩu trên DVWA**

2.1. Tham khảo các tài liệu đính kèm để thực hiện tấn công dò mật khẩu (Brute force attacks) của một tài khoản trên DVWA (security ở mức độ low) sử dụng công cụ Burp Suite (hoặc Hydra, John The Ripper, v.v.).

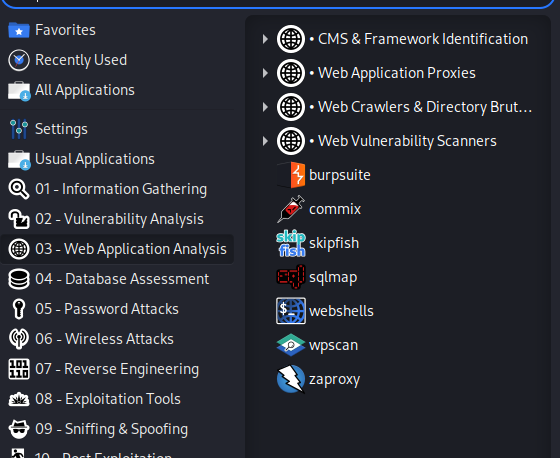
<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#Brute_Force>

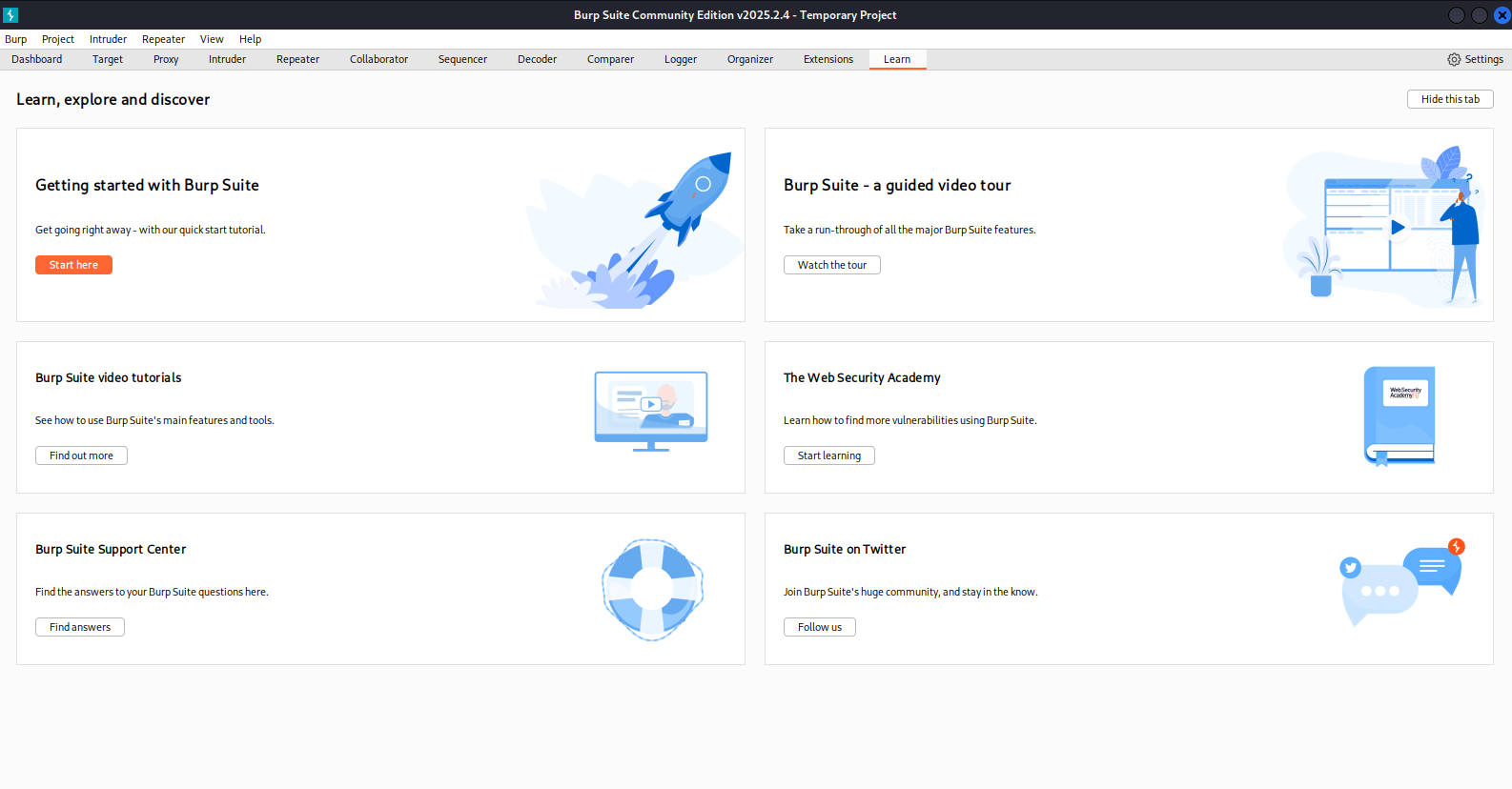
<https://www.youtube.com/watch?v=SWzxoK6DAE4&list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q&index=2>

<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2001:%20Brute%20Force.md>

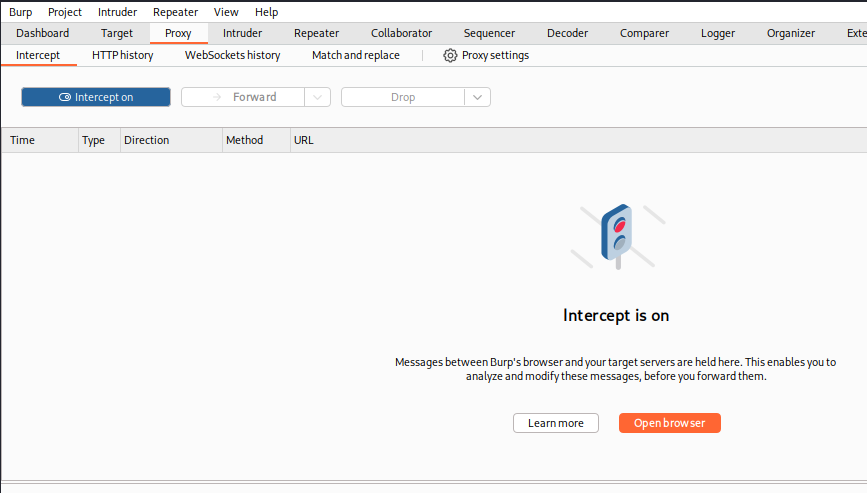
(Chụp hình minh họa quá trình thực hiện)

* Thực hiện Brute Force với Burpsuite
* Chọn burpsuite

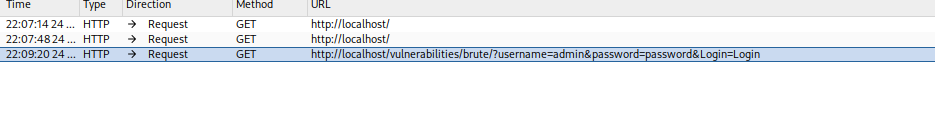




* Bật chức năng Intercept trên BurpSuite của tab proxy



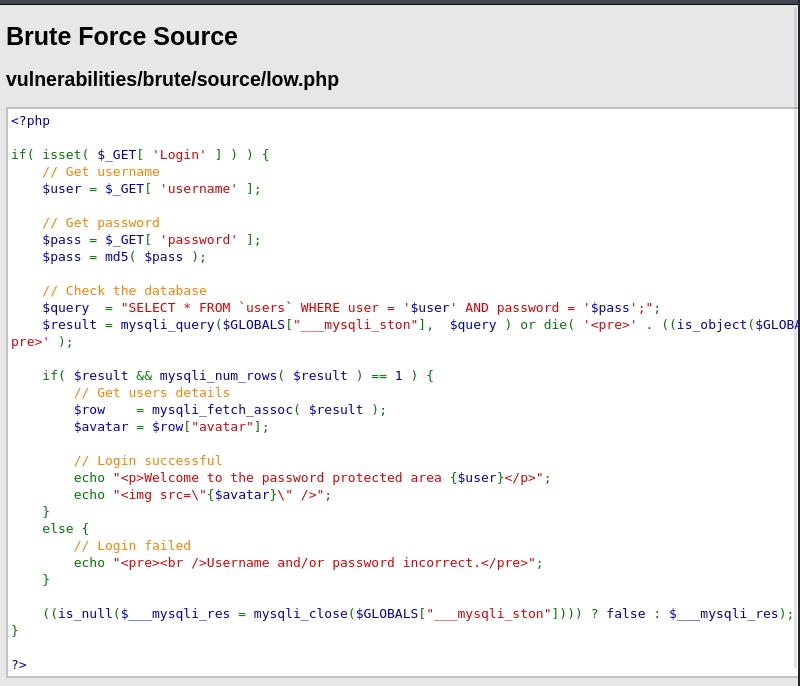
* Chọn Open browser để có thể truy cập vào DVWA qua BurpSuite

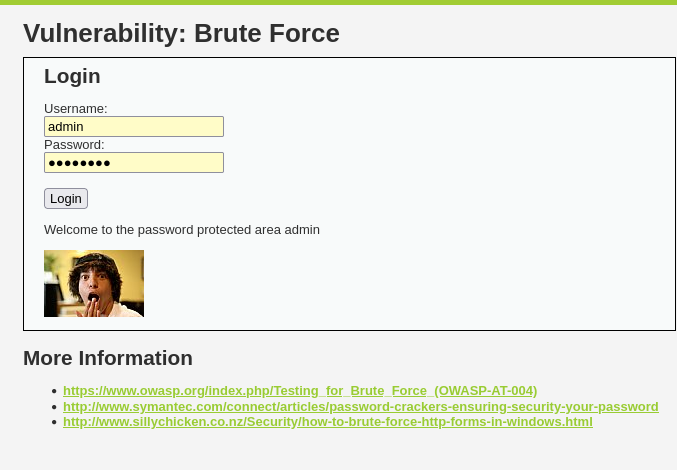


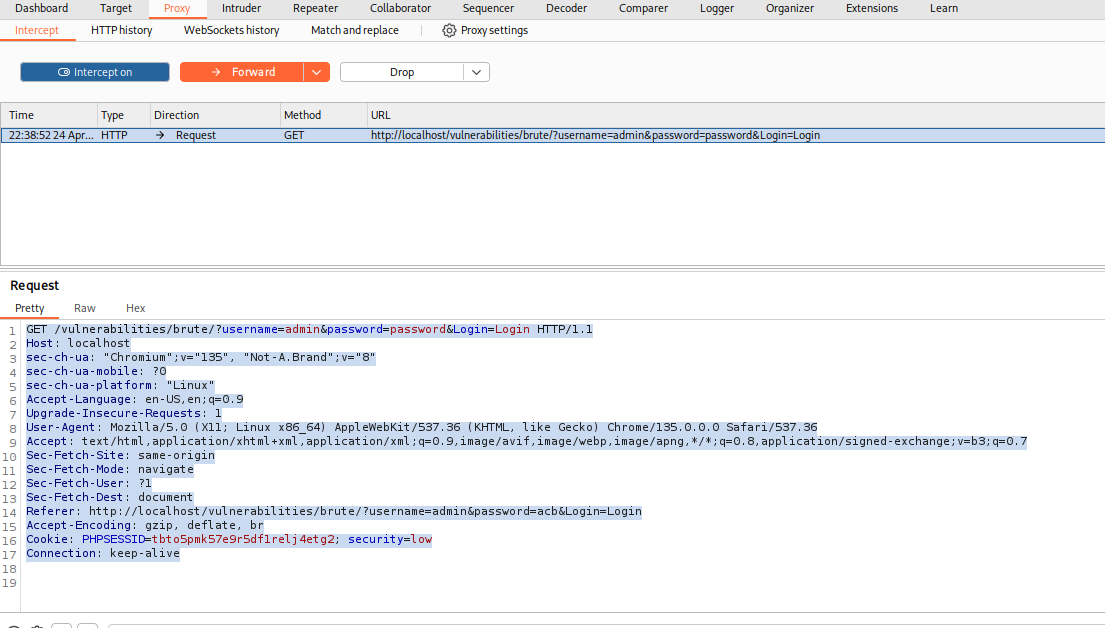
* Nhập giá trị cho phần login trong DVWA và kiểm tra Request trả về.

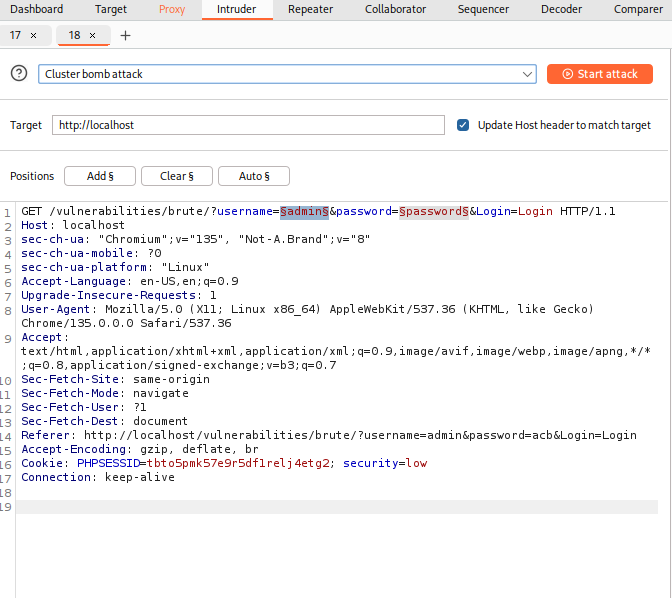


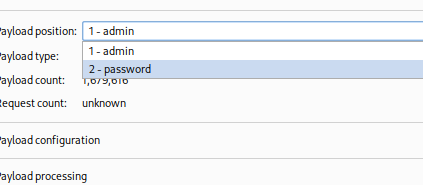


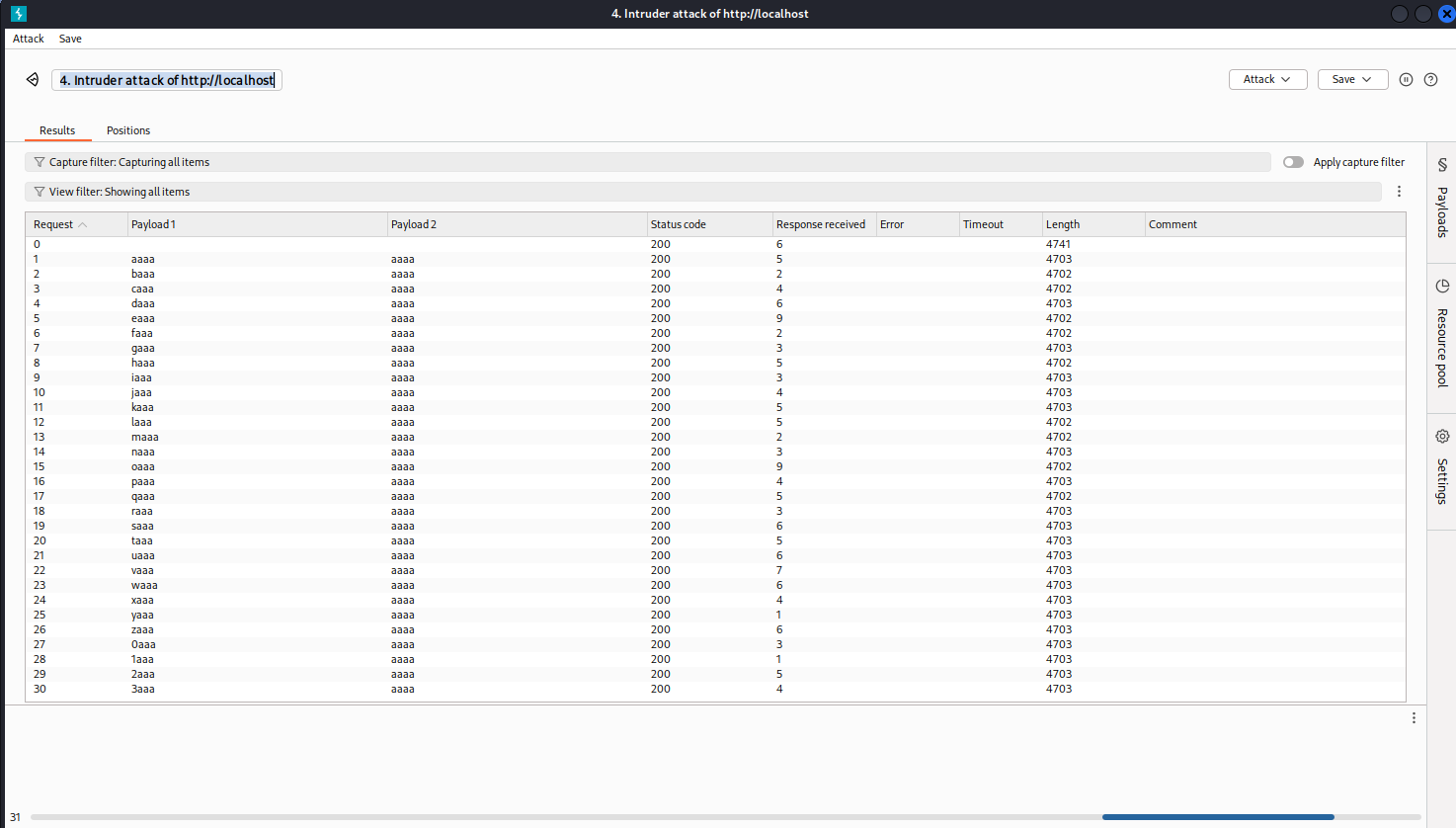












2.2. Tham khảo mã nguồn (view source), giải thích ngắn gọn cách DVWA với security ở mức độ medium, high, impossible ngăn chặn tấn công dò mật khẩu.

- Medium: Có 2 giây tạm dừng khi đăng nhập sai để hạn chế bị dò mật khẩu.

- High: Có ngẫu nhiên 0 đến 3 giây tạm dừng khi đăng nhập sai. Sinh ra token bí mật và gửi xuống cho người dùng, người dùng khi đăng nhập phải gửi token đó lên.

- Imposible: Nếu mật khẩu sai một số lần nhất định thì khóa tài khoản tạm thời.

**Câu 3: Khai thác lỗi Cross Site Request Forgery (CSRF) trên DVWA**

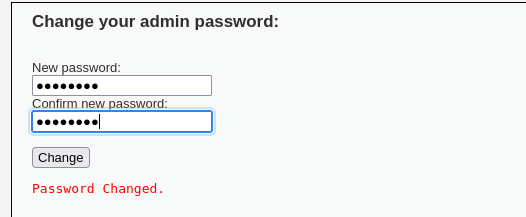
3.1. Tham khảo các tài liệu đính kèm để khai thác lỗi CSRF của DVWA (security ở mức độ low) để tự động đổi mật khẩu người dùng.

<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#CSRF>

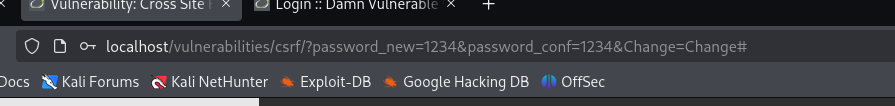
<https://youtu.be/Nfb9E8MJv6k?list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q>

<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2003:%20CSRF.md>

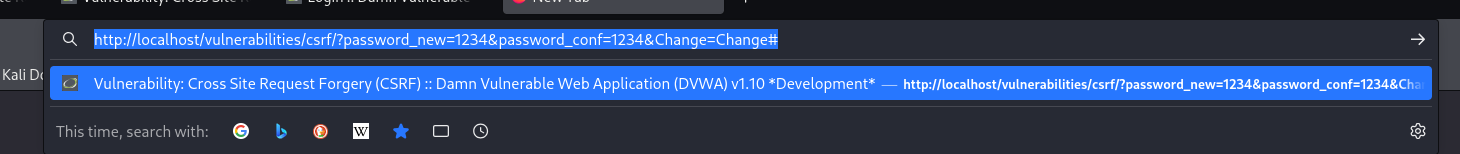
* Thử chọn CSRF để thử đổi mật khẩu
* Sau khi đổi thành công sẽ có thông báo Password Changed nghĩa là mật khẩu đã thay đổi thành công.



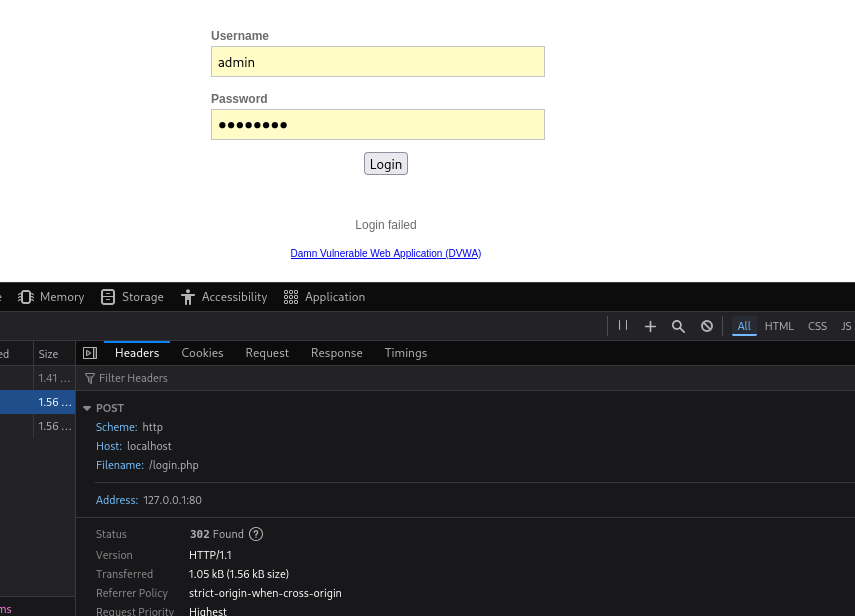
* Kiểm tra phần URL thì ta có thể thấy cấu trúc URL như sau
* password\_new : sẽ là mật khẩu mới
* password\_conf: là xác nhận mật khẩu mới



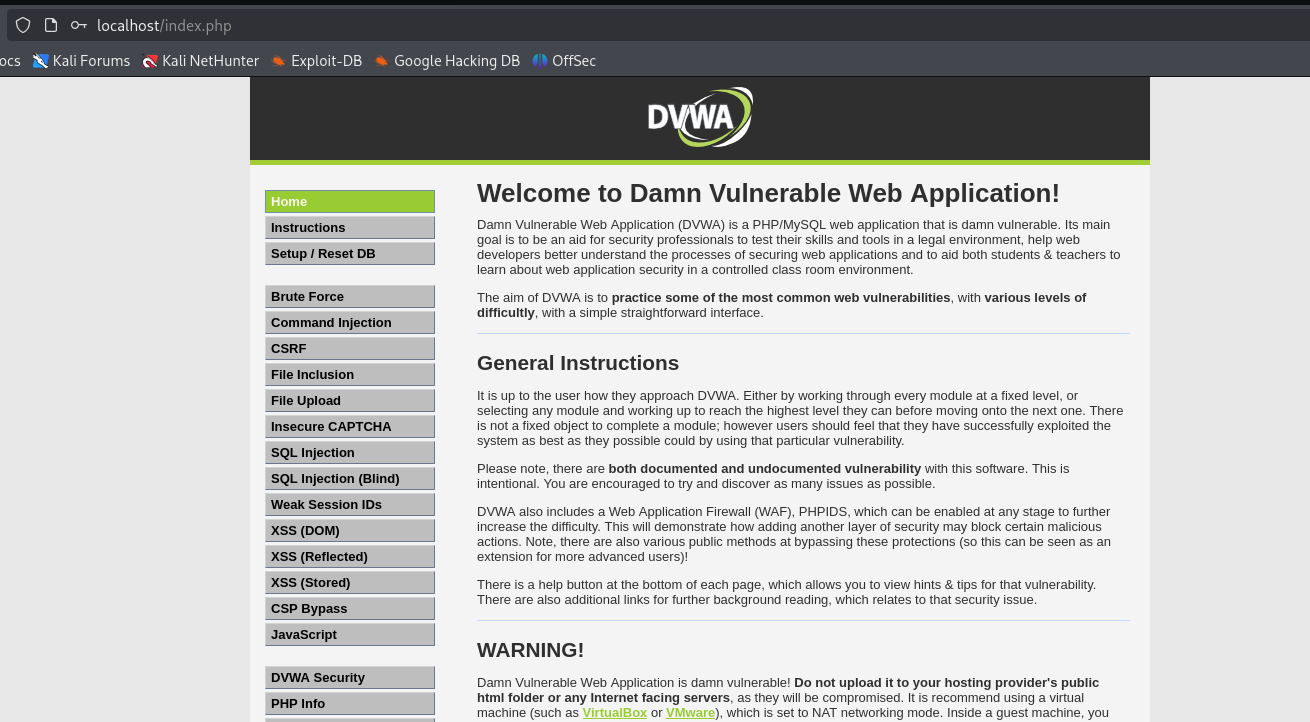
* Nếu Copy đường link thì ta có thể đổi mật khẩu nếu như ta truy cập vào đường link ví dụ như nhấp vào đường link.



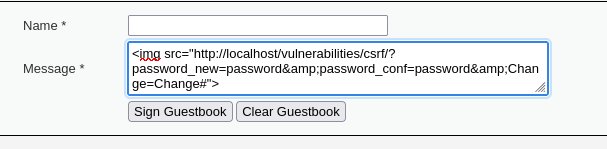
* Thử đăng nhập vào bằng mật khẩu cũ thì không thể đăng nhập được



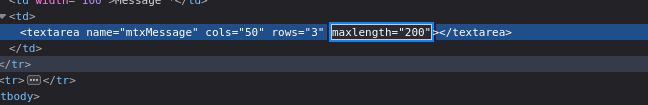
* Nếu đăng nhập được mật khẩu mới thì có thể đăng nhập vào được



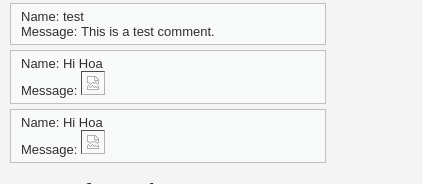
* Hacker có thể lợi dụng nhúng đường đường link vào một bức ảnh hoặc chỉ đơn các nút ẩn để lừa người người dùng nhấp vào
* Áp dụng nguyên lý này ta thử sử dụng XSS để nhúng link vào một bức ảnh
* Chọn phần XSS (Stored)
* Ta bỏ link dẫn đến trang đổi mật khẩu vào vào một thẻ img



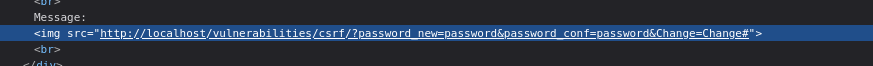
* Ô input trên DVWA chỉ giới hạn lại 50 ký tự nên ta phải sửa lại thành 200 để vừa với số ký tự ta sẽ viết vào ô input.



* Sau khi thành công thì ta có kết quả như sau



* Và khi kiểm tra Inspect thì ta được kết quả như sau



3.2. Tham khảo mã nguồn (view source), giải thích ngắn gọn cách DVWA với security ở mức độ medium, high, impossible ngăn chặn tấn công khai thác lỗi CSRF.

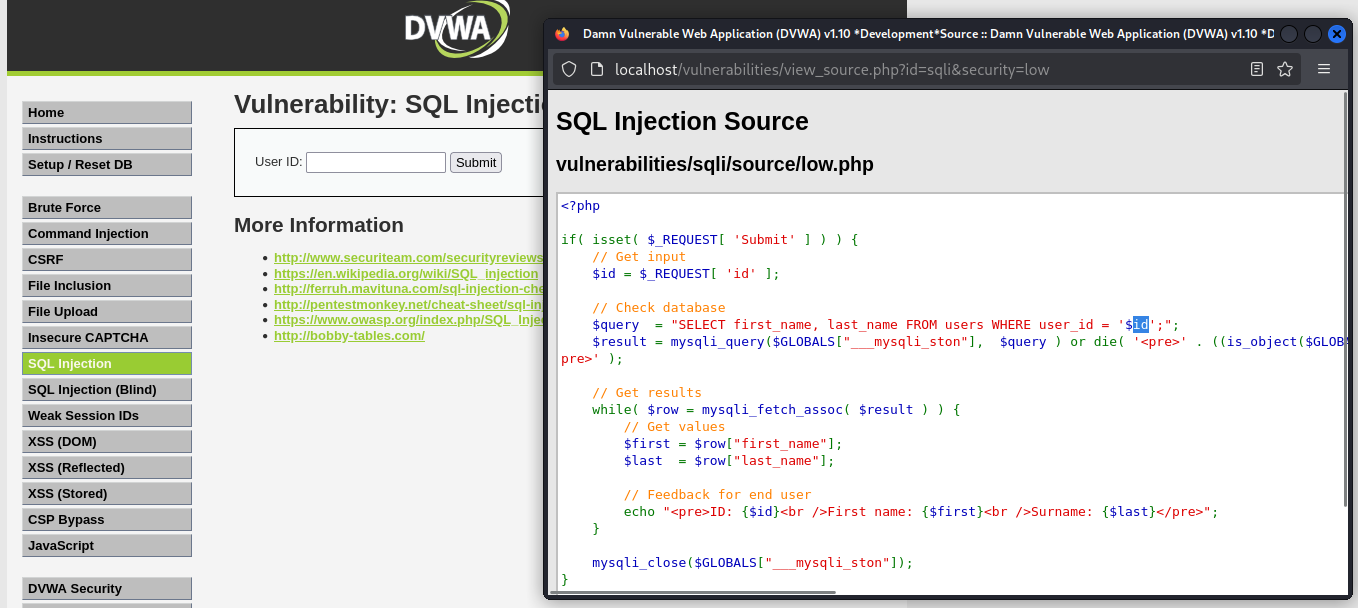
(Chụp hình minh họa quá trình thực hiện)

* Medium: Kiểm tra yêu cầu có phải từ chính bản thân trang web không, kiểm tra lời yêu cầu xuất phát từ đâu.
* High: Sinh ra token bí mật và gửi xuống cho người dùng, người dùng khi đổi mật khẩu phải gửi token bí mật đó lên.
* Imopossible: Phải nhập mật khẩu cũ khi muốn đổi mật khẩu.

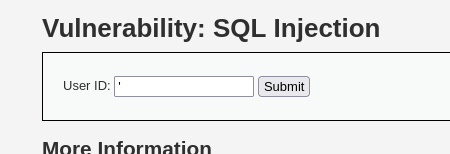
**Câu 4: Khai thác lỗi SQL injection trên DVWA**

4.1. Tham khảo các tài liệu đính kèm để khai thác lỗi **SQL injection** trên DVWA (security ở mức độ low) để lấy mật khẩu người dùng **admin**.

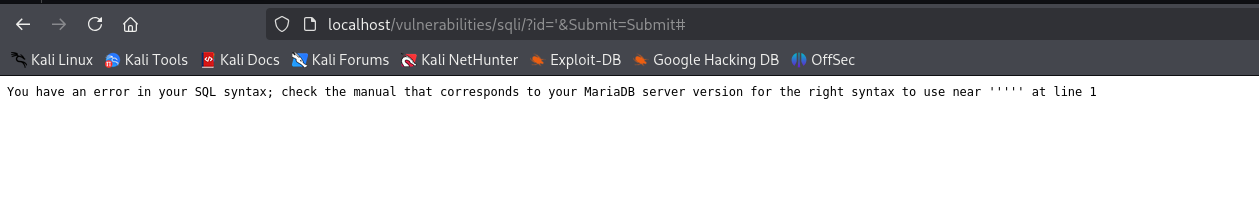
* Chọn SQL Injection và xem thử Source Code.



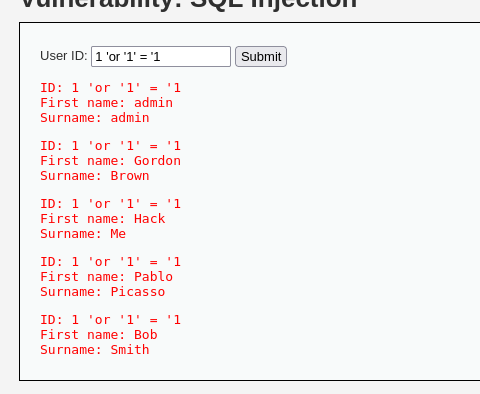
* Nhập thử vào dấu ngoặc đơn ‘



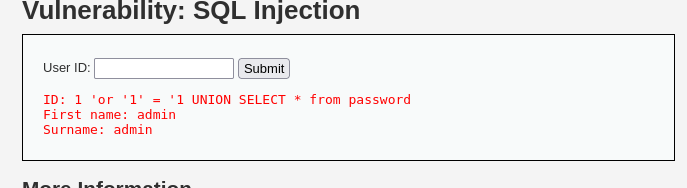
* Trang web trả về lỗi SQL như sau



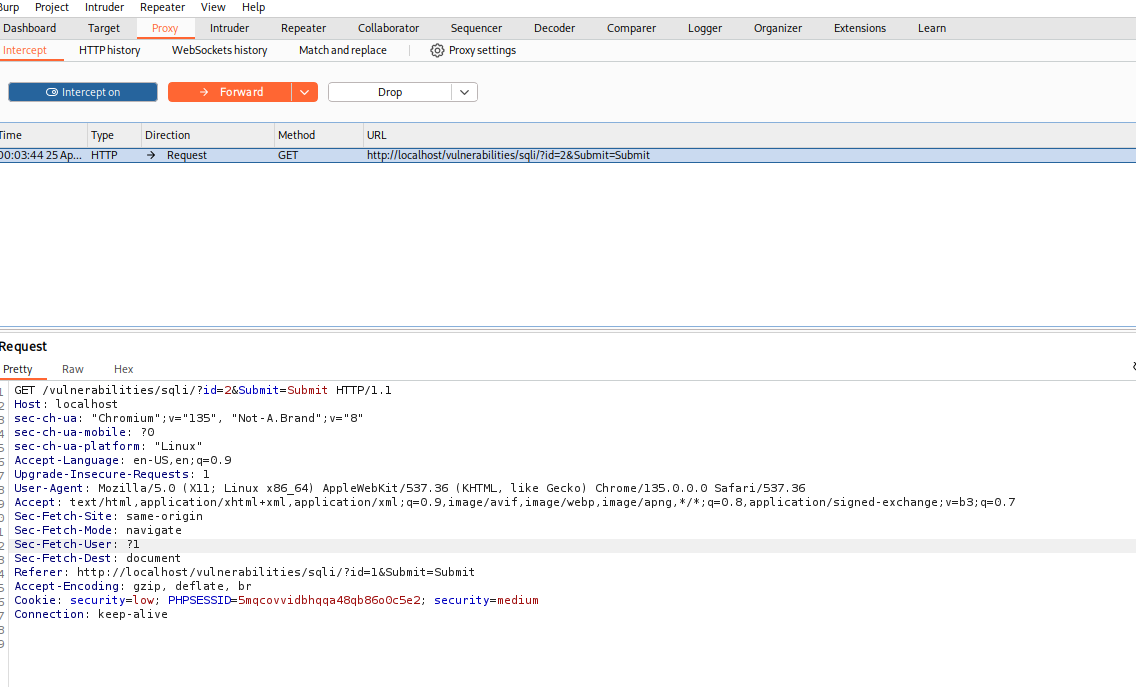
* Nhập vào 1 'or '1' = '1 thì ta nhận được kết quả truy vấn như sau



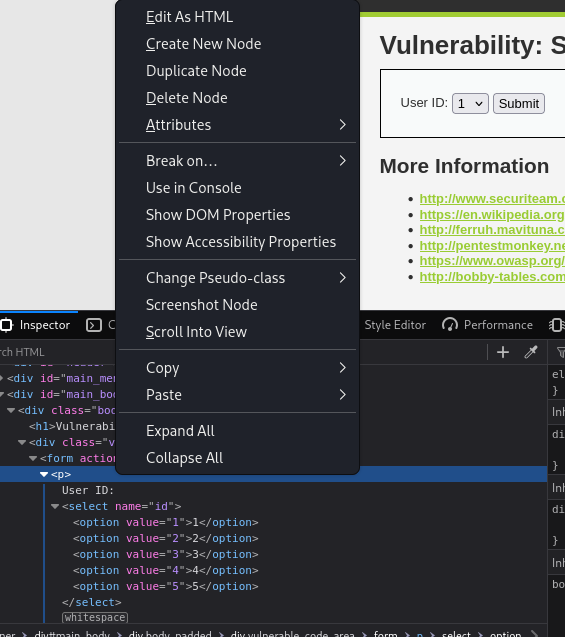
* Nhập vào 1 'or '1' = '1 UNION SELECT \* from password ta được kết quả như sau



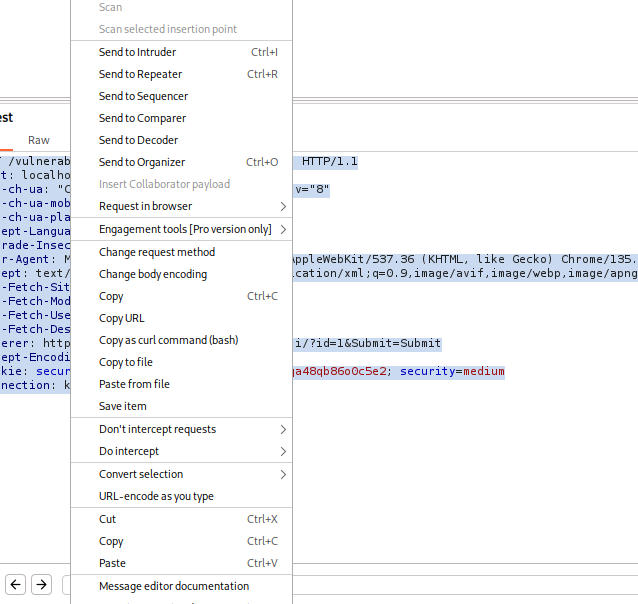
* Mở BurpSuite và truy cập vào DVWA trên BurpSuite



* Edit HTMl để chuyển từ nhập sang chọn trong một Dropdown

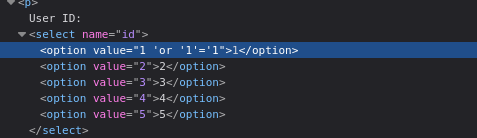


* Chọn Send to Repeater

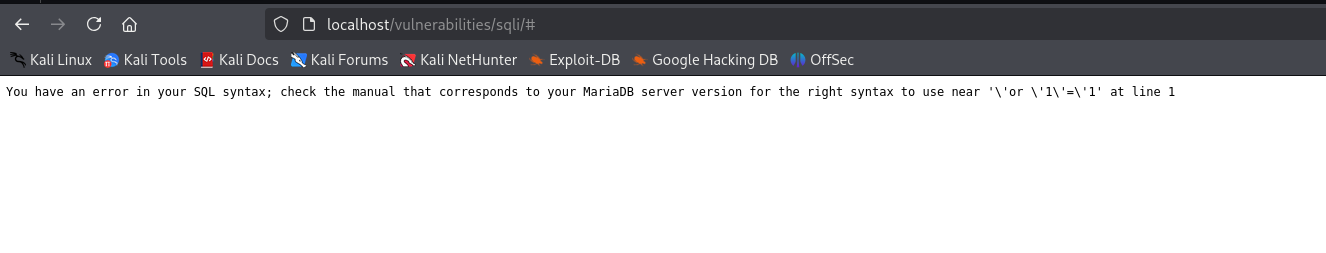




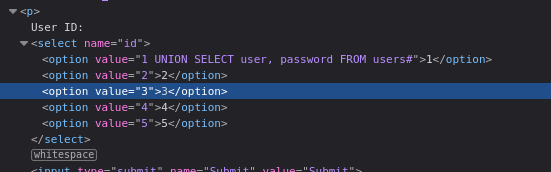
* Chèn mã độc SQL Injection vào Value của html



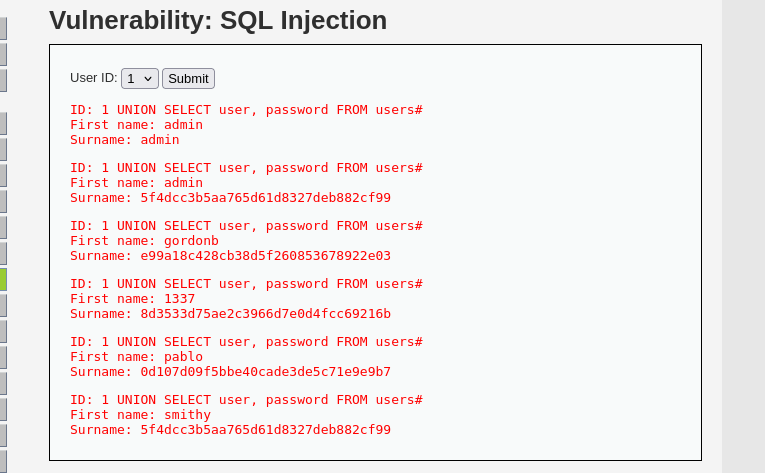
* Ấn Submit thì ta được chuyển sang trang chứa lỗi truy vấn của SQL nghĩa là nếu ta truyền như vậy thì mã độc đã được gửi đến Database và thực hiện truy vấn.



* Thử câu lệnh truy vấn khác



* Kết quả nhận được nhưu sau



4.2. Tham khảo các tài liệu đính kèm để khai thác lỗi **SQL injection** trên DVWA (security ở mức độ medium) để lấy mật khẩu người dùng **gordonb**.

<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#SQL_Injection>

<https://youtu.be/5bj1pFmyyBA>

<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2007:%20SQL%20Injection.md>

<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/medium/Challenge%2007:%20SQL%20Injection.md>

Chọn mật khẩu, tài khoản gordonb để giải mã:

4.3. Tham khảo mã nguồn (view source), giải thích ngắn gọn cách DVWA với security ở mức độ medium, high, impossible ngăn chặn tấn công khai thác lỗi SQL injection.

- Medium: sử dụng mysql\_real\_escape\_string (). Điều này không cho phép các dấu ngoặc kép trong giá trị được truyền. Chỉ cho người dùng chọn danh sách chọn để hạn chế bị chèn lệnh.

- High: yêu cầu nhập ID người dùng trên một trang khác nhưng vẫn tồn tại lỗ hổng bảo mật như mức độ Easy.

- Impossible: Kiểm tra xem có phải người dùng nhập số không và đảm bảo chỉ có một kết quả truy vấn được trả về.

---HẾT---