**LAB 4**

**Web Attack and Defense**

|  |
| --- |
| Họ tên và MSSV:Nguyễn Thái Hoành  Lớp: 10\_ĐH\_CNPM1  Linkyoutube:https://www.youtube.com/@Ho%C3%A0nhNguy%E1%BB%85nTh%C3%A1i  Link github: https://github.com/THAIHOANH/lab4-.git |

* *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.*

**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

Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

- Tải và thực thi image của DVWA từ Docker Hub

docker run --rm -it -p 81:81 vulnerables/web-dvwa

Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, máy tính

Nội dung do AI tạo ra có thể không chính xác.

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

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

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

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Nội dung do AI tạo ra có thể không chính xác.

- Sau khi hoàn thành bài thực hành dừng container DVWA

docker container ls

docker stop <container name>

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

(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)

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, phần mềm, Biểu tượng máy tính, Trang web

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

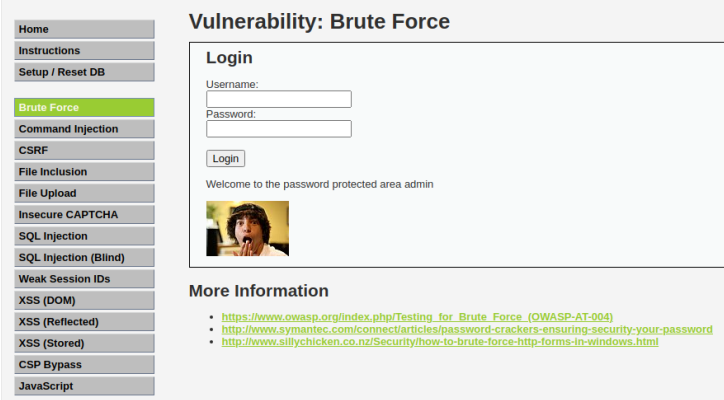
Nội dung do AI tạo ra có thể không chính xác.

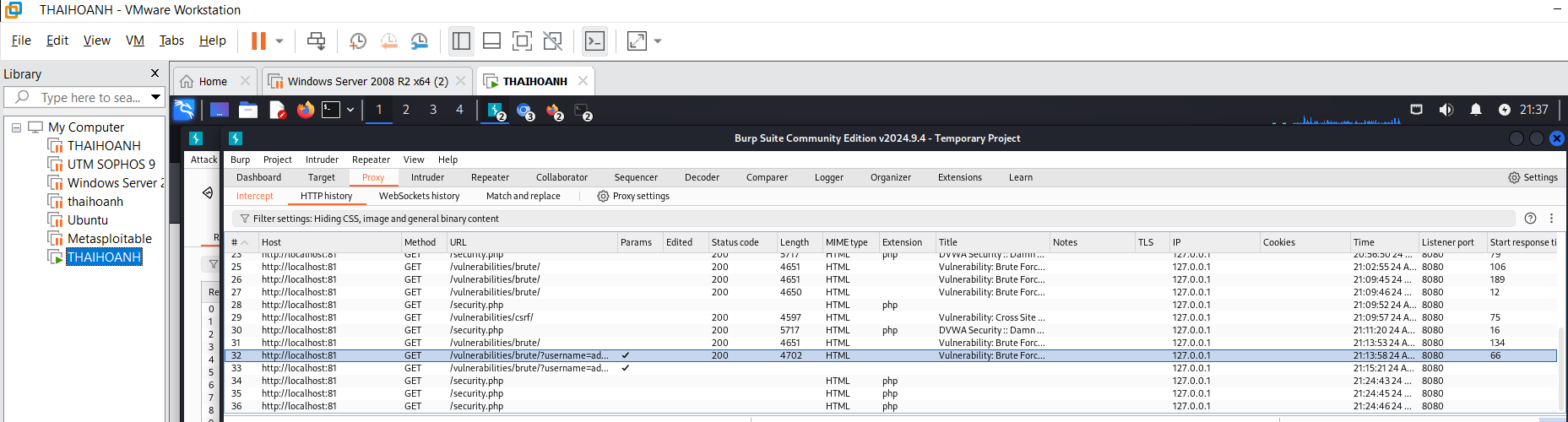
Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.





Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

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.

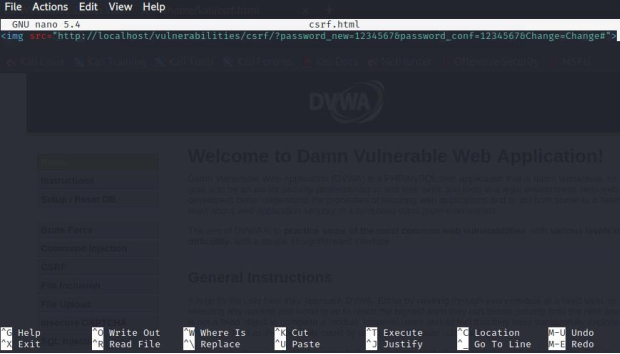
<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#CSRF>

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

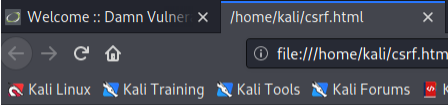
<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2003:%20CSRF.md>

(Chụp hình minh họa quá trình thực hiện)

Soạn file csrf.html chứa yêu cầu giả mạo:



Người dùng đăng nhập vào nhuw bình thường, người dùng click vào link giả mạo yêu cầu và sau đó mật khẩu bị đổi mà không hay biết



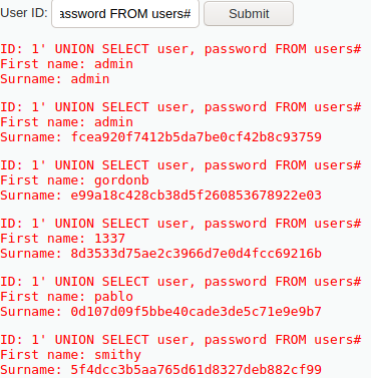
3.2. Tham khảo mã nguồn (view source), giải thích ngắn gọn cách DVWA với security ở mức độ medium, high, impossible ngăn chặn tấn công khai thác lỗi CSRF.

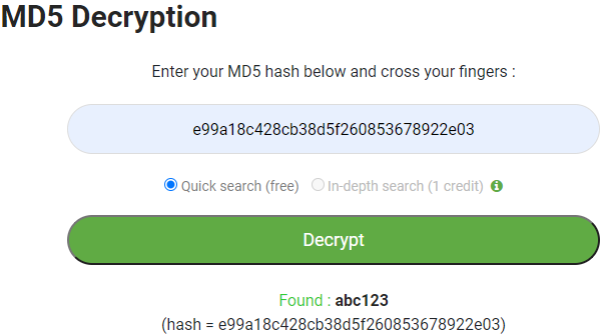
(Chụp hình minh họa quá trình thực hiện)

* 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**.





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**.

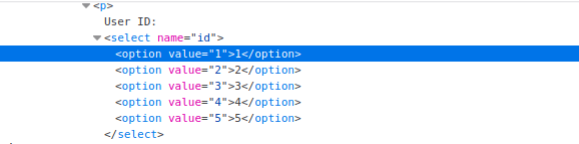
<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#SQL_Injection>

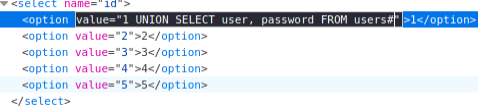
<https://youtu.be/5bj1pFmyyBA>

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

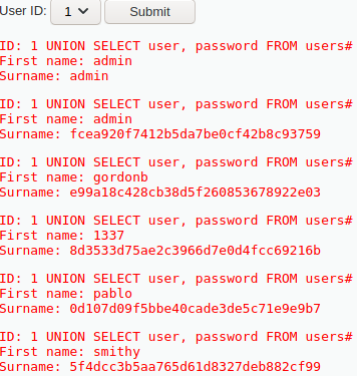
<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/medium/Challenge%2007:%20SQL%20Injection.md>

Mở giao diện dành cho nhà phát triển rồi coppy một câu lệnh để sửa:

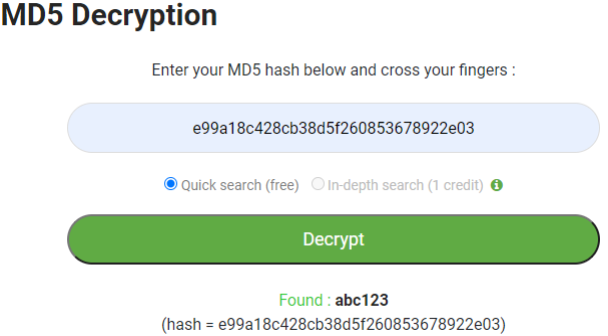




Khi chạy lệnh:



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---