

1

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Web Application Firewall

Thực hành môn An toàn mạng máy tính nâng cao

Tháng 3/2024

Lưu hành nội bộ

<Ng nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

- Tìm hiểu và triển khai Web Application Firewall.

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Máy tính/máy ảo Hệ điều hành Kali Linux (Tải xuống tại: <https://www.kali.org/get-kali/>)
- DVWA
- Modsecurity

C. THỰC HÀNH

1. Cài đặt và cấu hình DVWA

DVWA là viết tắt của Damn Vulnerable Web Application, một ứng dụng web PHP/MySQL chứa nhiều lỗ hổng đã biết

DVWA được thiết kế để giúp các nhà phát triển web và chuyên gia bảo mật tìm hiểu về bảo mật ứng dụng web.

a. Cài đặt và cấu hình DVWA Apache website

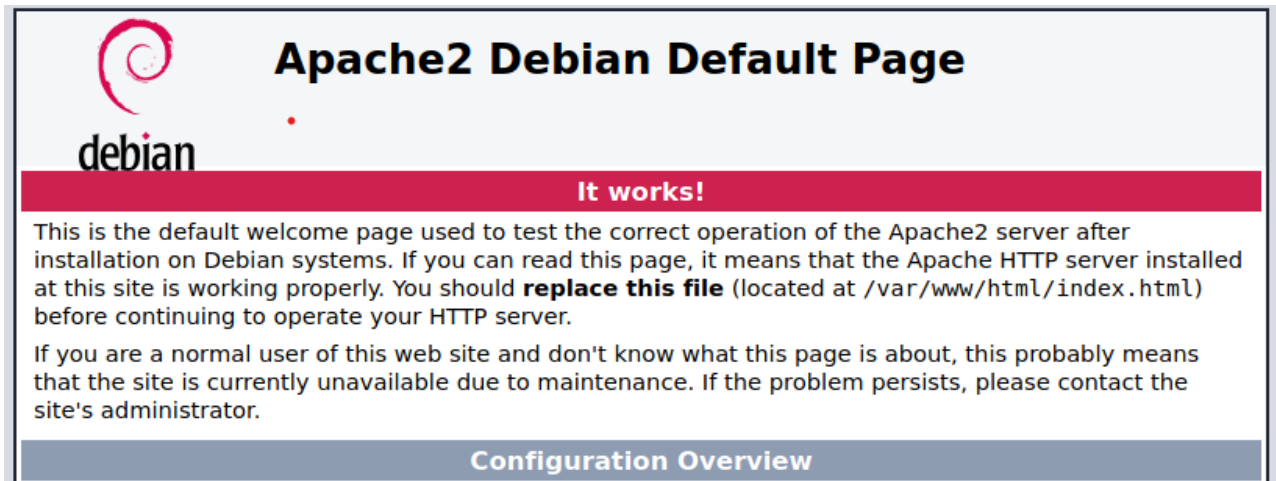
Để tải xuống source code DVWA, sử dụng Terminal thực thi các lệnh sau:

```
cd /var/www/html
git clone https://github.com/digininja/DVWA.git
sudo chmod 777 DVWA
```

Khởi động *apache2* service:

```
sudo service apache2 start
```

Sử dụng trình duyệt bất kỳ (Chrome, Firefox,...) truy cập vào địa chỉ to <http://127.0.0.1/> để kiểm tra Apache server đã triển khai thành công hay chưa.

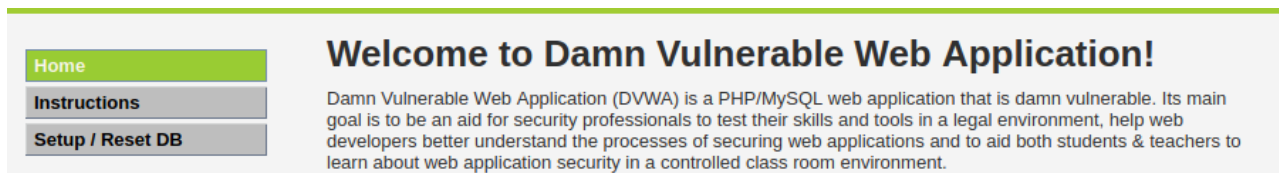


Hình 1 Apache server đã cài đặt và khởi động thành công

Thực thi các lệnh sau trong Terminal để cấu hình DVWA:

```
cd DVWA
sudo cp config/config.inc.php.dist config/config.inc.php
```

Truy cập vào đường dẫn <http://127.0.0.1/DVWA> trên trình duyệt. Bạn sẽ thấy trang Welcome Page:



Hình 2 Welcome page DVWA

b. Tạo DVWA user trong local database

Truy cập <http://127.0.0.1/DVWA/setup.php> Sau đó chọn **Create/Reset database** để tạo DVWA user.

Bây giờ DVWA đã sẵn sàng để tiến hành các thử nghiệm tấn công.

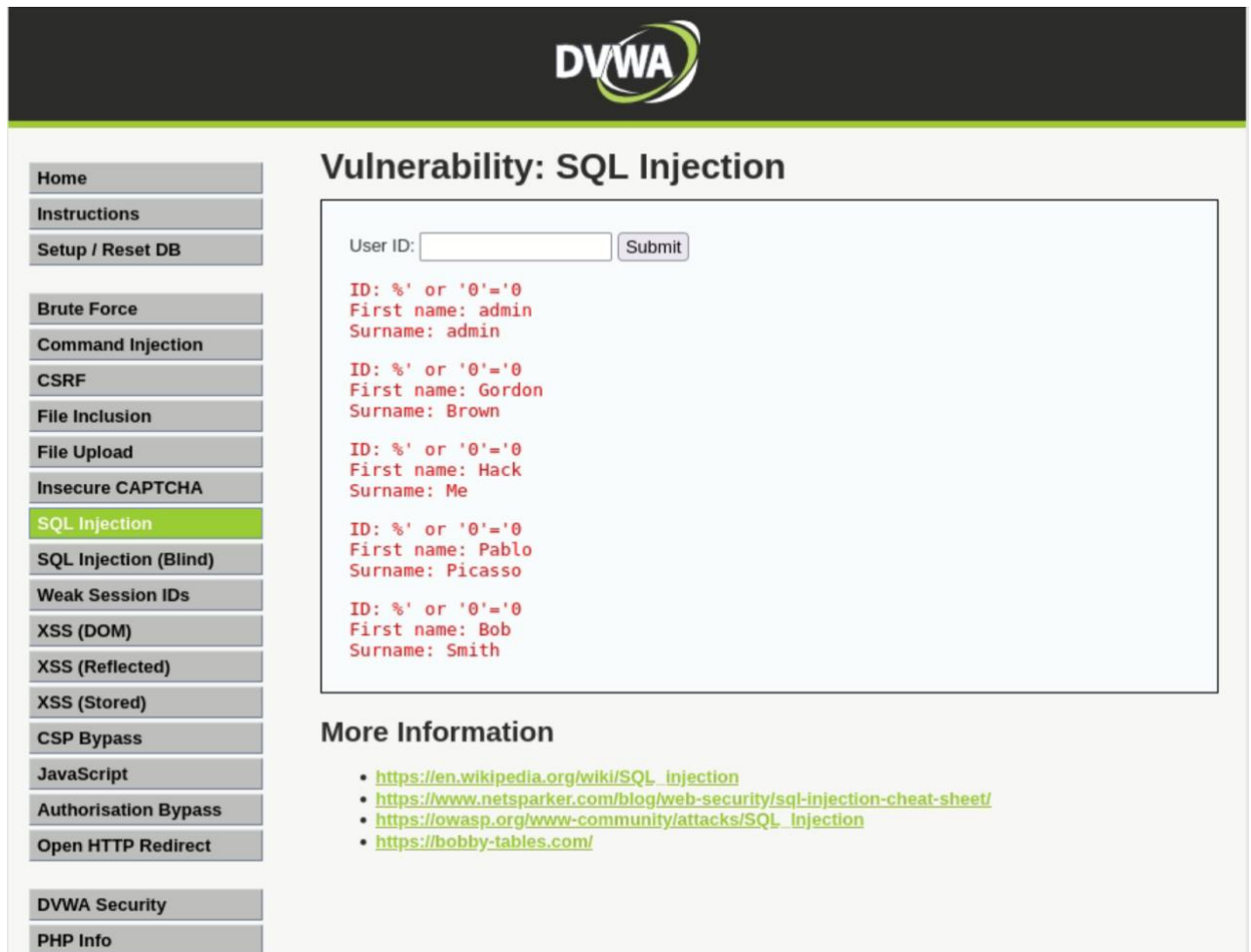
c. Thử nghiệm tấn công trên DVWA

DVWA cung cấp môi trường thử nghiệm các loại tấn công khác nhau. Dưới đây sẽ là hướng dẫn thực nghiệm tấn công SQL Injection.

Sau khi đăng nhập vào DVWA, tại thanh điều hướng, chọn SQL Injection. Tại ô User ID ta có thể nhập thông tin truy vấn.

Với các truy vấn thông thường, kết quả trả về là thông tin của User tương ứng với User ID. Để tấn công SQL Injection, thực hiện nhập câu lệnh truy vấn sau:

```
%' or '0'='0
```



DVWA

Vulnerability: SQL Injection

User ID:

ID: '%' or '0'='0
First name: admin
Surname: admin

ID: '%' or '0'='0
First name: Gordon
Surname: Brown

ID: '%' or '0'='0
First name: Hack
Surname: Me

ID: '%' or '0'='0
First name: Pablo
Surname: Picasso

ID: '%' or '0'='0
First name: Bob
Surname: Smith

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Navigation Links:

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection**
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- Authorisation Bypass
- Open HTTP Redirect
- DVWA Security
- PHP Info

Task: Thực hiện các tấn công khác trên DVWA

2. ModSecurity Web Application Firewall

ModSecurity là tường lửa ứng dụng web (WAF) cung cấp lớp bảo mật bổ sung cho các ứng dụng web. Nó là một mô-đun mã nguồn mở dành cho Máy chủ HTTP Apache, IIS và Nginx giúp bảo vệ các trang web có lỗ hổng web (SQLi, XSS, Path Traversal, ...). Mô-đun này hoạt động bằng cách phân tích các yêu cầu HTTP đến và áp dụng một bộ quy tắc để xác định và chặn các cuộc tấn công tiềm ẩn. Các quy tắc này có thể được tùy chỉnh để đáp ứng các yêu cầu bảo mật cụ thể của trang web hoặc ứng dụng.

Các tính năng của ModSecurity:

- Ngăn chặn các cuộc tấn công vào ứng dụng web (hỗ trợ Apache)
- Mã nguồn mở
- Ghi nhật ký và giám sát
- Hỗ trợ SSL/TLS
- Quy tắc tùy chỉnh

Phương pháp triển khai:

- **Embedded:** triển khai cùng với Máy chủ Web (chỉ một VM)
- **Reverse Proxy:** riêng biệt như một nút đứng trước Web Server

a. Cài đặt ModSecurity

Cài đặt ModSecurity

```
sudo apt install libapache2-mod-security2 -y
sudo a2enmod headers
sudo systemctl restart apache2
```

Cấu hình ModSecurity theo tập tin cấu hình mẫu:

```
sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

Sửa cấu hình tập tin /etc/modsecurity/modsecurity.conf. Thay đổi trường **SecRuleEngine** thành **On**

Khởi động lại apache server:

```
sudo systemctl restart apache2
```

b. Cấu hình Rule

ModSecurity sử dụng ModSecurity Rule Language rất linh hoạt để thiết lập các quy tắc.

Tham khảo hướng dẫn sử dụng ModSecurity Rule Language tại link

<https://github.com/owasp-modsecurity/ModSecurity/wiki/Reference-Manual-%28v3.x%29>

Trong nội dung bài thực hành này, chúng ta sẽ tham khảo bộ core rule OWASP sử dụng cho

ModSecurity tại link: <https://github.com/coreruleset/coreruleset>

Để cấu hình rule cho ModSecurity, chúng ta có thể cấu hình trực tiếp tại tập tin

/etc/httpd/conf.d/mod_security.conf hoặc cấu hình rule thành một tập tin riêng biệt.

Để có thể cấu hình file riêng biệt, chúng ta cần thêm dòng sau vào để hệ thống include sang 1 file cấu hình khác: **Include “/đường dẫn file cần tham chiếu/tên_file.conf”**

Dưới đây là ví dụ cho file cấu hình /etc/httpd/conf.d/mod_security.conf với tập tin cấu hình rule được lưu trữ tại /usr/share/modsecurity-crs

```
<IfModule security2_module>
    SecDataDir /var/cache/modsecurity
    Include /usr/share/modsecurity-crs/crs-setup.conf
    Include /usr/share/modsecurity-crs/rules/*.conf
</IfModule>
```

Task: Sử dụng bộ Core rule OWASP cấu hình cho ModSecurity và demo ít nhất 3 hành động trái phép được phát hiện và chặn bởi ModSecurity. Tham khảo:

https://github.com/khangtictoc/DVWA_ModSecurity_Deployment

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

- Báo cáo:
 - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
 - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
 - Ví dụ: [NT534.K11.ANTN.1]-Lab1_1852xxxx_1852yyyy.
 - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
 - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!