Môn học: Lập trình Web
LAB 05
Web Security

I. Mục tiêu

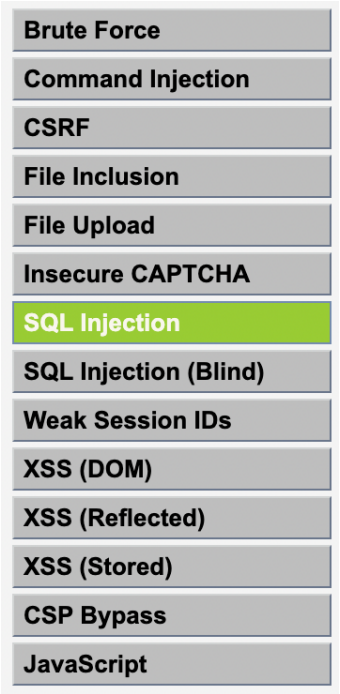
- Hiểu biết một số lỗ hổng bảo mật cơ bản trong ứng dụng web.
- Cài đặt môi trường thực hành pentest hợp pháp sử dụng công cụ DVWA.
- Thực hiện khai thác thử nghiệm các lỗ hổng bảo mật web trong mã nguồn DVWA.
- Tìm hiểu cách khắc phục một số lỗ hổng bảo mật web cơ bản trong ứng dụng Web sử dụng PHP.

II. Các bước thực hiện

Chú ý: các file liên quan đến bài Lab và tài liệu tham khảo được đặt trong thư mục **"refs"**

1. Giới thiệu DVWA

- DVWA (Damn Vulnerable Web Application) là một ứng dụng mã nguồn mở sử dụng PHP/MySQL tập hợp các lỗ hổng bảo mật ứng dụng web trong mã nguồn PHP.
- Mục tiêu chính của DVWA đó là tạo ra một môi trường thực hành pentest hợp pháp. Giúp cho người học/nghiên cứu hiểu hơn về các lỗ hổng bảo mật trong ứng dụng web, từ đó giúp cho việc lập trình ứng dụng web được bảo mật hơn.
- Công cụ hỗ trợ thực hành tấn công khai thác lỗi bảo mật ứng dụng web ở mức cơ bản và nâng cao.
- Các lỗ hổng bảo mật web được hiện thực trong mã nguồn DVWA bao gồm:



2. Các mức độ bảo mật hiện thực trong DVWA

- DVWA cung cấp 4 mức độ bảo mật tương ứng 3 level từ dễ cho đến khó gồm :
  - **Low**: mức độ thấp nhất mà DVWA cung cấp, mã nguồn PHP phơi bày khả năng tấn công khai thác lỗ hổng qua việc lập trình viết mã chưa bao quát vấn đề bảo mật.
  - **Medium**: mức độ trung bình cung cấp mã nguồn đã fix lỗ hổng cơ bản ở mức 'low'. Tuy nhiên lỗ hổng vẫn còn có thể được khai thác.
  - **High**: mức độ cao, bao gồm ví dụ về cách fix lỗ hổng chưa tốt, một số lỗ hổng có thể không còn khai thác được nữa ở chế độ này.
  - **Impossible**: hiện thực mã nguồn đã được tối ưu ở mức an toàn bảo mật, có thể dùng để tham khảo khi lập trình.

- Tính năng view source cho phép người dùng xem mã nguồn tương ứng của mỗi cấp độ.

3. Cài đặt công cụ DVWA

Download mã nguồn công cụ DVWA

Truy cập vào URL bên dưới để tải về mã nguồn của công cụ DVWA
https://github.com/digininja/DVWA
Hoặc sử dụng file có sẵn trong bài Lab (dvwa.zip)

Cài đặt công cụ DVWA

1. Giải nén file mã nguồn vào thư mục web root
2. Vào thư mục config, đổi tên file **config.inc.php.dist** thành **config.inc.php**
3. Tạo một CSDL trong hệ quản trị CSDL MySQL, ví dụ: dvwa
4. Mở file **config.inc.php**, nhập các thông tin cần thiết để kết nối CSDL MySQL đã tạo:

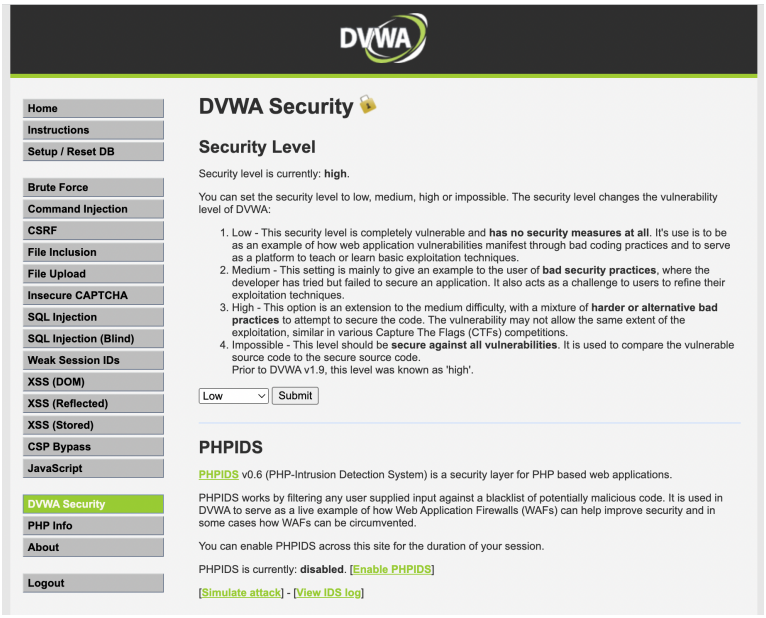
```
# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';
```

5. Khởi động trình duyệt web, truy cập vào địa chỉ URL bên dưới để tiến hành cài đặt:
   http://localhost/setup.php
6. Nhấn nút **Create / Reset Database** để tạo/reset CSDL cho ứng dụng DVWA
7. Đăng nhập vào công cụ DVWA sử dụng username/password mặc định:
   Username: admin
   Password: password

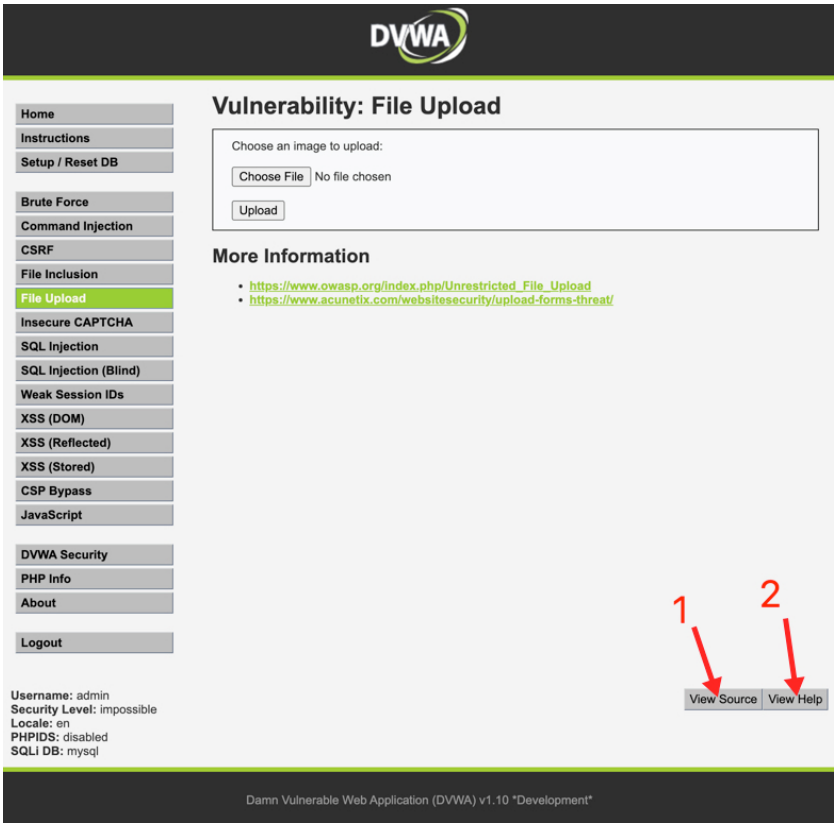
❖ Bài tập

Hướng dẫn chung:

- Chọn level thử nghiệm: Chọn mục DVWA Security ở menu bên trái, chọn level tương ứng (low, medium, high, impossible).



- Lặp lại với các level khác: xem xét mã nguồn của trang web hiện tại bằng cách nhấn vào nút **View Source** (1), xem hướng dẫn thực hiện tấn công cho mỗi level bằng cách nhấn vào nút **View Help** (2) như hình bên dưới.



1. Reflected XSS

Định nghĩa

Reflected XSS là dạng tấn công thường gặp nhất trong các loại hình XSS. Với Reflected XSS, kẻ tấn công gửi trực tiếp liên kết có chứa mã độc cho người dùng, khi người dùng click vào link này thì trang web sẽ được load và các đoạn script độc hại sẽ được chạy. Reflected XSS thường được kẻ tấn công dùng để ăn cắp cookie, chiếm session của người dùng trong ứng dụng web.

Các bước mô phỏng lỗ hổng Reflected XSS bằng DVWA

Bước 1.

- Chọn mục "XSS reflected" ở menu bên trái
- Nhập tên của bạn vào ô nhập
- Nhấn nút Submit

Chú ý rằng tên đã nhập xuất hiện trên màn hình. Tính năng này được thiết kế đơn giản là nhận dữ liệu đầu vào, sau đó hiển thị giá trị này trên trang web khi người dùng submit.

Bước 2. Trong mục "What's your name?", nhập vào thông tin sau:

```
<script>alert("Hello")</script>
```

Bước 3. Nhấn nút Submit

Trả lời câu hỏi:

Một hộp thoại alert đã được gọi sau khi nhấn nút submit, điều này làm cho tính năng của trang web hoạt động không còn giống như thiết kế. Hãy giải thích tại sao điều này có thể xảy ra?

Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

2. Stored XSS

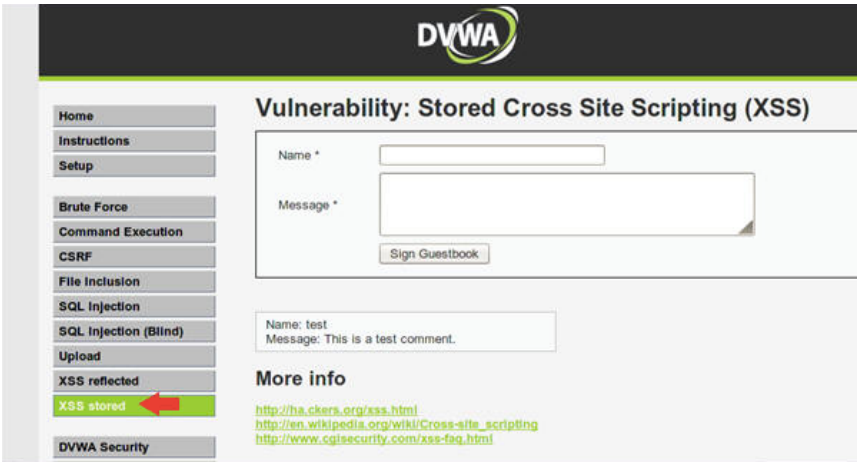
Định nghĩa

Stored XSS là dạng tấn công mà hacker chèn trực tiếp các mã độc vào cơ sở dữ liệu của ứng dụng web. Tấn công này xảy ra khi các dữ liệu được gửi lên server không được kiểm

tra kỹ trước mà lưu vào cơ sở dữ liệu. Khi người dùng truy cập vào trang web này thì những đoạn script độc hại sẽ được thực thi chung với quá trình load trang web.

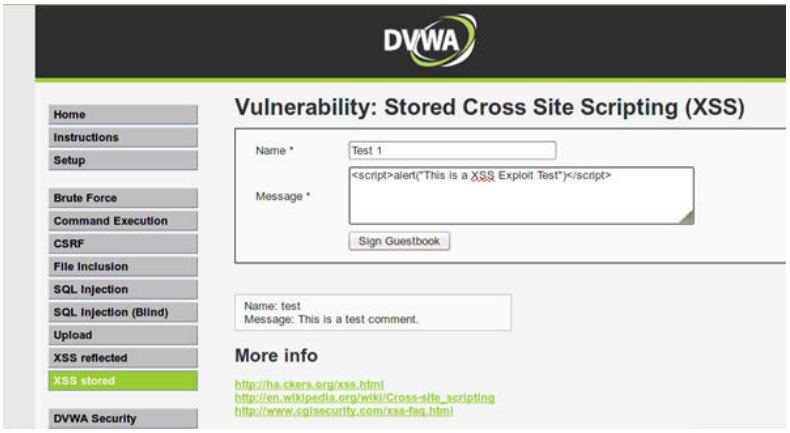
Các bước mô phỏng lỗ hổng Stored XSS bằng DVWA

Bước 1. Chọn mục "XSS Stored" ở menu bên trái.



Bước 2. Nhập thông tin sau vào form

Name: Test 1
Message: <script>alert("This is a XSS Exploit Test")</script>



Bước 3. Nhấn nút **Sign Guestbook**

Trả lời câu hỏi:

Chú ý rằng mỗi lần reload lại trang web thì trên màn hình đều xuất hiện hộp thoại alert, điều này làm cho tính năng của trang web hoạt động không còn giống như thiết kế. Hãy giải thích tại sao điều này có thể xảy ra?

Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

3. XSS Stored với IFRAME

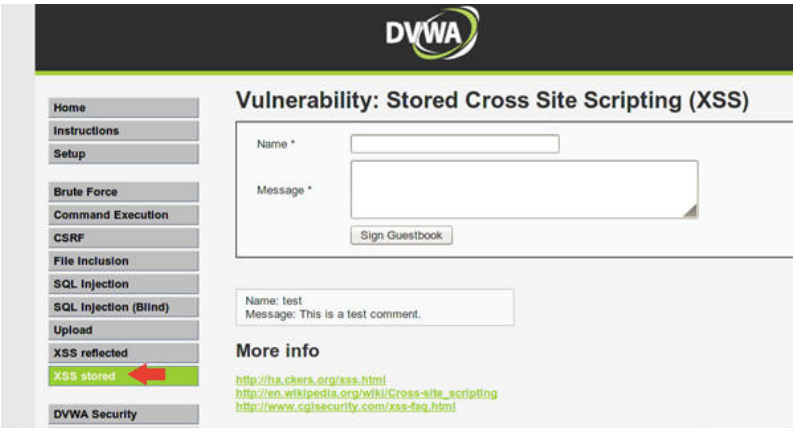
Các bước mô phỏng lỗ hổng Stored XSS với IFRAME bằng DVWA

Bước 1. Reset cơ sở dữ liệu

- Chọn mục "Setup / Reset DB" ở menu bên trái.
- Nhấn nút **Create / Reset Database**.

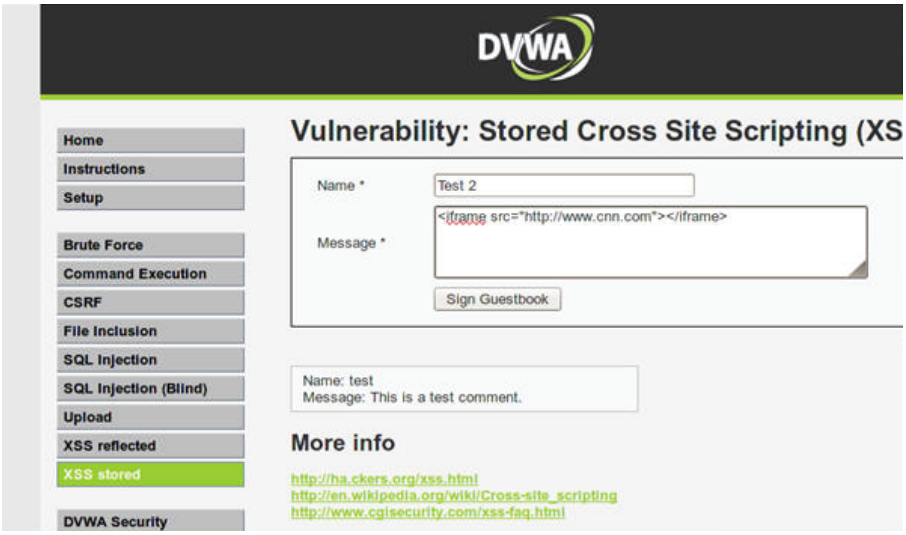
Chúng ta nên reset lại dữ liệu của ứng dụng sau mỗi lần thử nghiệm tấn công vào các lỗ hổng.

Bước 2. Chọn mục "XSS Stored" ở menu bên trái



Bước 3. Nhập vào form form thông tin sau

Name: Test 2 Message: <iframe src="https://hcmut.edu.vn"></iframe>



Bước 4. Nhấn nút **Sign Guestbook**

Trả lời câu hỏi

Chú ý rằng nội dung của trang web https://hcmut.edu.vn hiển thị bên dưới "Test 2", kẻ tấn công có thể khai thác lỗ hổng này bằng cách nhúng trang web giả có chứa mã độc và đánh lừa người dùng thao tác. Hãy nêu cách khắc phục lỗ hổng này?

Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

4. Brute Force

Sinh viên thực hành theo các bước, ghi trả lời/ảnh chụp màn hình vào file báo cáo:
Bước 1. Reset cơ sở dữ liệu của ứng dụng DVWA
Bước 2. Tìm hiểu về lỗ hổng Brute Force?
Bước 3. Thực hành Demo lỗ hổng Brute Force trên ứng dụng DVWA, nêu ra những nguy cơ của lỗ hổng đối với ứng dụng web, chụp ảnh màn hình các bước thực hiện.
Bước 4. Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

5. Command Execution

Sinh viên thực hành theo các bước, ghi trả lời/ảnh chụp màn hình vào file báo cáo:
Bước 1. Reset cơ sở dữ liệu của ứng dụng DVWA
Bước 2. Tìm hiểu về lỗ hổng Command Execution?
Bước 3. Thực hành Demo lỗ hổng Command Execution trên ứng dụng DVWA, nêu ra những nguy cơ của lỗ hổng đối với ứng dụng web, chụp ảnh màn hình các bước thực hiện.
Bước 4. Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

6. CSRF

Sinh viên thực hành theo các bước, ghi trả lời/ảnh chụp màn hình vào file báo cáo:
Bước 1. Reset cơ sở dữ liệu của ứng dụng DVWA
Bước 2. Tìm hiểu về lỗ hổng CSRF?
Bước 3. Thực hành Demo lỗ hổng CSRF trên ứng dụng DVWA, nêu ra những nguy cơ của lỗ hổng đối với ứng dụng web, chụp ảnh màn hình các bước thực hiện.
Bước 4. Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

7. File Inclusion

Sinh viên thực hành theo các bước, ghi trả lời/ảnh chụp màn hình vào file báo cáo:
Bước 1. Reset cơ sở dữ liệu của ứng dụng DVWA
Bước 2. Tìm hiểu về lỗ hổng File Inclusion?
Bước 3. Thực hành Demo lỗ hổng File Inclusion trên ứng dụng DVWA, nêu ra những nguy cơ của lỗ hổng đối với ứng dụng web, chụp ảnh màn hình các bước thực hiện.
Bước 4. Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

8. SQL Injection & SQL Injection (Blind)

Sinh viên thực hành theo các bước, ghi trả lời/ảnh chụp màn hình vào file báo cáo:
Bước 1. Reset cơ sở dữ liệu của ứng dụng DVWA
Bước 2. Tìm hiểu về lỗ hổng SQL Injection & SQL Injection (Blind)?
Bước 3. Thực hành Demo lỗ hổng trên ứng dụng DVWA, nêu ra những nguy cơ của lỗ hổng đối với ứng dụng web, chụp ảnh màn hình các bước thực hiện.
Bước 4. Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

9. Upload

Sinh viên thực hành theo các bước, ghi trả lời/ảnh chụp màn hình vào file báo cáo:
Bước 1. Reset cơ sở dữ liệu của ứng dụng DVWA
Bước 2. Tìm hiểu về lỗ hổng được demo trong ứng dụng DVWA?
Bước 3. Thực hành Demo lỗ hổng trên ứng dụng DVWA, nêu ra những nguy cơ của lỗ hổng đối với ứng dụng web, chụp ảnh màn hình các bước thực hiện.
Bước 4. Xem mã nguồn của tính năng ở các level khác nhau (Low, Medium, High, Impossible) và thử tìm cách khai thác lỗ hổng ở các level này, rút ra kết luận về việc hiện thực tính năng để tránh được lỗ hổng trên.

III. Cách thức nộp bài

- Thực hành theo các bước đã cho trong bài Lab, chụp ảnh màn hình và trả lời các câu hỏi trong file **<MSSV>.docx** và nộp bài vào mục "Nộp bài Lab 05". Làm tất cả các mục trong phần bài tập.
- Các bài nộp sai quy định sẽ không được tính điểm.
- Các bài làm giống nhau sẽ bị xem là gian lận và bị 0 điểm,
- **Chỉ nhận bài nộp thông qua LMS, không nhận bài nộp qua email hay các hình thức khác.**

--HẾT--