Introduction to OWASP ZAP

Task 1: Intro to ZAP

- Zap là viết tắt của Zed attack proxy
- Triển khai máy ảo của Tryhackme và truy cập vào IP của THM ta vào đươc trang web DVWA

Task 2: Disclaimer

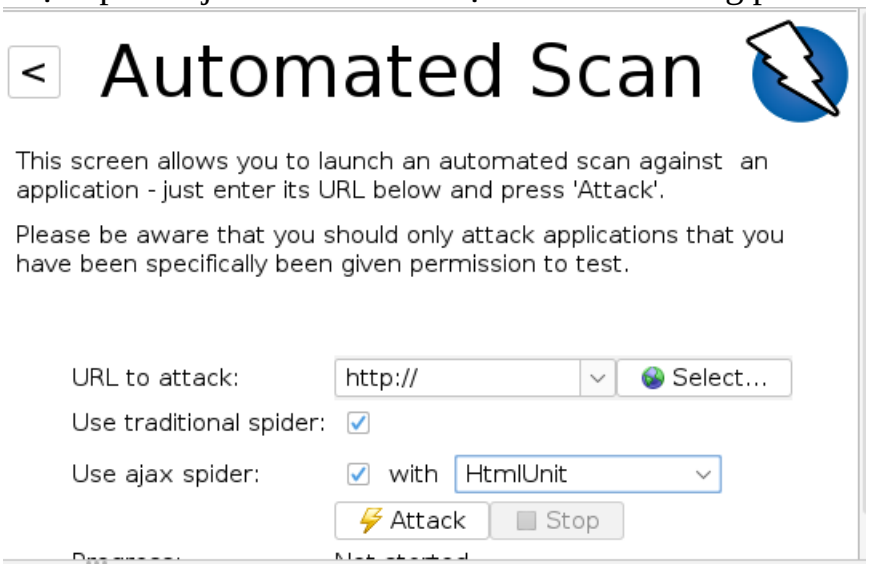
- Đọc kĩ hướng dãn trách nhiệm của Task

Task 3: Installation

- Cài đặt và sử dụng phần mềm Owasp Zap

Task 4: How to perform an automated scan

- Ta tải HtmlUnit về và cài đặt sau đó vào Zap chon automated scan tiếp đó chọn spider ajax và tick vào chọn HtmlUnit trong phần chọn xuống



Task 5: Manual Scanning

- Ta làm theo hướng dẫn của THM cài đặt proxy và certificate trên Zap và trên trình duyệt wep

Task 6: Scanning an Authenticated Web Application

- Ta truy cập DVWA bằng IP của THM sau đó ta chuyển qua tab security rồi mở dev tool trên web lên qua tab storage kiển tra PHPSESIS

PHPSESSID	4arvkd1v7nqkp8roq0gn6vhag2
security	low

Tiếp đó trên ZAP ta vào HTTP Sessions vào kiểm tra session trùng với web thì chuột phải set as active

Task 7: Brute-force Directories

- Ta tải thư mục của THM sau đó ở ZAP ta vào tools>options> forced browse>add custums file và bỏ file vừa tải về vào. Sau đó ở site chuột phải>attack>forced browse list nhấp vào file vừa impost vào và nhấn nút chạy

Task 8: Bruteforce Web Login

- Làm theo yêu cầu của task và với mật khẩu lơn hơn 8 kí tự ta đã dò ra đuược mật khẩu

Reflected	password
	Password1
	Password1!
	P@ssw0rd
	password12
	Password12
Reflected	security

Task 9: ZAP Extensions

- Ta làm theo hướng dẫn của Task tải về và cài đặt them extension trong ZAP

Task 10: Further Reading