# CÔNG CỤ ZAP

## Giới thiệu về ZAP:

OWASP Zed Attack Proxy (ZAP) là một công cụ miễn phí và phổ biến được duy trì bởi hằng trăm nghìn tình nguyện viên trên toàn thế giới. Nó là công cụ bổ ích khi kiểm tra bảo mật thủ công vì nó giúp chúng ta tìm ra các lỗ hỏng bảo mật trên website một cách tự động.
ZAP là được gọi là "man-in-the-middle proxy", nó đứng giữa trình duyệt của người test và ứng dụng web, nó có thể ngăn chặn và kiểm trả các thông điệp được gửi đi, sửa đổi và gửi tiếp các thông điệp đó đến đích.

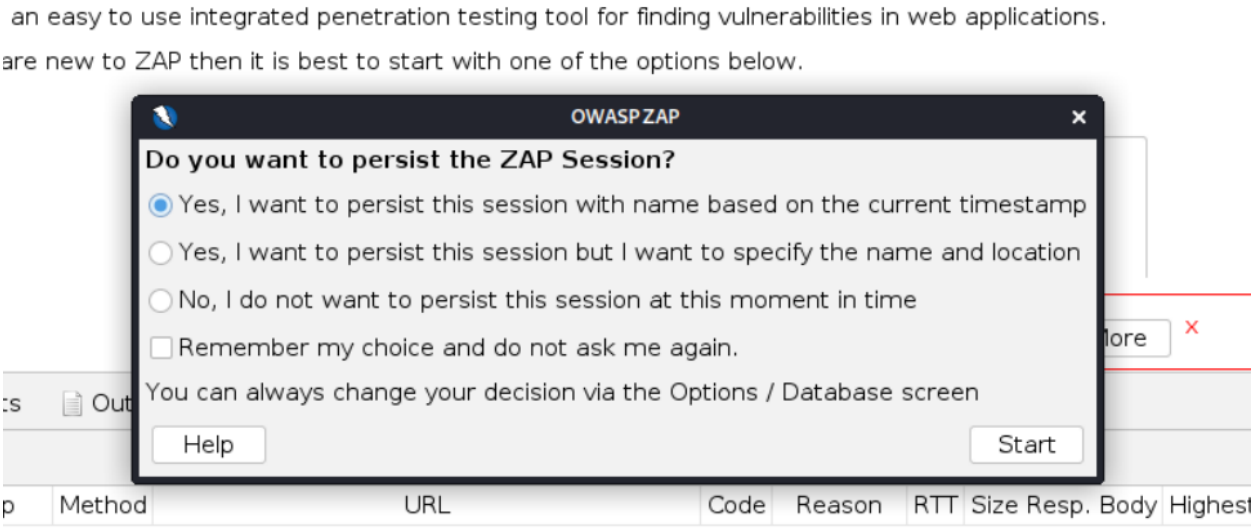
## Các tính năng cơ bản của ZAP:

- Intercepting Proxy
- Traditional and AJAX spiders
- Automated scanner
- Passive scanner
- Forced browsing
- Fuzzer
- Dynamic SSL certificates
- Smartcard and Client Digital Certificates support
- Web sockets support
- Support for a wide range of scripting languages
- Plug-n-Hack support
- Authentication and session support
- Powerful REST based API
- Automatic updating option
- Integrated and growing marketplace of add-ons

## Sử dụng ZAP tool với chế độ Automated scan:

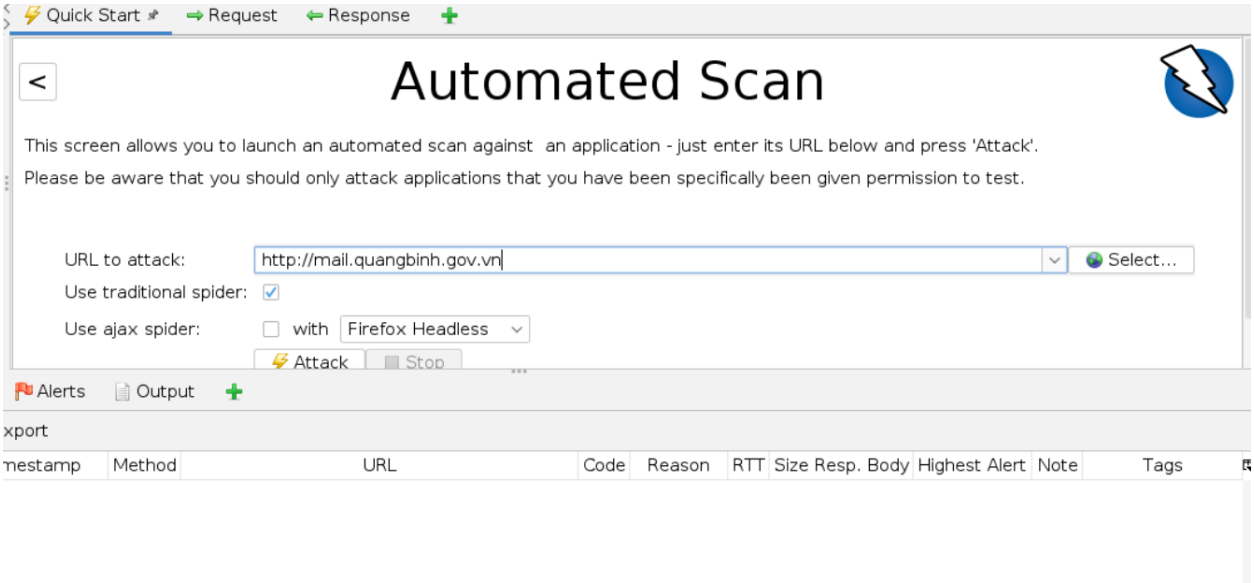
### *Bước 1:*

Khi open App bạn sẽ được lựa chọn có lưu giữ lại Session hay không. Theo mặc định, ZAP session sẽ được ghi vào đĩa ở HSQLDB với tên và location mặc định. Nếu bạn lựa chọn không duy trì session, các tệp được ghi sẽ được xóa khi thoát ZAP. Nếu bạn duy trì session, thông tin sẽ được ghi lại, bạn sẽ có thể truy cập lại tệp và tùy chỉnh tên và vị trí.



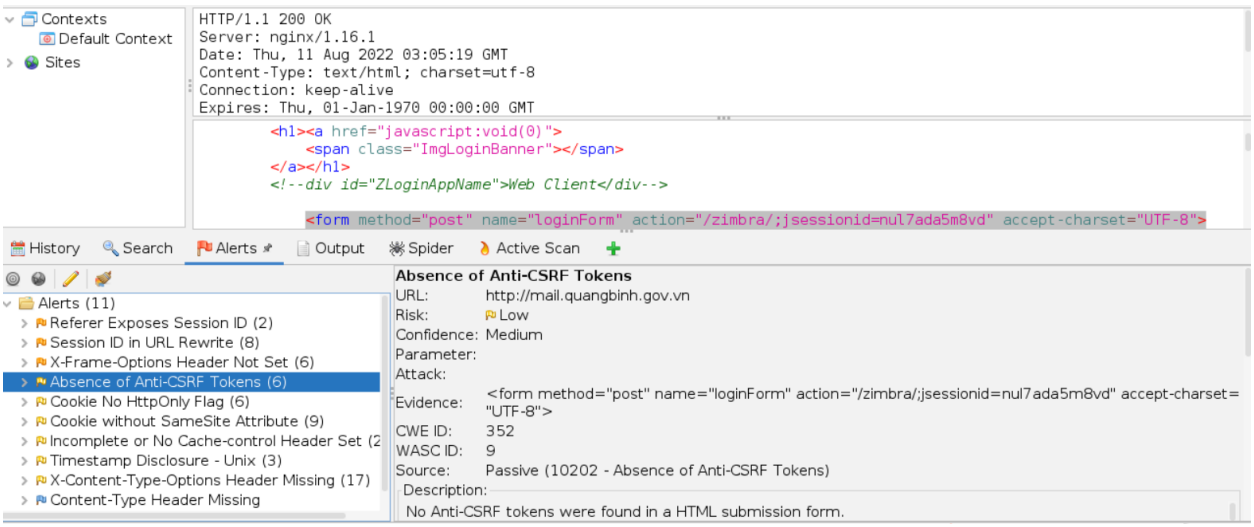
***Bước 2:***

Nhập URL của website mà bạn muốn check vào field URL to attack




***Bước 3:***

Click Attack button



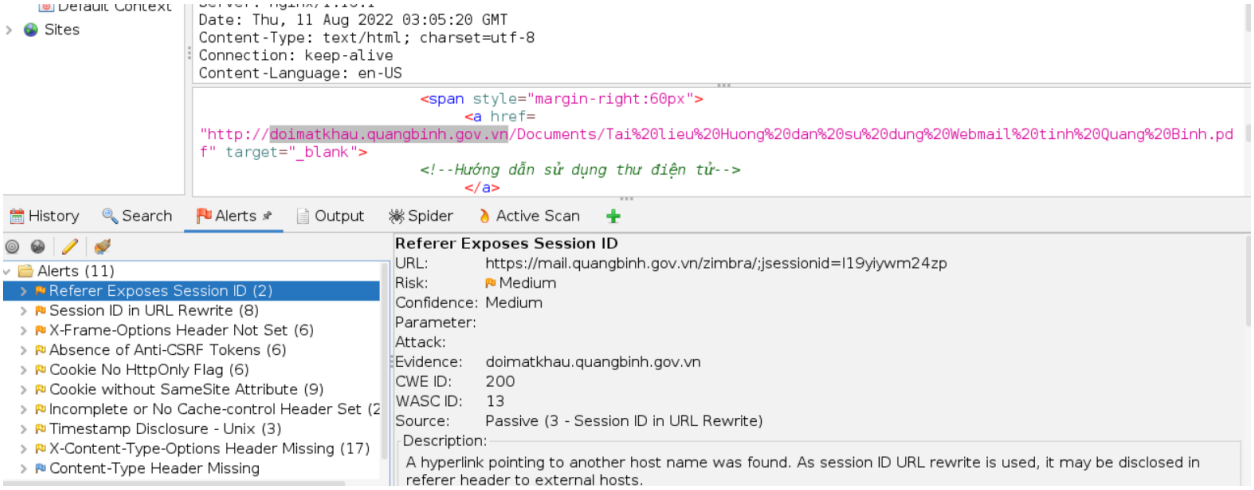

Zap sẽ scan tự động website mà bạn đã nhập và show các report các lỗ hỏng tìm được ở Tab Alert. Các báo cáo được thể hiện theo từng loại lỗi

hỏng và show số lượng lỗi tìm được của từng lỗ hỏng và URL tìm ra nó. Các loại warming sẽ khác nhau tùy thuộc vào trang web của bạn, ví dụ như:

1. X-Frame-Options Header Scanner
2. Session ID in URL Rewrite
3. Cookie Without Secure Flag
4. Private IP Disclosure

***Bước 4:***

Bạn có thể xem các thông tin chi tiết của lỗ hỏng bằng cách click vào một lỗ hỏng bất kỳ từ tab Alert. Các dòng code gây ra lỗi sẽ được highlight như ảnh dưới đây




*Ngoài ra, bạn có thể tìm được giải pháp được suggest ở mục Solution, thông tin lỗ hỏng ở Description và thông tin tham khảo ở Reference*