

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 hàng 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 hổng 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 tra các thông điệp được gửi đi, sửa đổi và gửi tiếp các thông điệp đó đến đích.

Các tính năng cơ bản của ZAP:

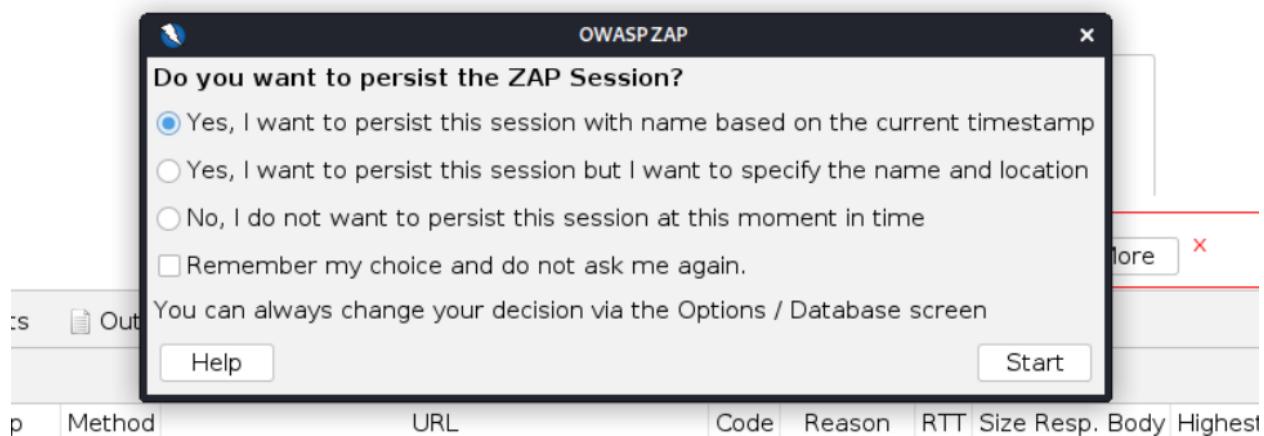
- Intercepting Proxy
- Traditional and AJAX spiders
- Automated scanner
- Passive scanner
- Forced browsing
- Fuzzer
- Dynamic SSL certificates
- Smartcard and Client Digital Certificates support
- Web sockets support
- Support for a wide range of scripting languages
- Plug-n-Hack support
- Authentication 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:

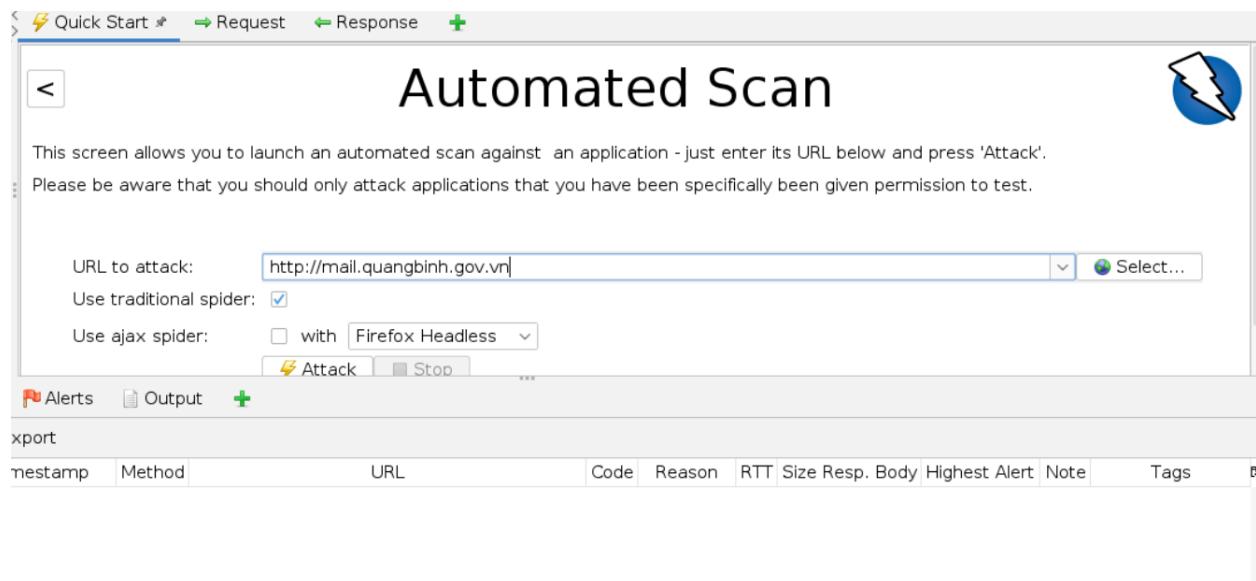
Khi open App bạn sẽ được lựa chọn có lưu giữ lại Session hay không. Theo mặc định, ZAP session sẽ được ghi vào đĩa ở HSQLDB với tên và location mặc định. Nếu bạn lựa chọn không duy trì session, các tệp được ghi sẽ được xóa khi thoát ZAP. Nếu bạn duy trì session, thông tin sẽ được ghi lại, bạn sẽ có thể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

an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
are new to ZAP then it is best to start with one of the options below.



Bước 2:

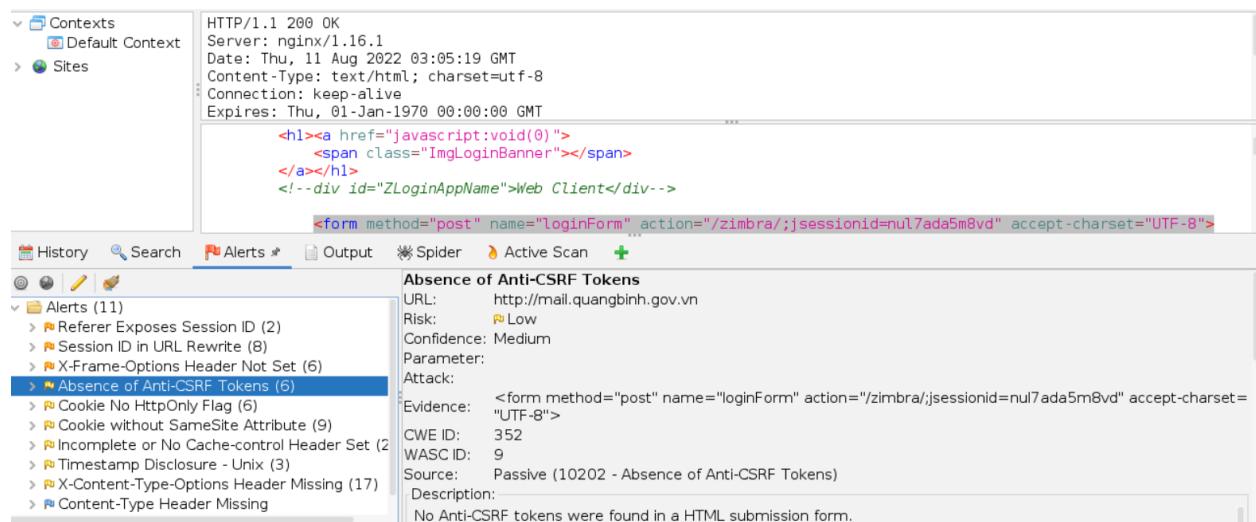
Nhập URL của website mà bạn muốn check vào field URL to attack



The screenshot shows the ZAP (Zed Attack Proxy) interface in 'Automated Scan' mode. The 'URL to attack' field contains 'http://mail.quangbinh.gov.vn'. Below it, there are options for 'Use traditional spider:' (checked) and 'Use ajax spider:' (unchecked). A large blue 'Attack' button is prominently displayed. The interface includes tabs for 'Alerts' and 'Output'.

Bước 3:

Click Attack button



The screenshot shows the ZAP interface with the 'Alerts' tab selected. It displays a list of findings under the 'Absence of Anti-CSRF Tokens' category. The findings include:

- Referer Exposes Session ID (2)
- Session ID in URL Rewrite (8)
- X-Frame-Options Header Not Set (6)
- Absence of Anti-CSRF Tokens (6)
- Cookie No HttpOnly Flag (6)
- Cookie without SameSite Attribute (9)
- Incomplete or No Cache-control Header Set (2)
- Timestamp Disclosure - Unix (3)
- X-Content-Type-Options Header Missing (17)
- Content-Type Header Missing

Each finding includes details like URL, Risk level (Low), Confidence, Parameter, and CWE/WASC IDs.

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

hỗng và show số lượng lỗi tìm được của từng lỗ hổng 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 hổng bằng cách click vào một lỗ hổng bất kỳ từ tab Alert. Các dòng code gây ra lỗi sẽ được highlight như ảnh dưới đây

The screenshot shows a web-based security tool interface. At the top, there's a header with 'Default Context' and 'SITES'. Below it, a sidebar on the left lists 'History', 'Search', 'Alerts (11)', and 'Output'. The 'Alerts' section is expanded, showing a list of findings under 'Referer Exposes Session ID (2)'. The first item in this list is selected. The main pane displays the following details:

```
Date: Thu, 11 Aug 2022 03:05:20 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Language: en-US



<!--Hướng dẫn sử dụng thư điện tử-->


```

Below this, a detailed description of the issue is provided:

Referer Exposes Session ID

URL:	https://mail.quangbinh.gov.vn/zimbra/:jsessionid=19iywm24zp
Risk:	Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	doimatkhau.quangbinh.gov.vn
CWE ID:	200
WASC ID:	13
Source:	Passive (3 - Session ID in URL Rewrite)
Description:	A hyperlink pointing to another host name was found. As session ID URL rewrite is used, it may be disclosed in referer header to external hosts.

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