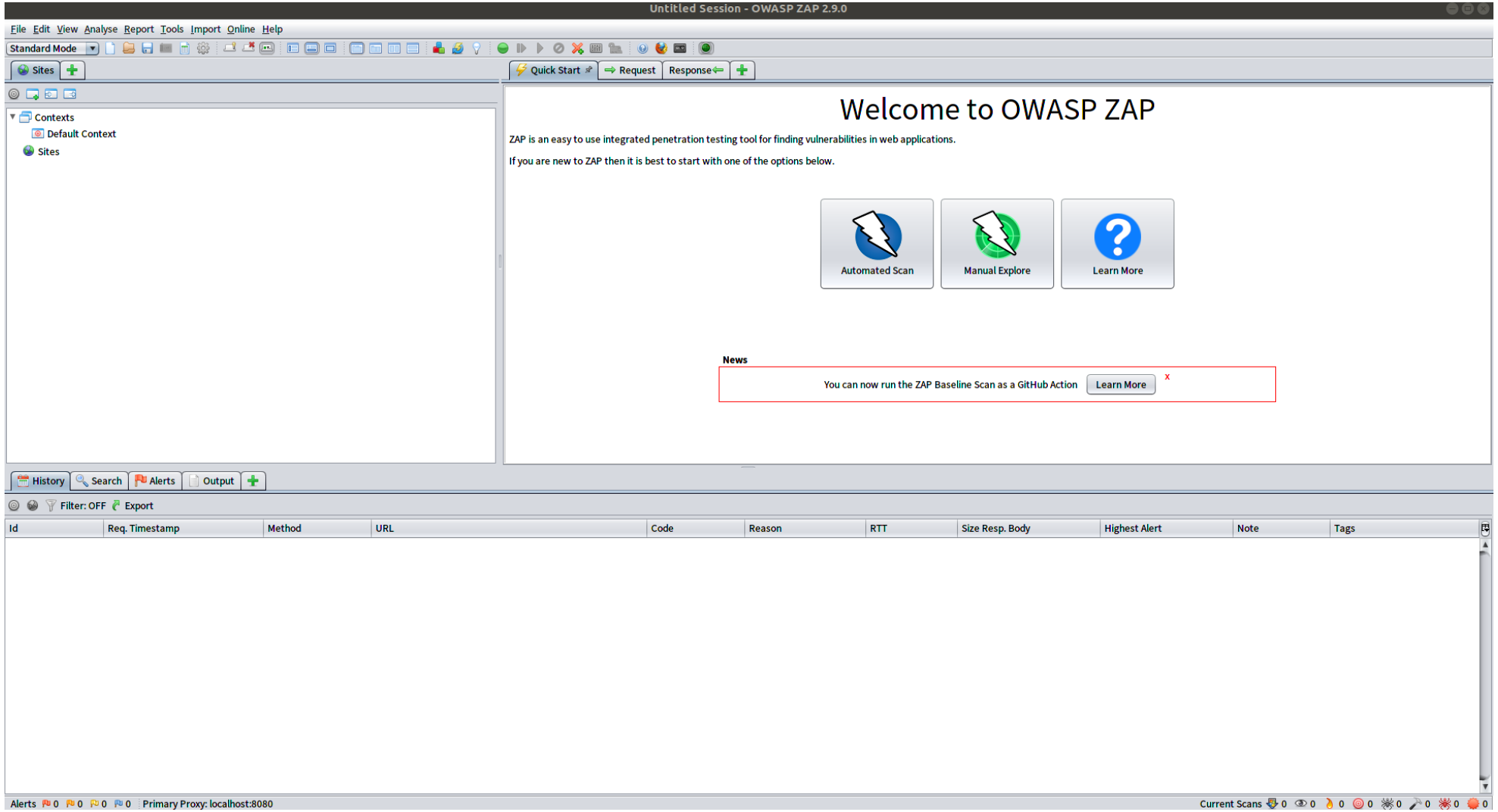
蘭陽女中 網頁檢測工具簡介

2020. 08. 19

OWASP ZAP

- OWASP Zed Attack Proxy(ZAP)
  - OWASP(Open Web Application Security Project)
    - 開放社群、非營利性組織
    - OWASP 2017 TOP 10
      - 「行政院國家資通安全會報技術服務中心」說明文件
- 圖形化的網頁漏洞測試工具
  - 免費且跨平台
  - 自動化攻擊
  - 網頁爬蟲
  - 弱點報告

OWASP ZAP


Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
Welcome to OWASP ZAP
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.
Automated Scan
Manual Explore
Learn More
News
You can now run the ZAP Baseline Scan as a GitHub Action
Learn More
History
Search
Alerts
Output
Filter: OFF
Export
Id
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Alerts
Primary Proxy: localhost:8080
Current Scans

- 測試網站
  - http://120.101.173.14
  - http://lisc.lygsh.ilc.edu.tw
  - http://120.101.173.250/
  - Webgoat
    - OWASP提供的弱點測試網站

Nmap

- Nmap
  - 圖型化的漏洞檢測或掃描的工具
  - 免費且跨平台
- 功能
  - 發現主機
  - 掃描 Port
  - 偵測應用程式或作業系統版本
  - NSE指令碼

Nmap

- 使用方式(指令)
  - nmap
    - -sS : 透過 TCP SYN 的方式偵測port是否開啟
    - -sU : 偵測udp Port是否開啟
    - -sV : 偵測已開啟 port 的服務或版本
    - -Pn : 直接掃描範圍內的主機
    - -p : 指定要掃描的 port
    - -O : 偵測作業系統版本
    - --script : 使用 NSE 指令碼
    - -A : 偵測作業系統, 應用程式版本..等

Nmap

- 使用方式(指令)
  - nmap 120.101.173.1/24
    - 掃描主機上預設的1000個 port
  - nmap -p 80,443,3389 120.101.173.1/24
    - 掃描主機上是否開啟 80,443,3389 的 port
  - nmap -p 80,443,3389 120.101.173.1/24 -O
    - 掃描主機上開啟 80,443,3389 的 port，且偵測主機的作業系統
  - nmap -p 80,443,3389 120.101.173.1/24 -sV
    - 掃描主機上開啟 80,443,3389 的 port，且偵測應用程式的版本

Nmap

- 使用方式(指令)
  - nmap 120.101.173.1/24 --script vuln
    - 依現有的 script 腳本測試主機的安全性
  - nmap -script http-methods 120.101.173.3
    - 偵測網站主機開啟的 methods