SER421 Lab Security Fall 2023 Session A

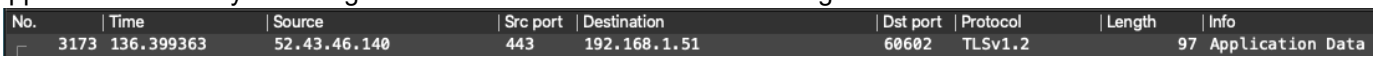
Background:
Security is a huge area of software engineering nowadays, and the web is the primary way we use software. This lab has you inspect security-related aspects of the web, specifically key exchange in HTTPS and an XSS attack.

This lab has been verified with Wireshark v4.0.8 (Activity 1), ZAP 2.13, Java 17, and Maven 3.3.1 (Activity 2).

Objectives:
S1. Understand what an HTTPS exchange looks like at the network transport level.
S2. Apply a pen test tool to discover, and then fix, XSS vulnerabilities

Activity 1: Sniff HTTPS traffic looking for key exchanges (22 points)
Setup:

1. You will need to download *Wireshark*, a network packet sniffing utility.
2. Bring up wireshark, and start a capture on the loopback interface (lo0). In the *display* filter line, specify the filter string: tcp.port==8443 and tcp and not tcp.len==0
3. Make sure you can see columns "No." "Time" "Source" "Src port" "Destination" "Dest port" "Protocol" "Length" and "Application Data". If you can't go into Wireshark Preferences and configure.



No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
3173	136.399363	52.43.46.140	443	192.168.1.51	60602	TLSv1.2	97	Application Data

4. Locally, run the https_echo server you can download on the assignment page. You will need Node and the command-line is all, unzip the download in an empty directory, and type in "node https_echo.js"

USE ONLY FIREFOX FOR THIS ACTIVITY!

Steps:
S1. Make sure you have Wireshark open and listening on lo0 using the display filter given above.
S2. Open Firefox and ensure you have only one tab open. Access https://localhost:8443. You will get a one-line textbox; type in anything and hit return.
S3. In Wireshark, you should have seen some packet traffic. With that traffic, do the following:
   a. (4)Provide screen captures of each of the handshake packets, and indicate what step in the handshake is going on
   b. (4)Identify the set of cipher suites (screenshot) available in the browser, and the one selected by the server.
   c. (4)Identify the client Random and the server Random in the given packets
S4. View the digital certificate for the application within Firefox (click on the lock symbol in the address bar)
   a. (5)What is the Subject and Issuer Name? What is the Validity and Public Key Info? Provide a screen capture.
   b. (5)Why is the certificate not trusted by the browser?

Submission: Create a Word document named *ser421_labsecurity_<asurite>.docx* that includes all the screenshots and answers/explanations asked for in the task description under a section named "Activity 1". *I have underlined each place where this is asked for. Clearly label the step number, and provide a complete answer to what is asked for.*

Notes:
- You should be using at least Wireshark version 3.6.8 (Mac/Windows/Linux), latest verified is v4.0.8.
- Do not confuse *display* filter in Wireshark with *capture* filter. We are only using display filters in this lab.
- It will be easier to ascertain traffic in Wireshark if you close every non-essential application on your machine. You would be surprised how many applications are constantly sending network packets in the background. Even MS-Word sends data over SSL to its remote APIs (the world is tracking you…).

Activity 2: Find, document and eliminate XSS vulnerabilities (18 points)
S1. For this activity you need to download and install these tools in order to launch the server and test:
   a. JDK 17
   b. Maven 3.3.1 or better
   c. ZAP 2.08 (latest verified 2.13)

S2. Download the activity2.zip file from Canvas and unzip in a clean directory. It should create a subfolder xss. From the command-line/terminal, cd into *xss/lab/patchxss.* (please note: the location is relative to where you cloned the repository on your system) and run the server under the repository directory (**mvn spring-boot:run**):

S3. Visit the following URL in your browser: http://localhost:8082/xss.html

S4. (4) Identify the type of XSS vulnerabilities/attack found against this URL using the ZAP tool. Follow the steps at the end of this specification to understand how to run ZAP for this activity and generate a report. Name the report ser421_act2ZAPinitial_<asurite>.pdf. Please be sure to start a new ZAP session for the URL in step S3.

S5. In your *ser421_labsecurity_<asurite>.docx* file, in a section clearly marked "Activity 2", describe the vulnerability details which must include:

   a. (2) Full URL
   b. (2) Type of XSS Attack/Vulnerability
   c. (4) Steps to exploit the XSS vulnerabilities with respect to this webpage
   d. (6) The CWE number (you will find it in the PDF report or the Alerts description for the High vulnerability in ZAP). Follow the web link to the CWE website and give its Title, [short] Description, Likelihood of Exploit. Review the "Potential Mitigations" section of the CWE page and choose the one that you feel would be most useful for preventing the kind of defect this example injects, and say why.

You are not required to correct the vulnerability, but I suggest you try to in order to cement your understanding of what is going on.

Overall, your submission for activity 2 must include these files:

1. ZAP generated PDF report (step S4)
2. Updated *ser421_labsecurity_<asurite>.docx. Clearly label the step number, and provide a complete answer to what is asked for.*

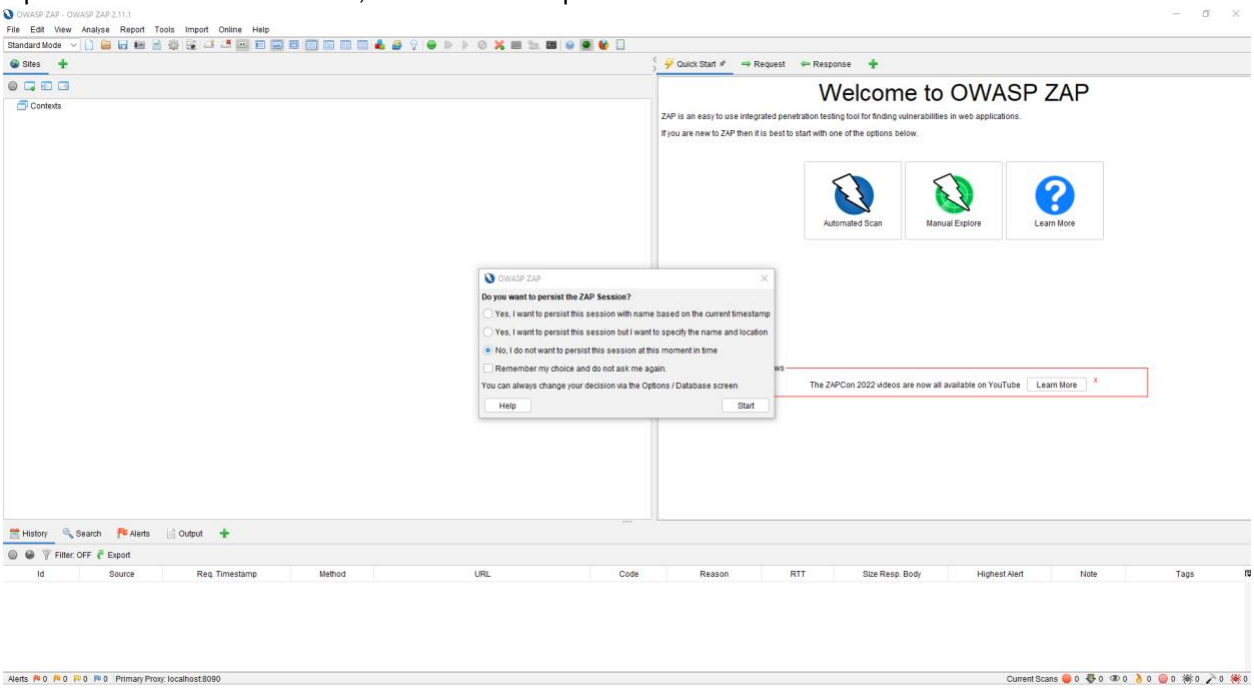
Your full submission is Word docx file, plus the ZAP report PDF. Please combine the files in a submission zip named ser*421_labsecurity_<asurite>.zip* and submit on Canvas.

Then go rejoice because your labs for this class are OVER!!!

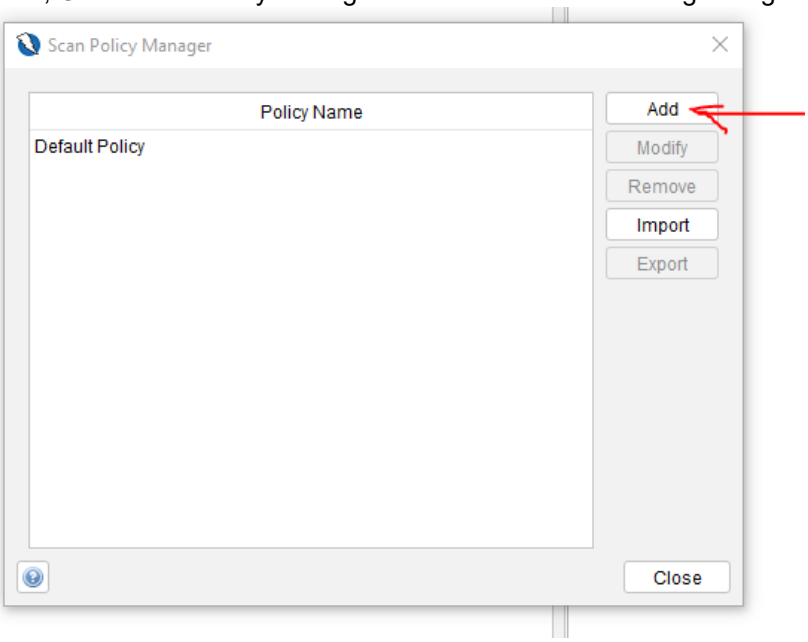
How to configure and run the OWASP ZAP tool

The OWASP ZAP tool may be downloaded from https://owasp.org/www-project-zap/

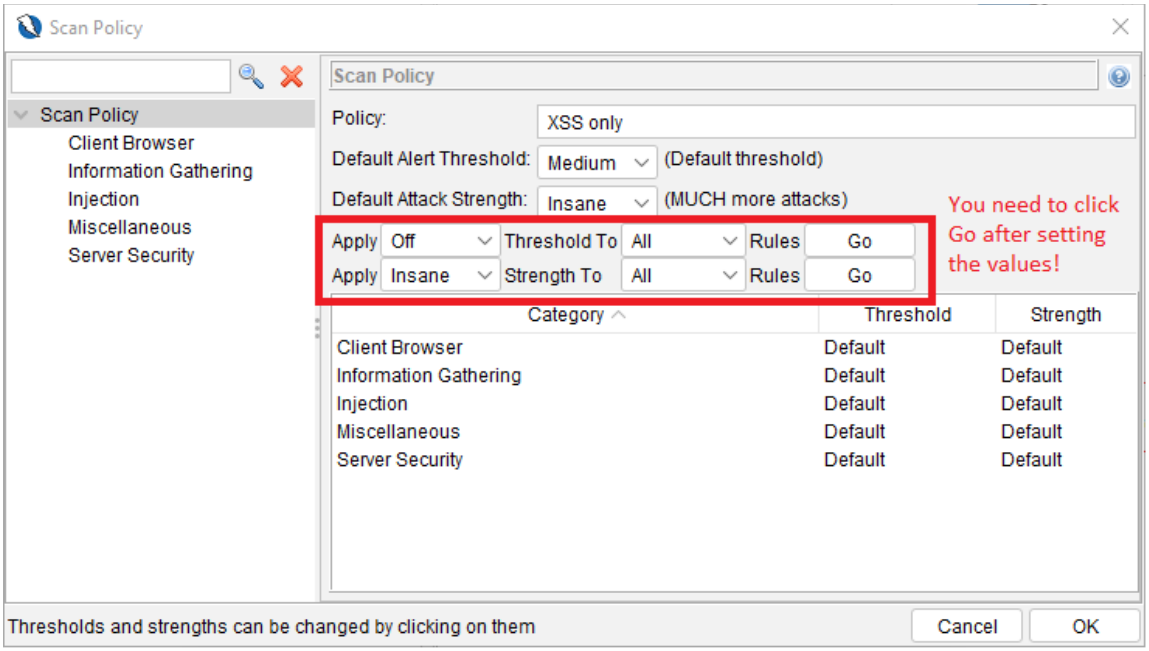
1. Open the ZAP tool. Select 'No, I do not want to persist this session at this moment in time'



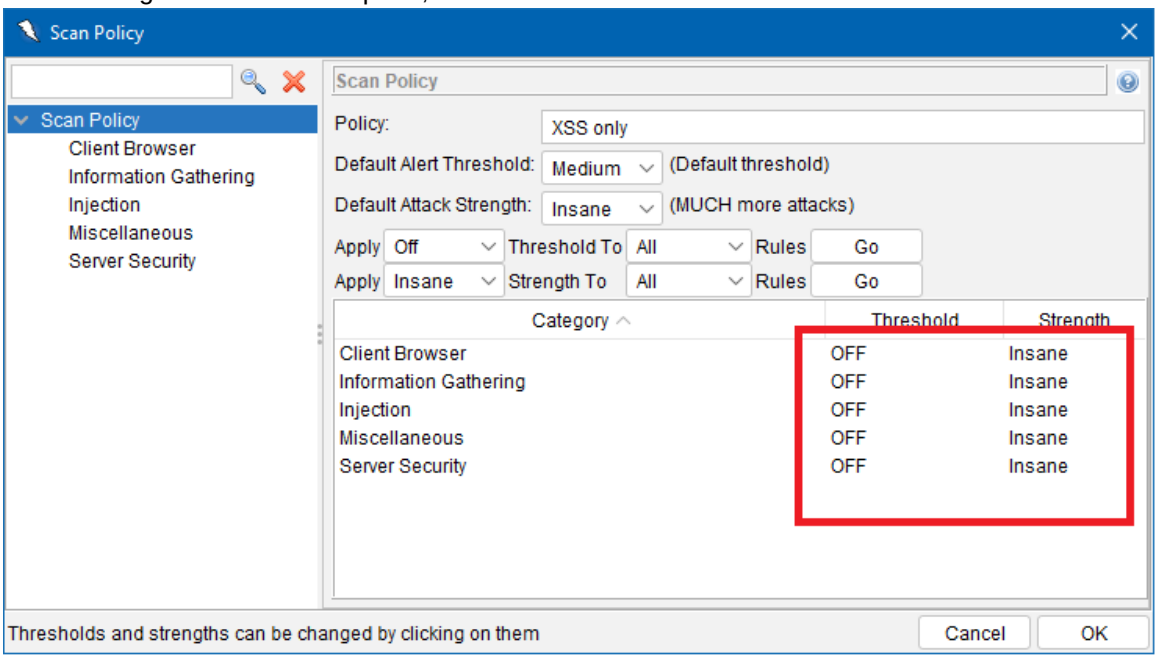
2. Since we are mainly interested in finding XSS vulnerabilities, we need to configure 'Scan Policy'. Click on 'Analyse' menu. Under the drop-down, Click 'Scan Policy Manager'. You should see following dialog box. Click on 'Add'



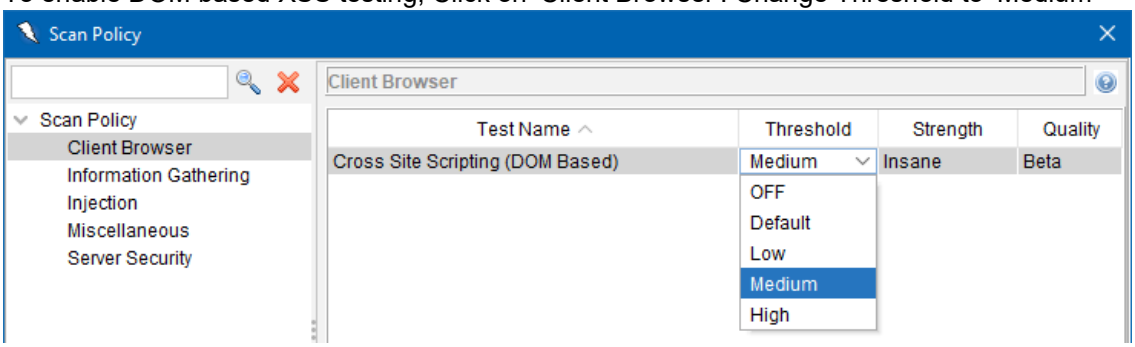
3. This is a multi-step process: (**PLEASE DO NOT CLICK 'OK' UNTIL STEP 3.h**)
    a. Type in Policy Name: 'XSS only'
    b. Set Default Alert Threshold to 'Medium'
    c. Set Default Attack Strength to 'Insane'
    d. Apply 'Off' Threshold to 'All' Rules and Click Go
    e. Apply 'Insane' Strength to 'All' Rules and Click Go



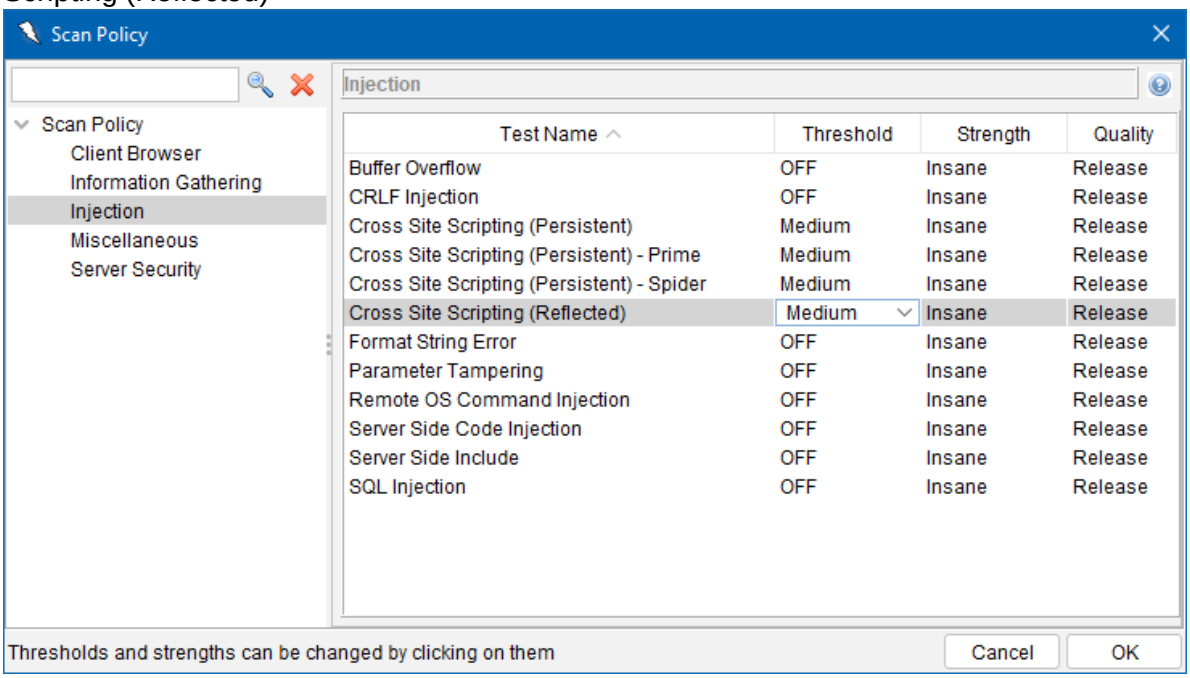
After clicking Go buttons in step 3.e, it should look like this:



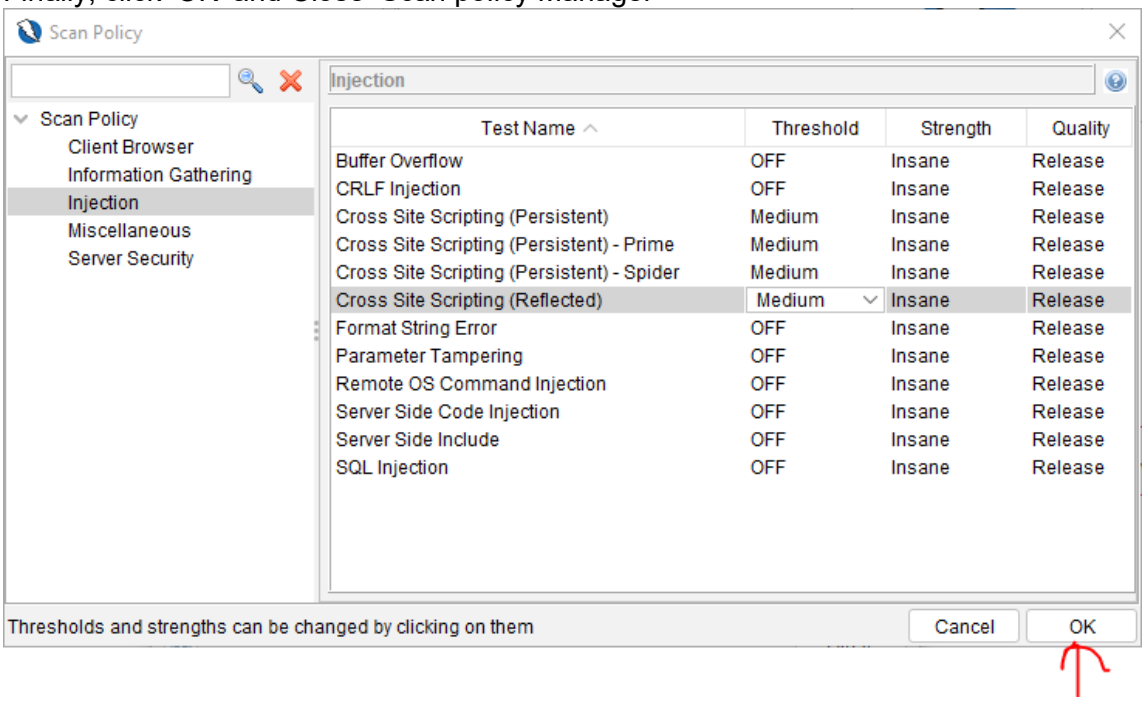
f. To enable DOM based XSS testing, Click on ‘Client Browser’. Change Threshold to ‘Medium’



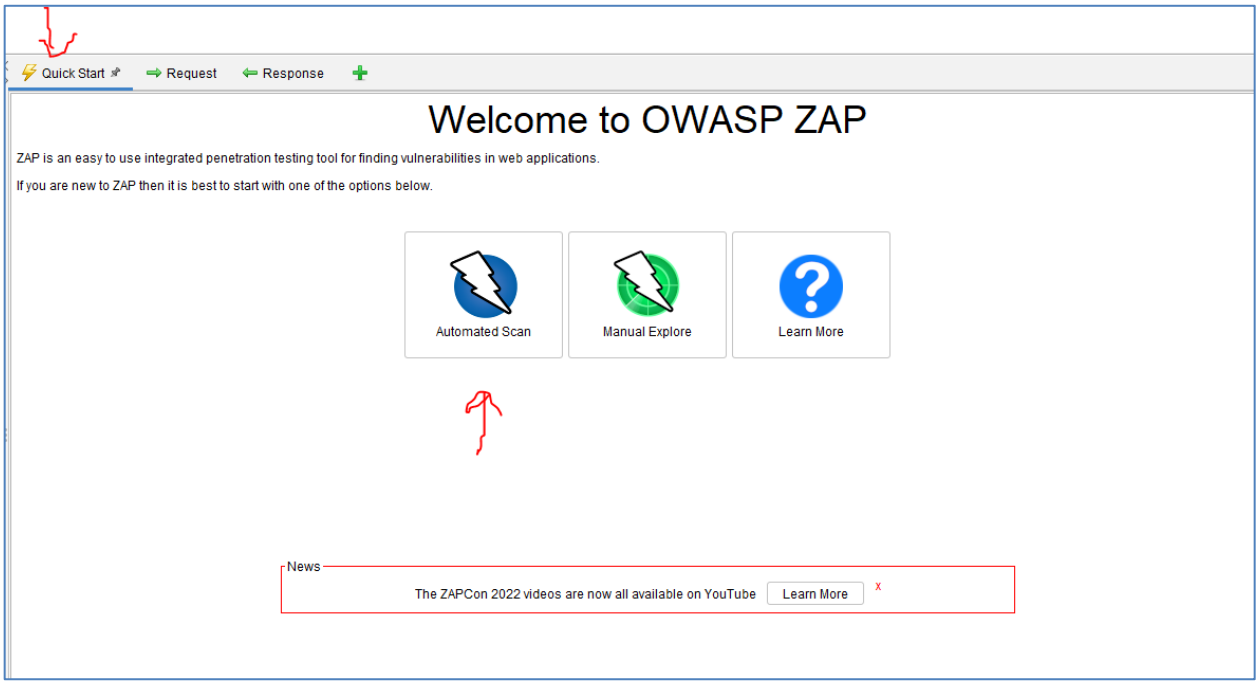
g. To enable Reflected XSS and Stored/Persistent XSS vulnerability testing: Click on Injection. Change the thresholds to ‘Medium’ for all 4: Cross Site Scripting (Persistent), Cross Site Scripting (Persistent) – Prime, Cross Site Scripting (Persistent) – Spider and Cross Site Scripting (Reflected)



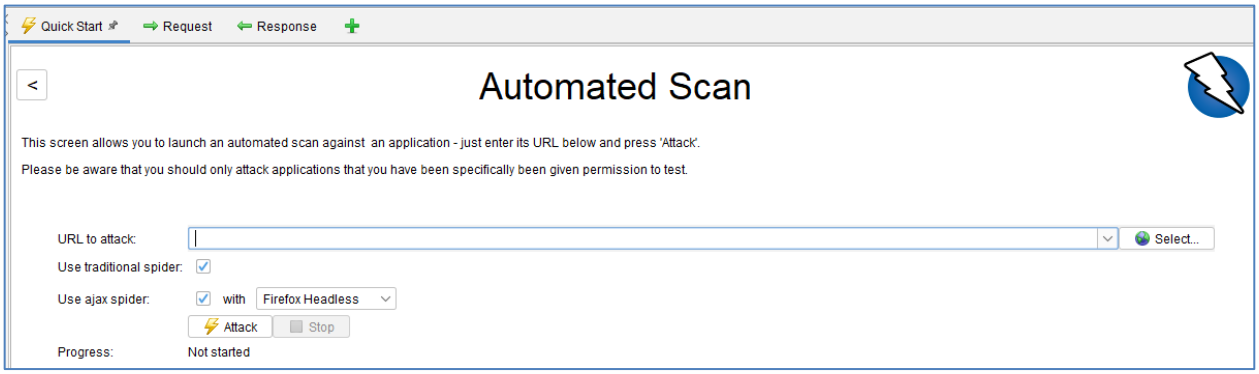
h. Finally, click ‘OK’ and Close ‘Scan policy Manager’



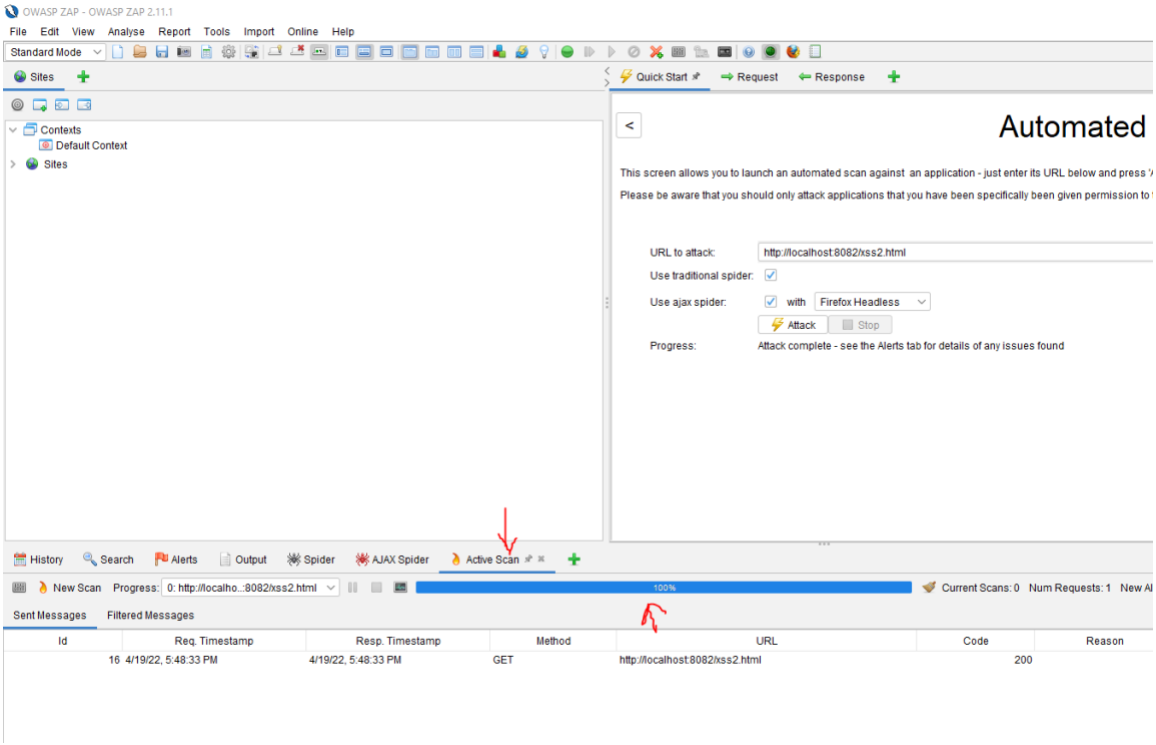
4. Under ‘Quick Start’ click ‘Automated Scan’:



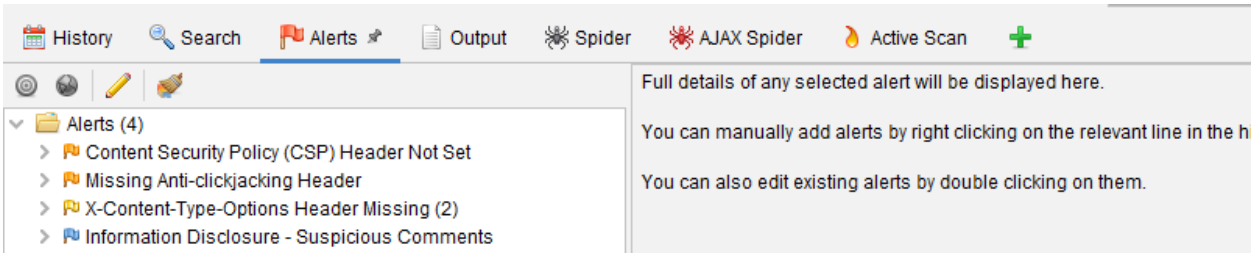
5. Type ‘URL to attack’: http://localhost:8082/xss.html. Select ‘Use traditional spider’, ‘Use ajax spider’. Please ONLY use headless browser versions (Chrome Headless or Firefox Headless)



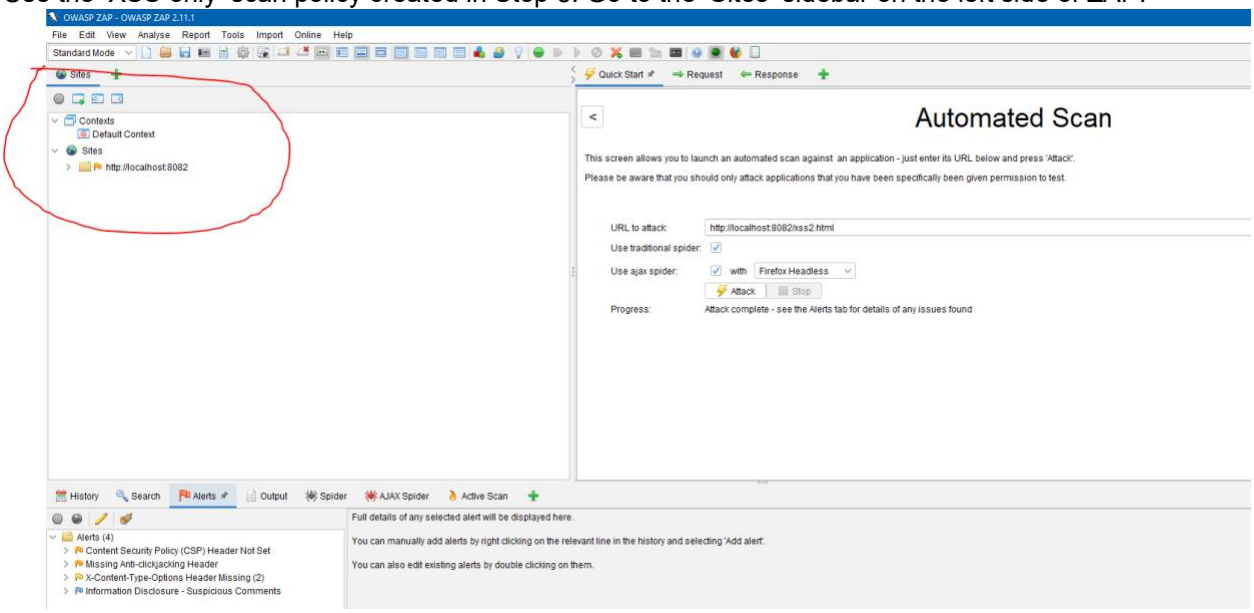
6. Click on ‘Attack’ and let ZAP tool finish the scan. To see the scanning progress, click on ‘Active Scan’



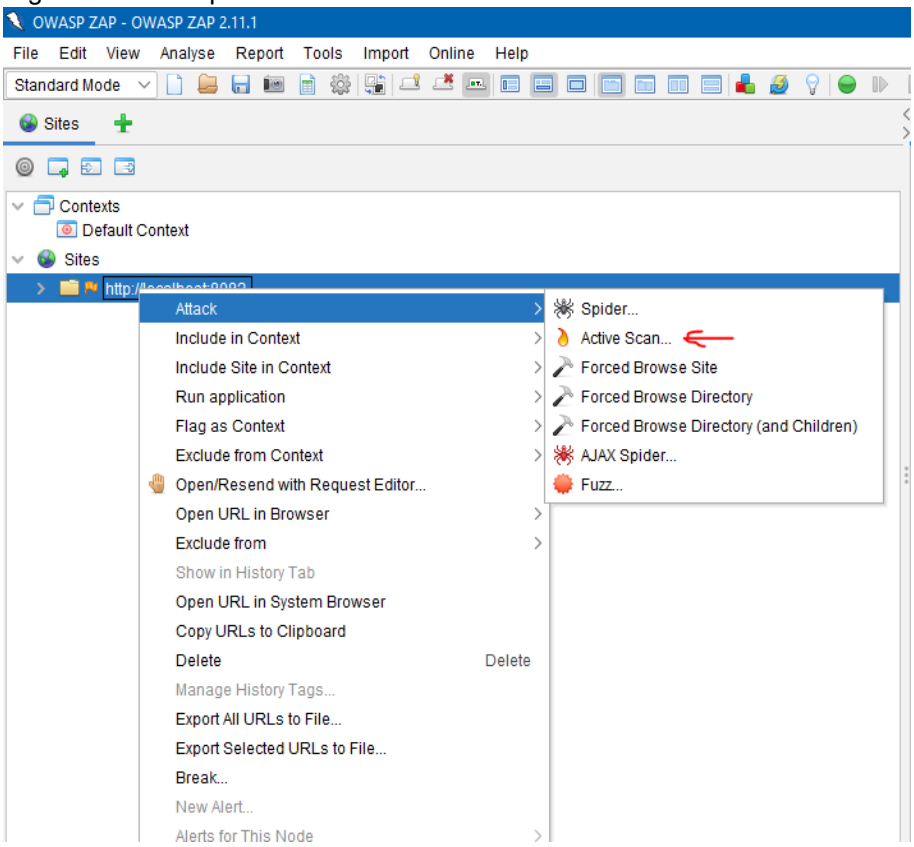
7. Check ‘Alerts’ tab for reported issues. If you do not see XSS vulnerabilities here, relax; it’s expected because we only created a new scan policy, but the scanner did not use it when we first ran the ‘Automated scan’ on the URL.



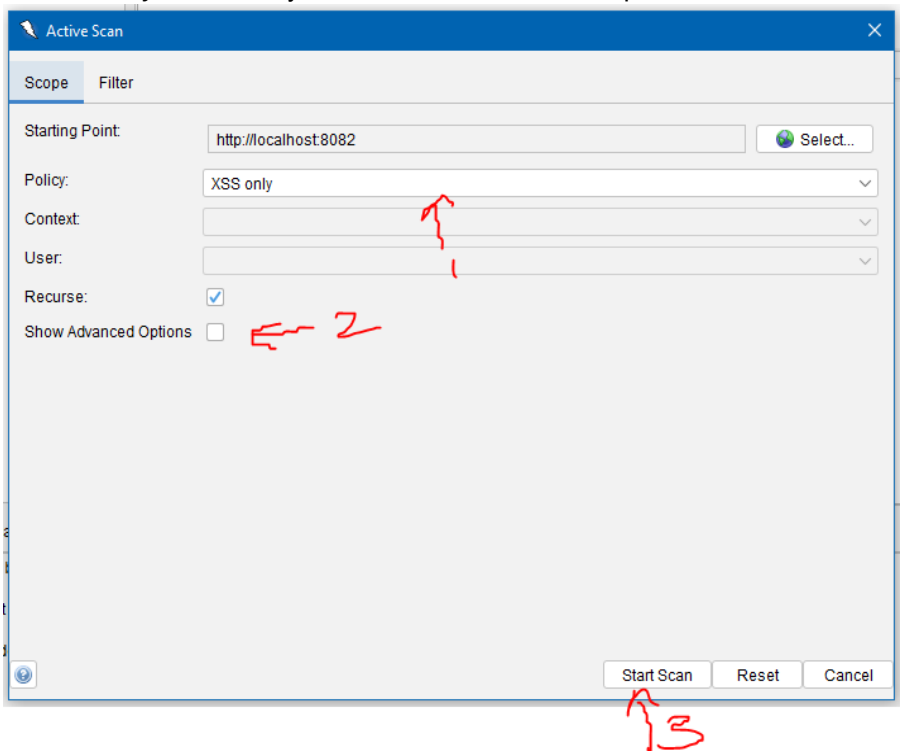
8. Use the ‘XSS only’ scan policy created in Step 3. Go to the ‘Sites’ sidebar on the left side of ZAP:



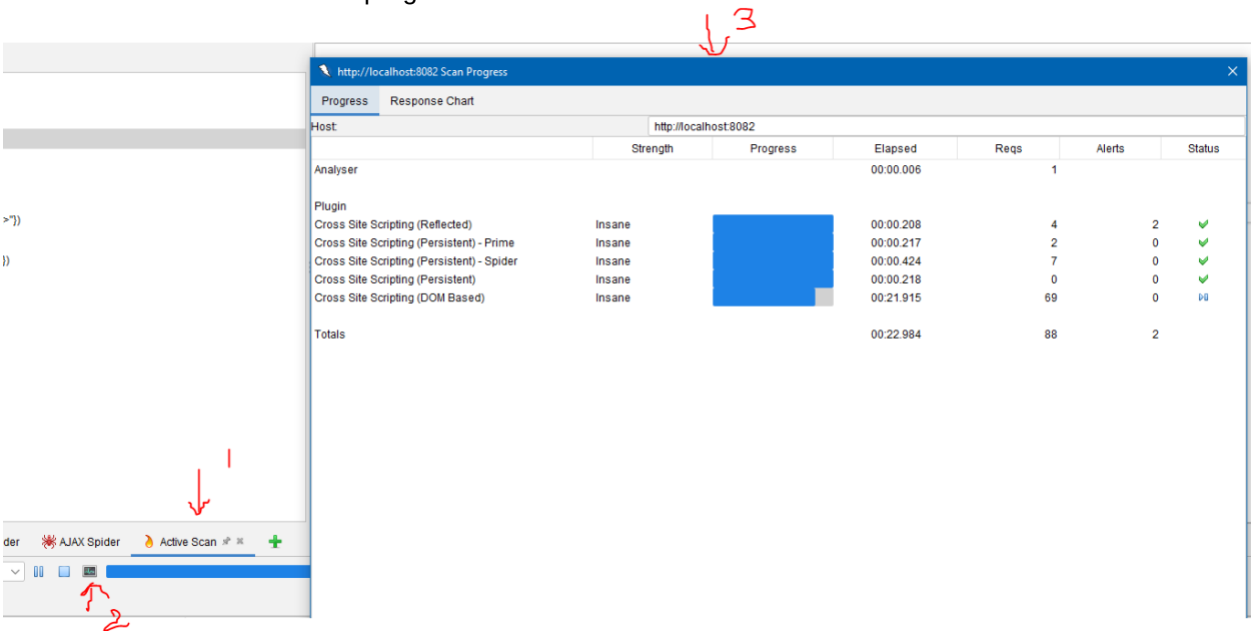
9. Right Click on ‘http://localhost:8082’ under ‘Sites’ tree. Click ‘Attack’ and Click ‘Active Scan…’



10. Select Policy – ‘XSS only’; Untick ‘Show Advanced options’ if selected and Check ‘Recurse’. Click ‘Start Scan’



11. Wait for the scanner to finish. You can monitor the progress of the running tests by clicking on ‘Active scan’ and click on Monitor icon to view a progress window:



When the scan complete you should see the XSS vulnerabilities detected under the Alerts Tab!

12. To generate a PDF report, click on ‘Report’ menu and click ‘Generate Report’