Unauthenticated Scan

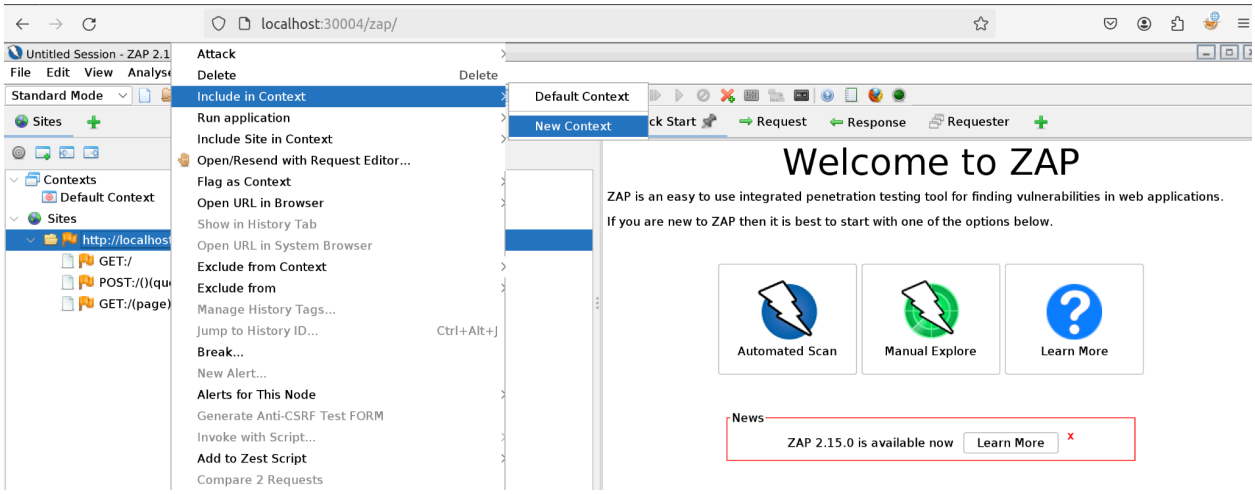
In ZAP, we have contexts and Sites.

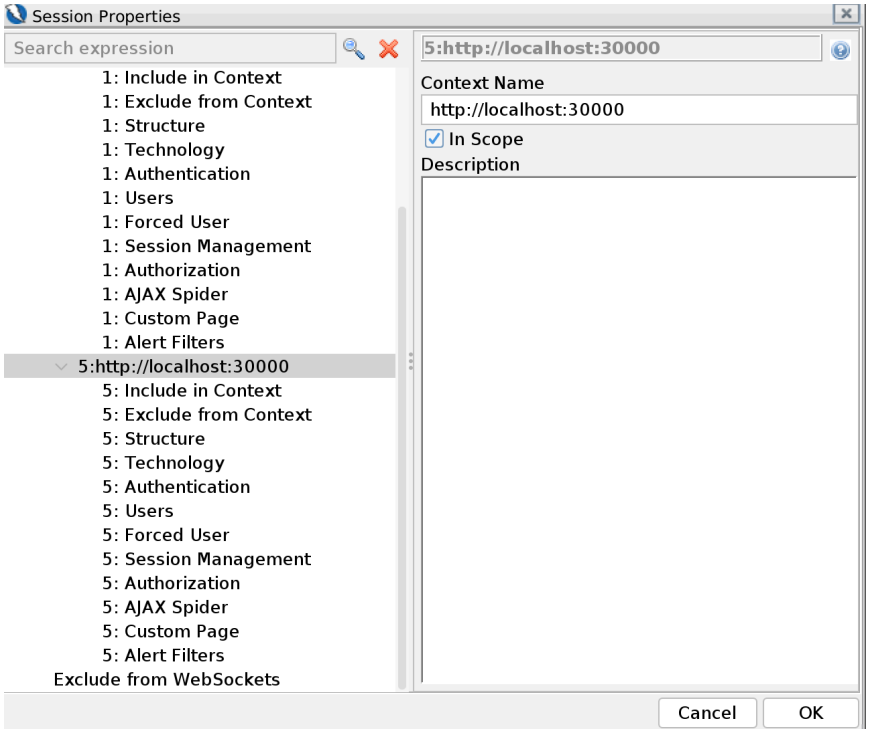
The Sites tree displays the structure of the websites you are testing. It shows all the discovered URLs, directories, and files within the target web applications, helping you navigate and analyze the components of the sites you are evaluating.

A context, on the other hand, is a way to group together a set of related URLs and define a scope for testing (particularly useful in a very large website), including specific rules, authentication settings, and user permissions. It allows you to manage and organize your testing environment effectively.

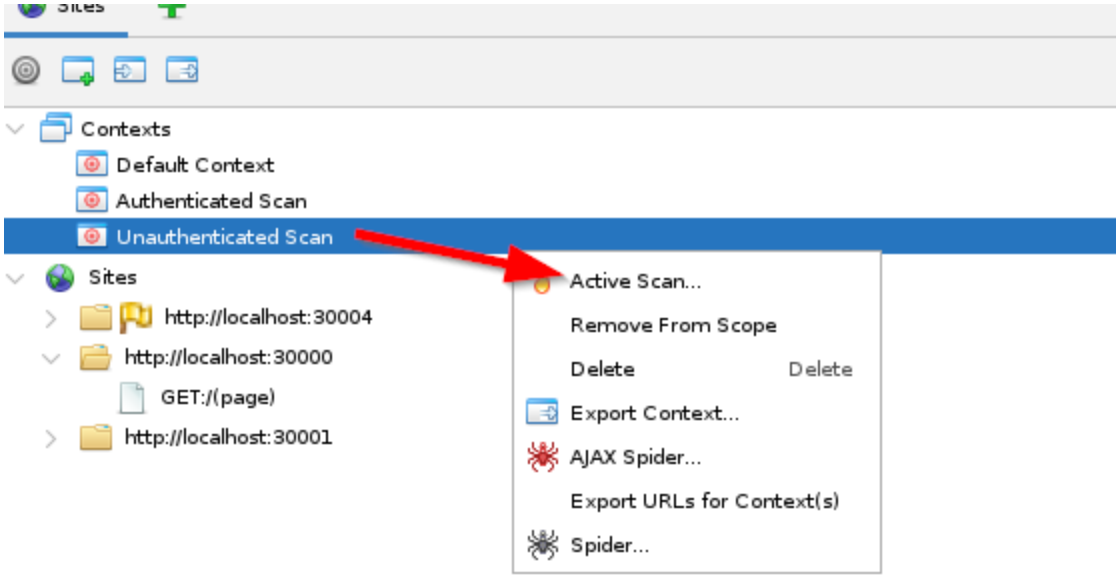
We will make use of these both for active scans.

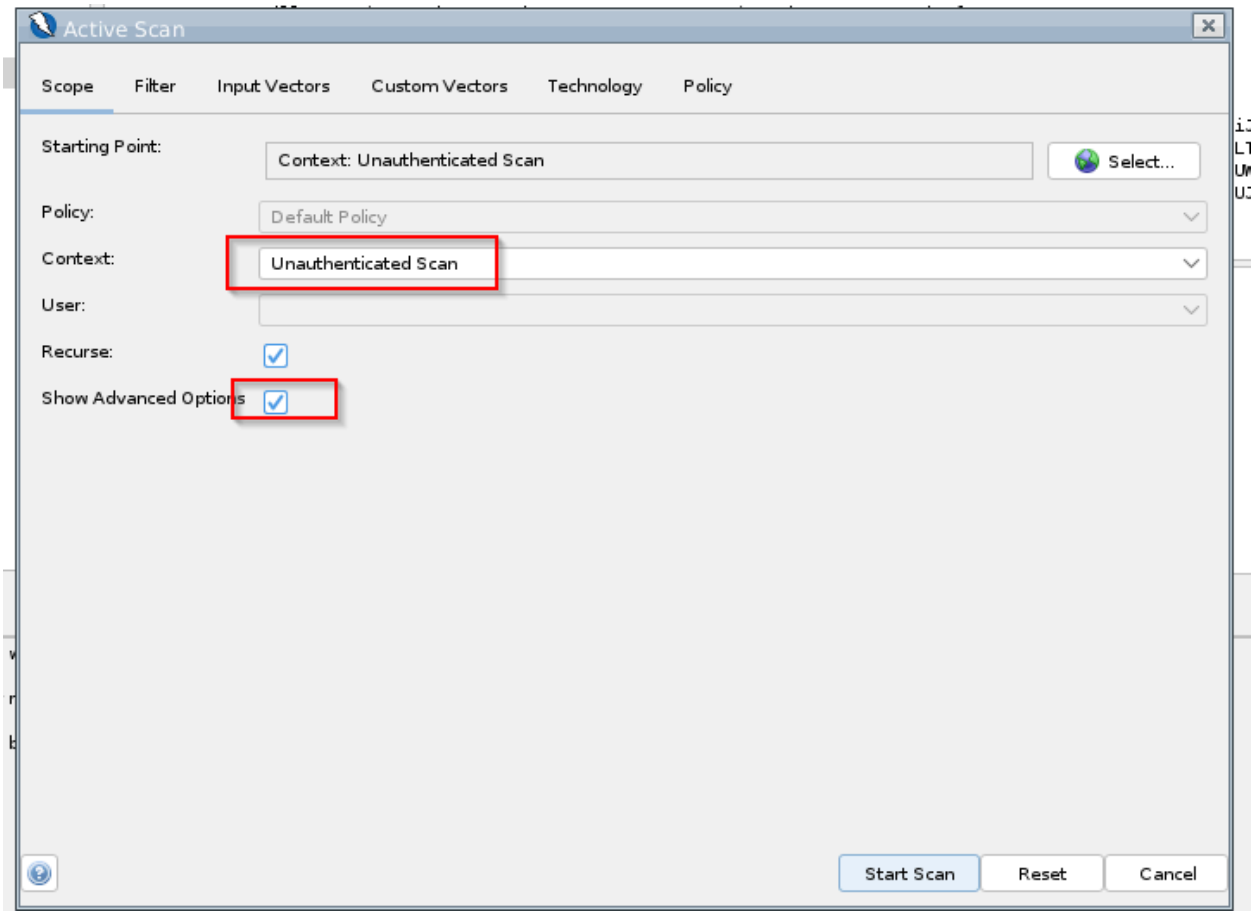
- Ensure FoxyProxy is disabled first. This is important, since without ZAP running, it won't know where to forward traffic
- Then visit http://localhost:30004/zap/ (this can take a few minutes), followed by http://localhost:30000/
- Then in ZAP, ensure HUD is disabled and also enable FoxyProxy now with the right pattern to forward the traffic of http://localhost:30000/ to ZAP (as covered in activity 1)
- If you specify a URL, normally ZAP can scan through the website via spidering. However automated scan for vulnerabilities post this, may not work well. Manual navigation in ZAP is often necessary due to missing dynamic paths, multi-step processes, and stateful pages. Manual interaction also can uncover content generated by JavaScript or AJAX calls. Manual input is also needed for fields where SQL injection and XSS vulnerabilities often reside. So, to be thorough, navigate through http://localhost:30000/ thoroughly. Be sure to enter values where possible. Post this you will see the URLs visited under Sites.
- Include the website under a new context to start a scan by following the below screenshots (right click as needed). If you wish to change the name of the context, once http://localhost:30000/ appears under context after the above step, double click it and change the name, see the session properties screenshot. (Assume we named it Unauthenticated Scan)

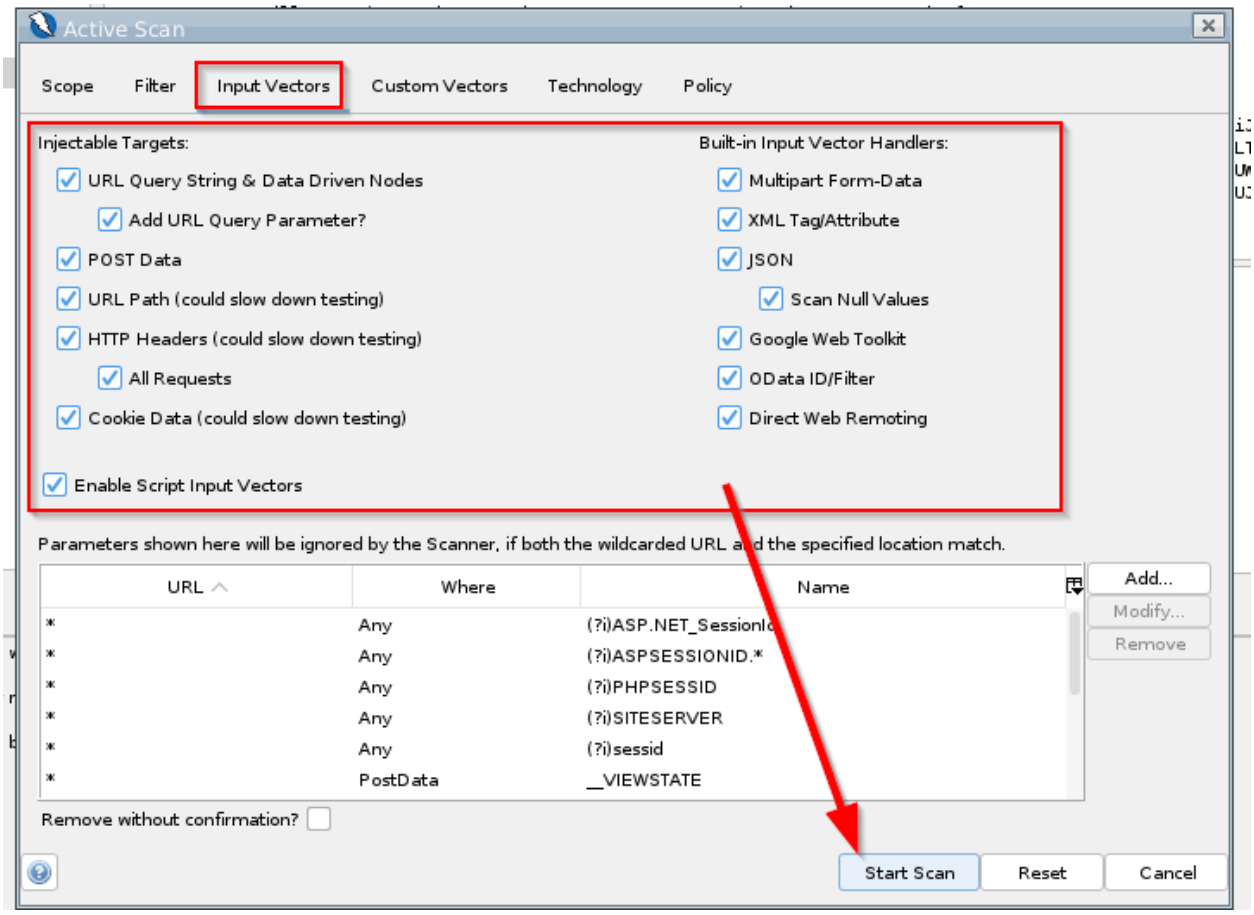




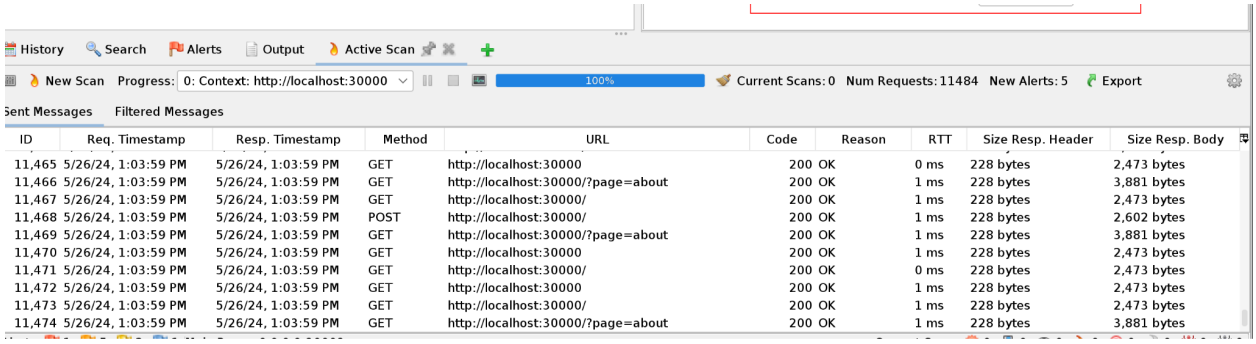
- Then right click on Unauthenticated Scan in Context, and so an active scan. See below. Select Show Advanced options, click on Input vectors, select all and start scan.


Contexts
Default Context
Authenticated Scan
Unauthenticated Scan
Sites
http://localhost:30004
http://localhost:30000
GET:/(page)
http://localhost:30001
Active Scan...
Remove From Scope
Delete
Delete
Export Context...
AJAX Spider...
Export URLs for Context(s)
Spider...

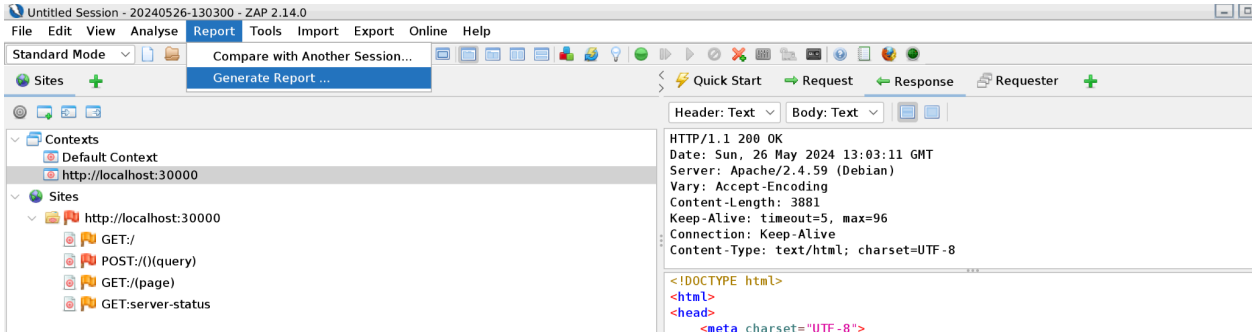

Active Scan
Scope
Filter
Input Vectors
Custom Vectors
Technology
Policy
Starting Point:
Context: Unauthenticated Scan
Select...
Policy:
Default Policy
Context:
Unauthenticated Scan
User:
Recurse:
Show Advanced Options
Start Scan
Reset
Cancel

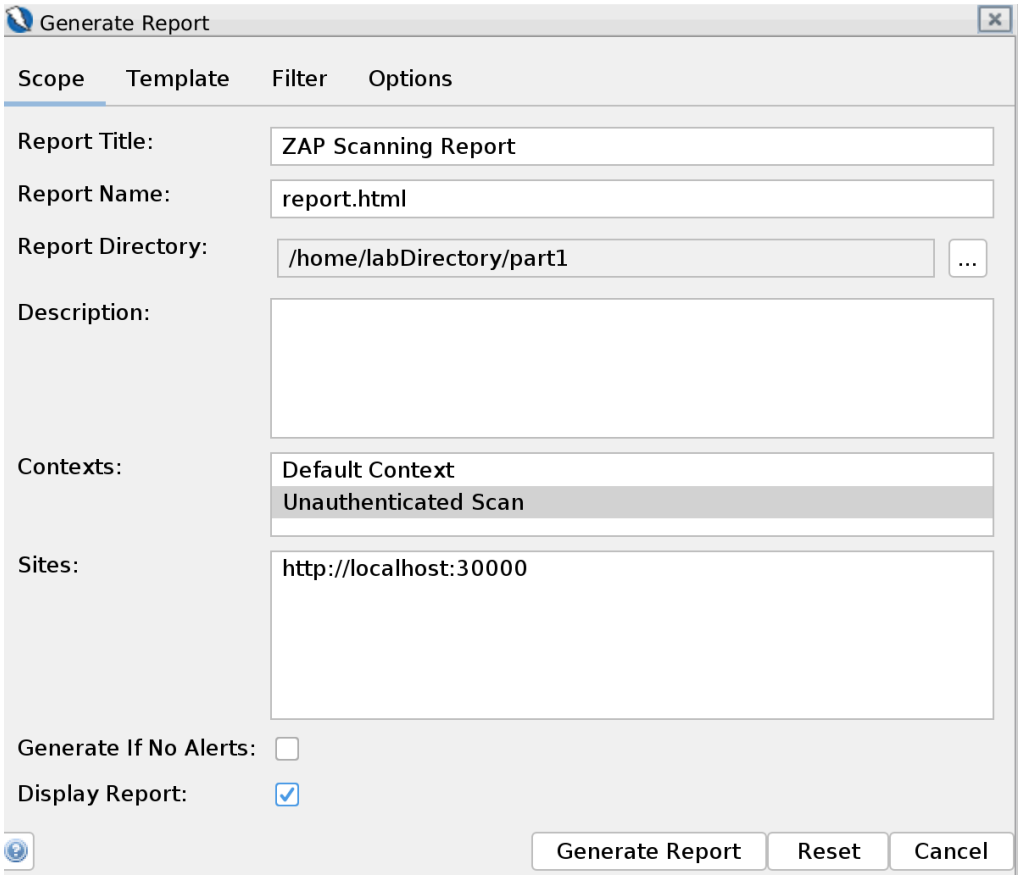


- When the scan runs, you will see something like this. Notice the progress bar. Once it hits 100%, click on Alerts to see what all vulnerabilities it found. Go through each Alert (drop down, and single click items) and see what it says.



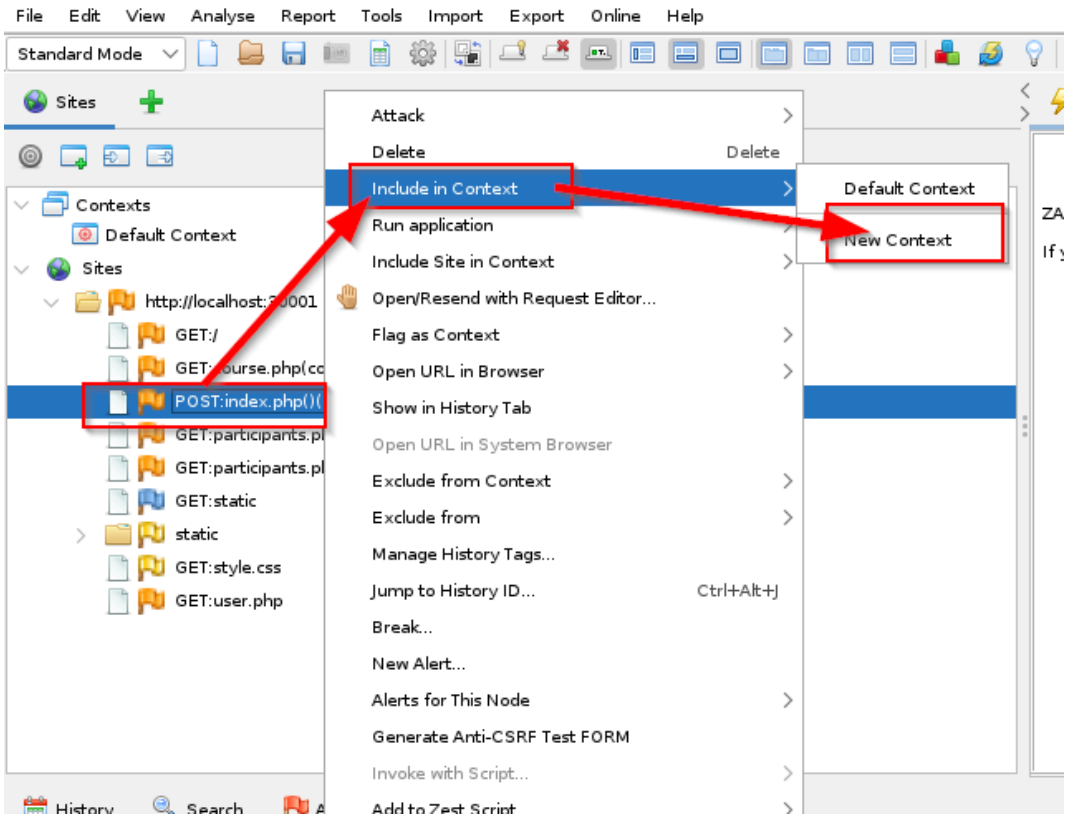
- You can now generate a report via below screenshots. Ensure report is named report.html. Navigate to the right folder also /home/labDirectory/part1. Be sure to select the right context (whatever you named). Then Generate report.

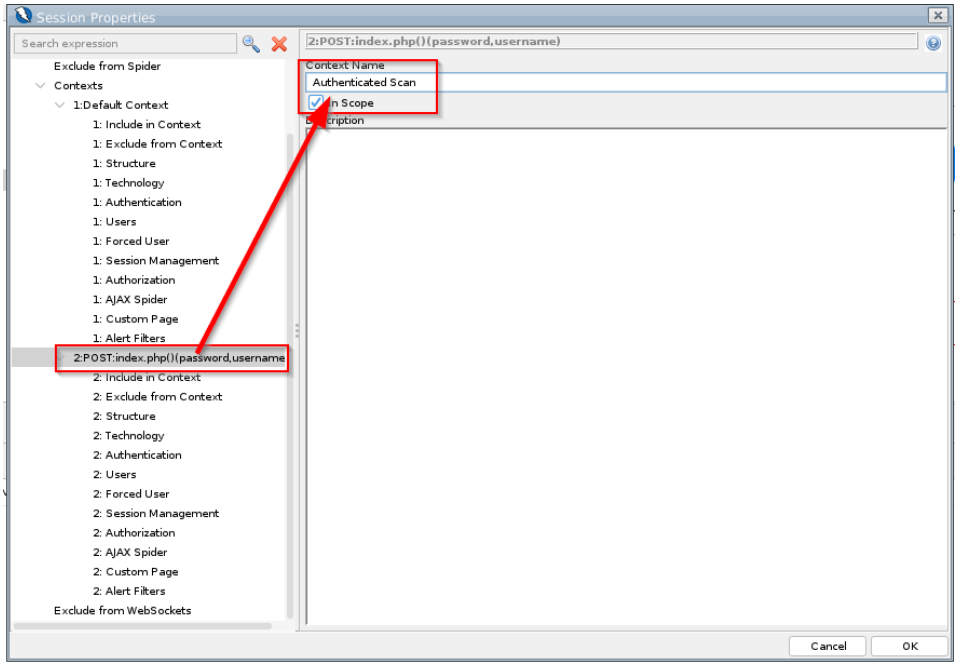

Untitled Session - 20240526-130300 - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Compare with Another Session...
Generate Report ...
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
http://localhost:30000
Sites
http://localhost:30000
GET:/
POST:/()(query)
GET:/(page)
GET:server-status
HTTP/1.1 200 OK
Date: Sun, 26 May 2024 13:03:11 GMT
Server: Apache/2.4.59 (Debian)
Vary: Accept-Encoding
Content-Length: 3881
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">


Generate Report
Scope
Template
Filter
Options
Report Title:
ZAP Scanning Report
Report Name:
report.html
Report Directory:
/home/labDirectory/part1
...
Description:
Contexts:
Default Context
Unauthenticated Scan
Sites:
http://localhost:30000
Generate If No Alerts:
Display Report:
Generate Report
Reset
Cancel

Authenticated Scan

- The process of authenticated scan is very similar, except we need to specify a few other parameters for it to work. Much like before, navigate manually the website http://localhost:30001/ , first login and then browse around and enter values in some fields.
- Earlier, we scanned the entire website of http://localhost:30000/, but this will take very long for http://localhost:30001/. So, let us restrict what URLs to scan. So, instead of entering the entire website in context, let us just add the POST request. See below steps, which are very similar to before. Name the context Authenticated Scan.

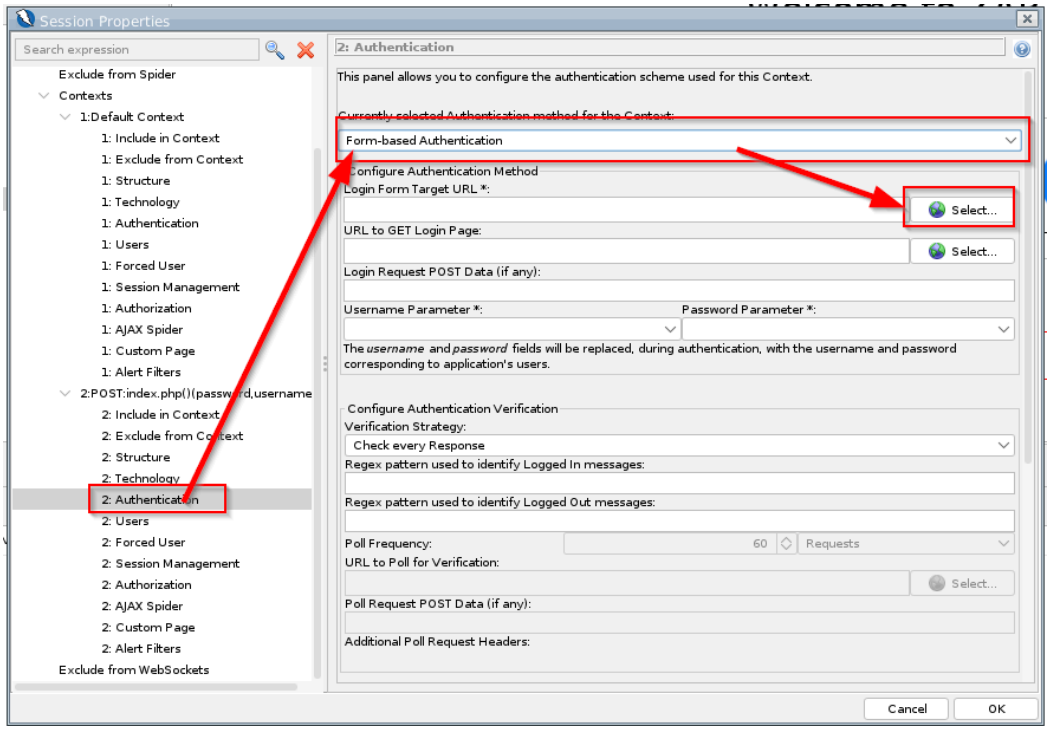


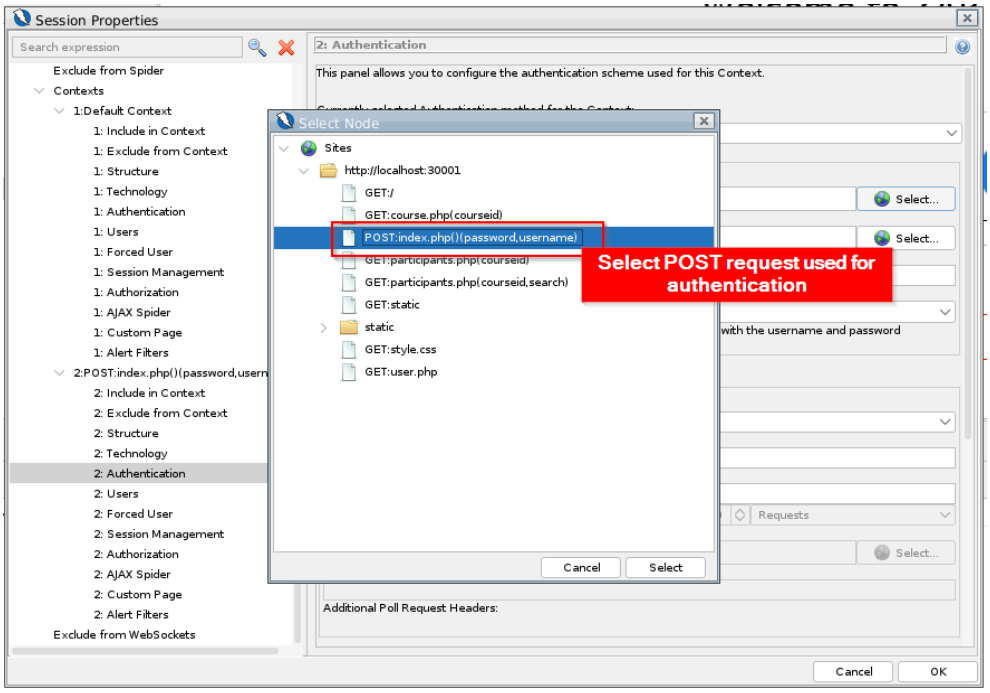


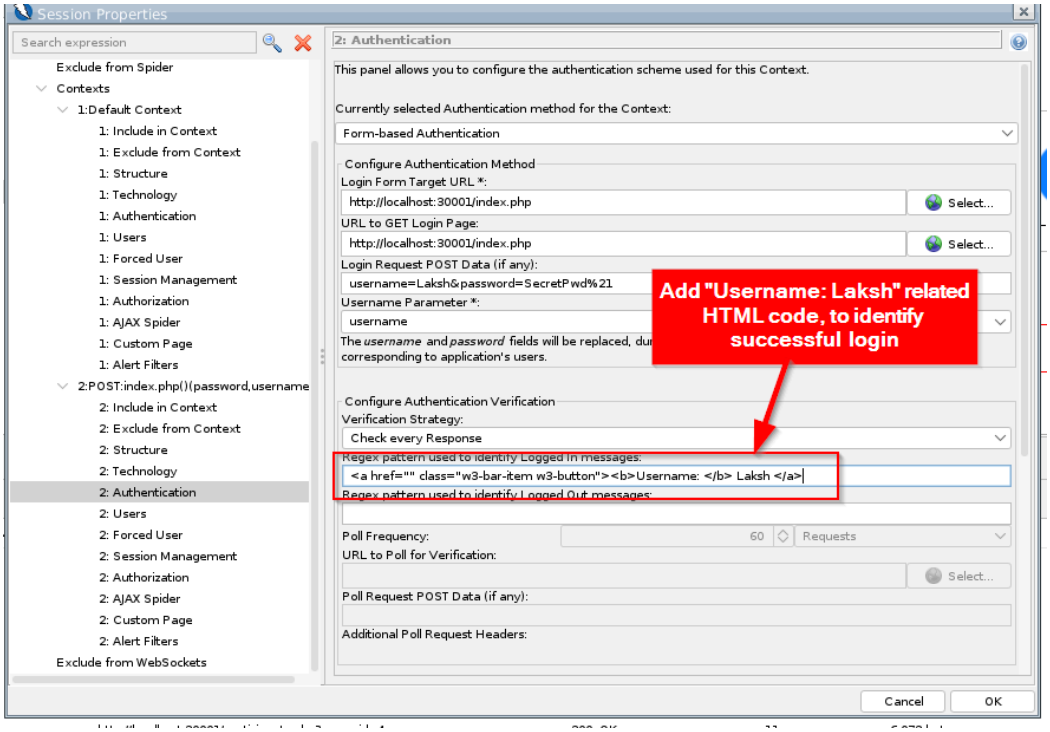
- Under Context, we have to specify a few parameters for the scan to work properly. Double click “Authenticated scan,” below pop up will open. Select Authentication within. And do what is listed in screenshots. There is specifically something called “regex pattern used to identify logged in messages”. ZAP needs to know whether the pages are “authenticated pages” i.e they can be accessed only post login. Lot of websites maintain some state for this like "Welcome, [username]". The regex pattern helps ZAP determine if a login attempt was successful by matching specific strings or patterns in the server's response. Here, you can see

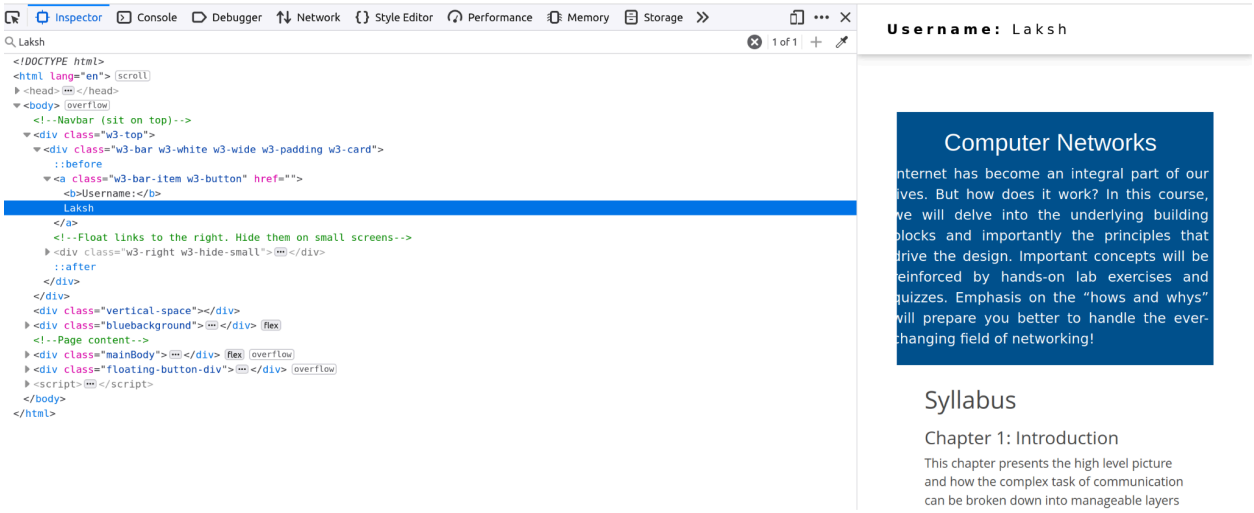
  Username: Laksh

  on all pages, post login. This can be our regex. But how to get this? Let us take the help of firefox developer tools. See screenshots further below. Search for Laksh in Inspector. Select the div class, rightclick and select edit as html. You can then cut/paste from there onto ZAP form. Once you enter this string (or you can also type manually), click ok in zap.

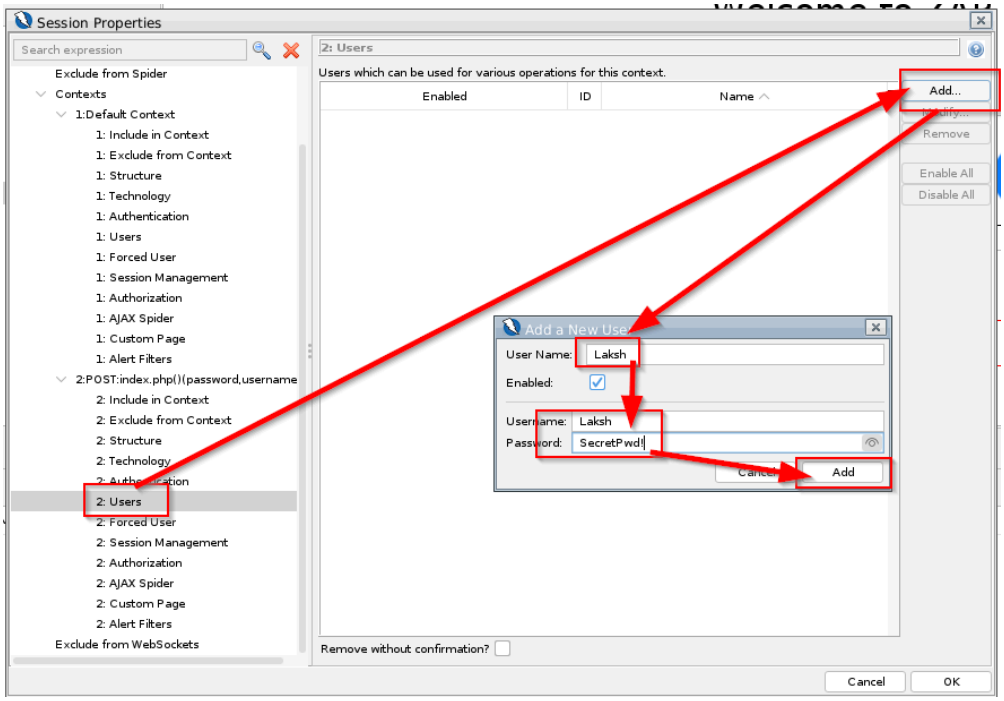

Session Properties
Search expression
Exclude from Spider
Contexts
1:Default Context
1: Include in Context
1: Exclude from Context
1: Structure
1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Management
1: Authorization
1: AJAX Spider
1: Custom Page
1: Alert Filters
2:POST:index.php()(password,username
2: Include in Context
2: Exclude from Context
2: Structure
2: Technology
2: Authentication
2: Users
2: Forced User
2: Session Management
2: Authorization
2: AJAX Spider
2: Custom Page
2: Alert Filters
Exclude from WebSockets
2: Authentication
This panel allows you to configure the authentication scheme used for this Context.
Currently selected Authentication method for the Context:
Form-based Authentication
Configure Authentication Method
Login Form Target URL *:
Select...
URL to GET Login Page:
Select...
Login Request POST Data (if any):
Username Parameter *:
Password Parameter *:
The username and password fields will be replaced, during authentication, with the username and password corresponding to application's users.
Configure Authentication Verification
Verification Strategy:
Check every Response
Regex pattern used to identify Logged In messages:
Regex pattern used to identify Logged Out messages:
Poll Frequency:
60
Requests
URL to Poll for Verification:
Select...
Poll Request POST Data (if any):
Additional Poll Request Headers:
Cancel
OK


Session Properties
Select Node
Sites
http://localhost:30001
GET:/
GET:course.php(courseid)
POST:index.php()(password,username)
GET:participants.php(courseid)
GET:participants.php(courseid,search)
GET:static
static
GET:style.css
GET:user.php
Cancel
Select
Select POST request used for authentication
Additional Poll Request Headers:
Cancel
OK

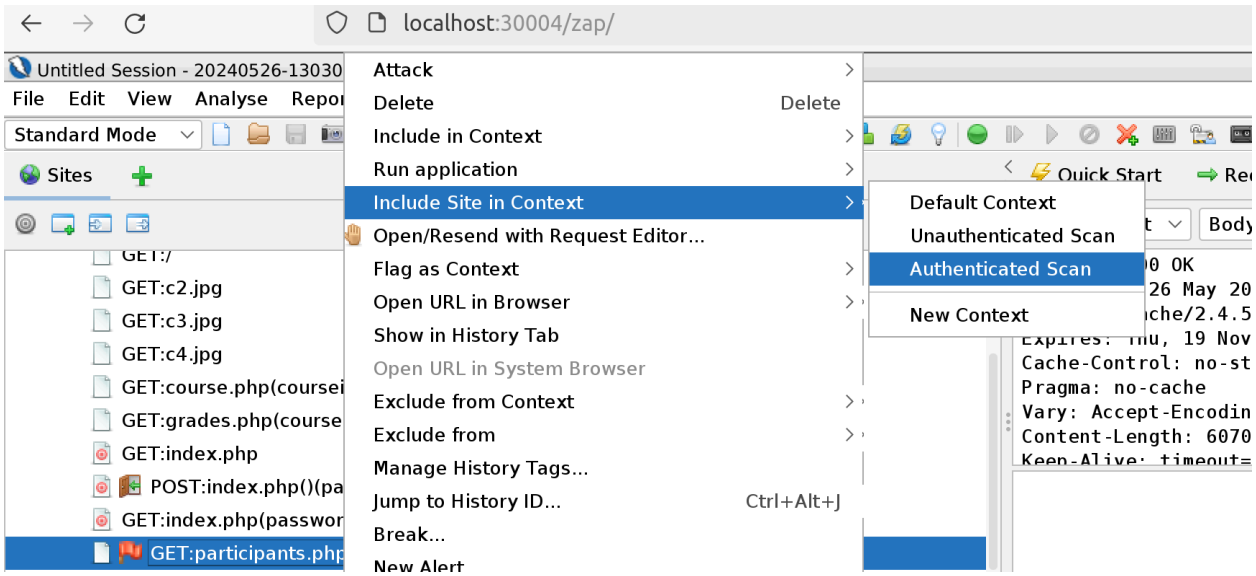




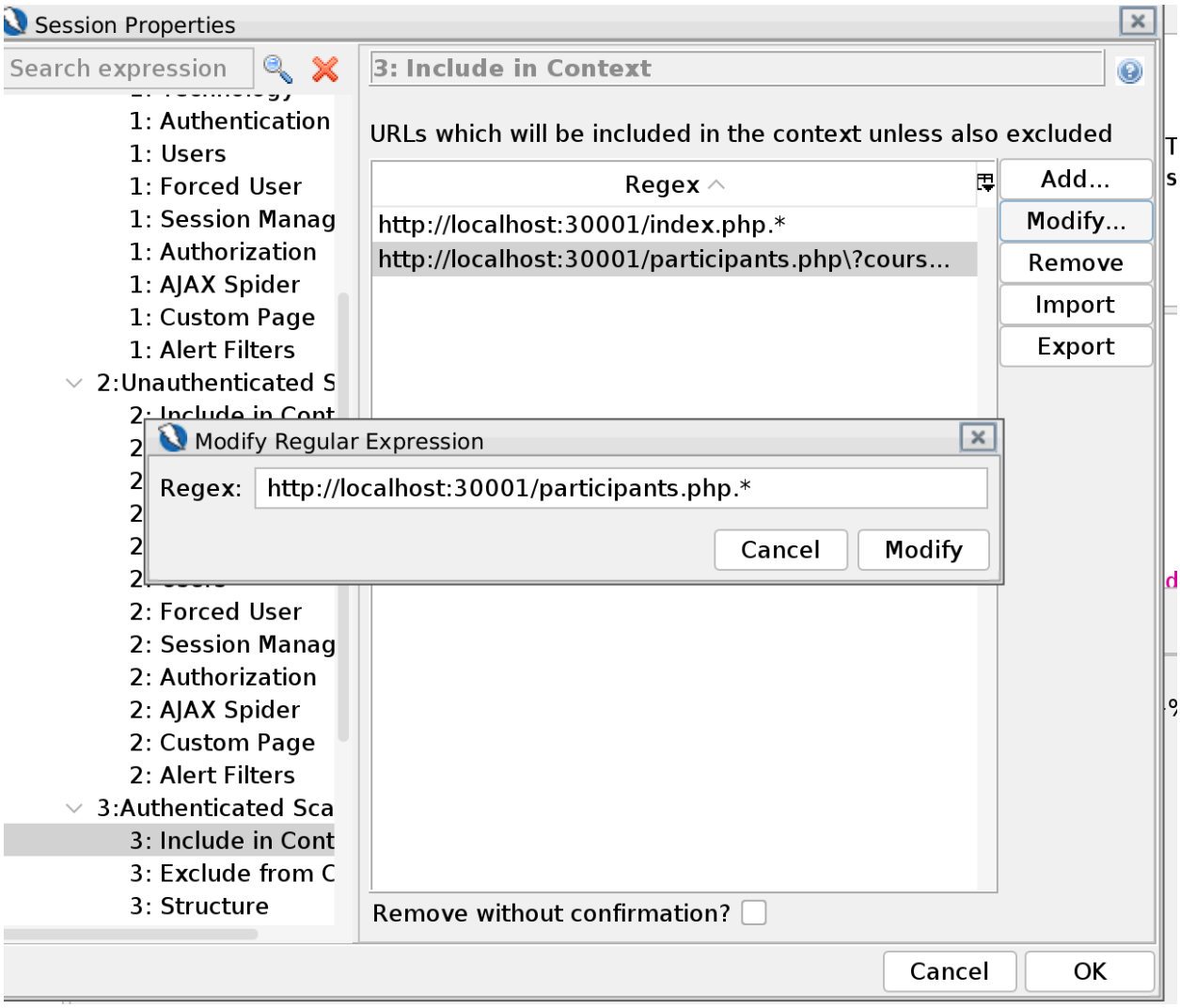
- We also need to enter User info for ZAP to login. For this click on Users, see below and follow the steps.



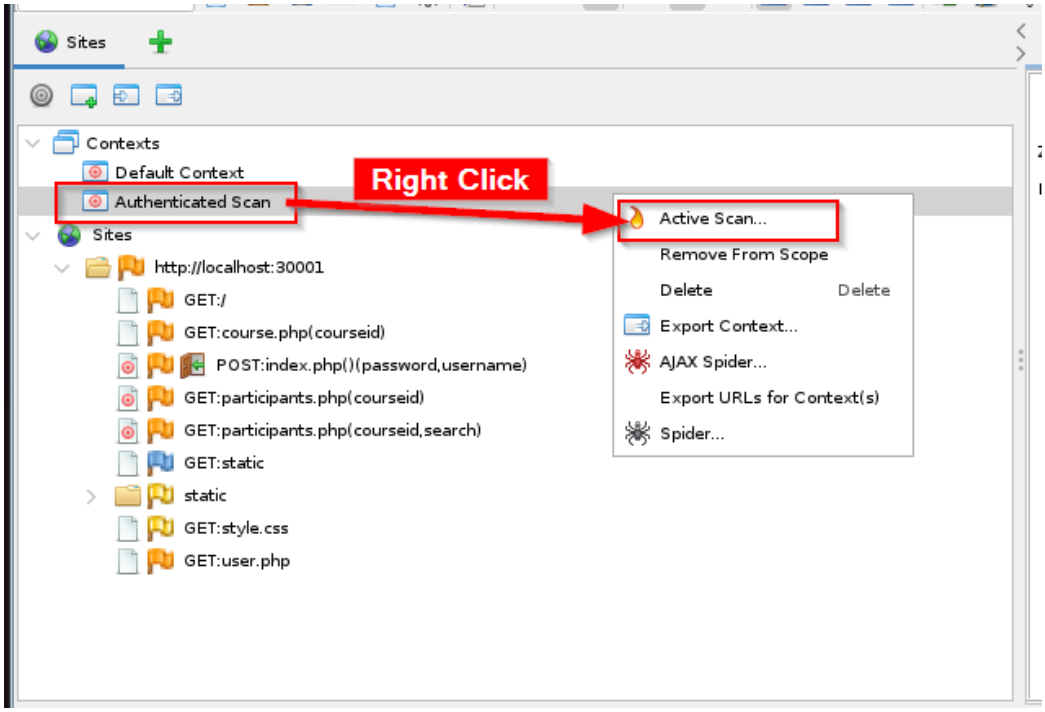
- So far we have added one POST URL to scan. Suppose we also want to add participants.php URL also to scan (remember it has a search bar and that may be vulnerable to attacks). We can do this by selecting the teh URL under sites and adding it to the “Authenticated Scan” context.

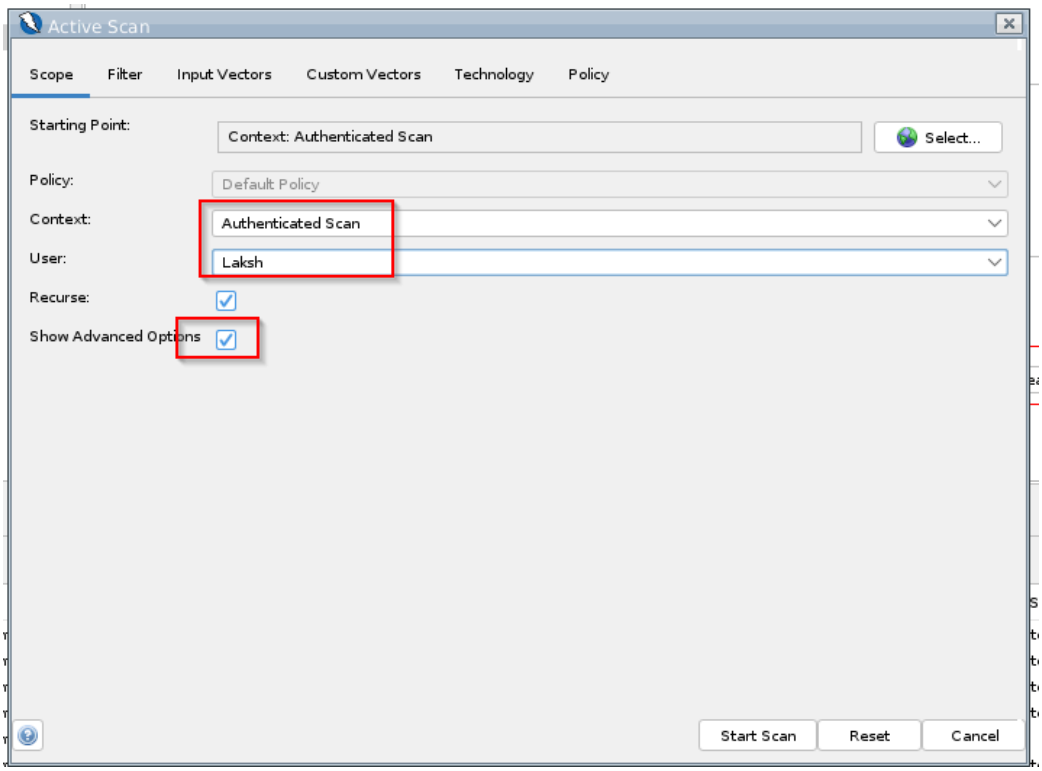


- But we want everything under participants to be covered, so go back to contexts, double click authenticated scan, below will pop up. Select participants and click modify. And change it to what is shown, this will catch every thing under participants.

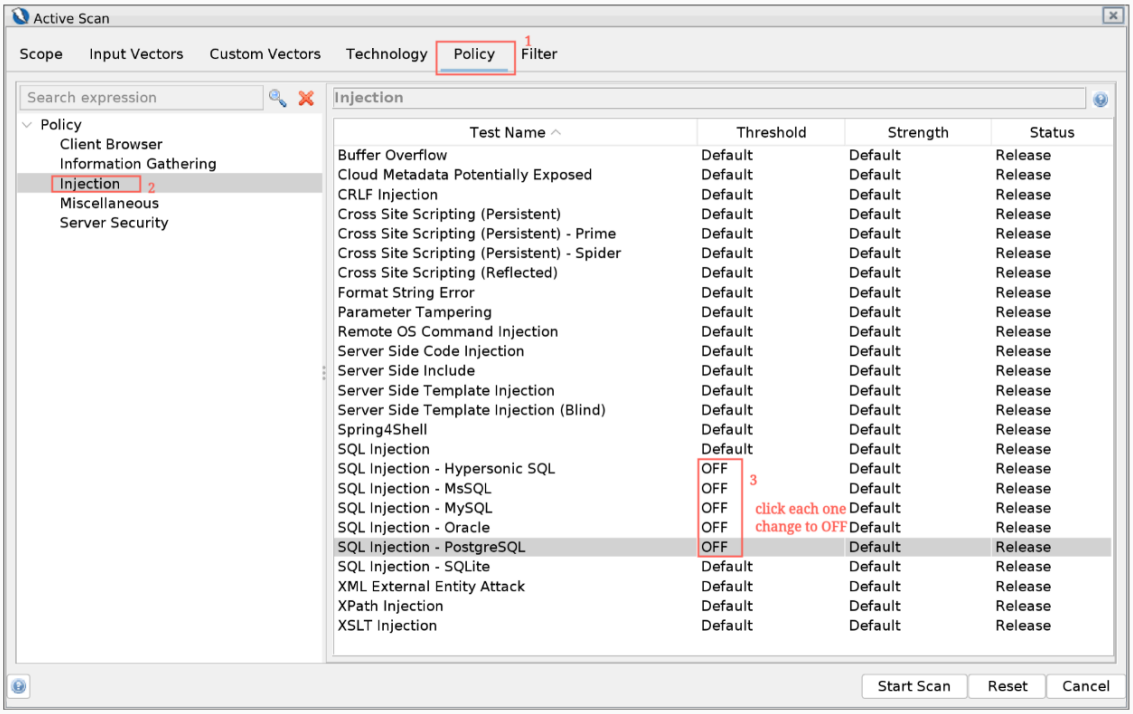


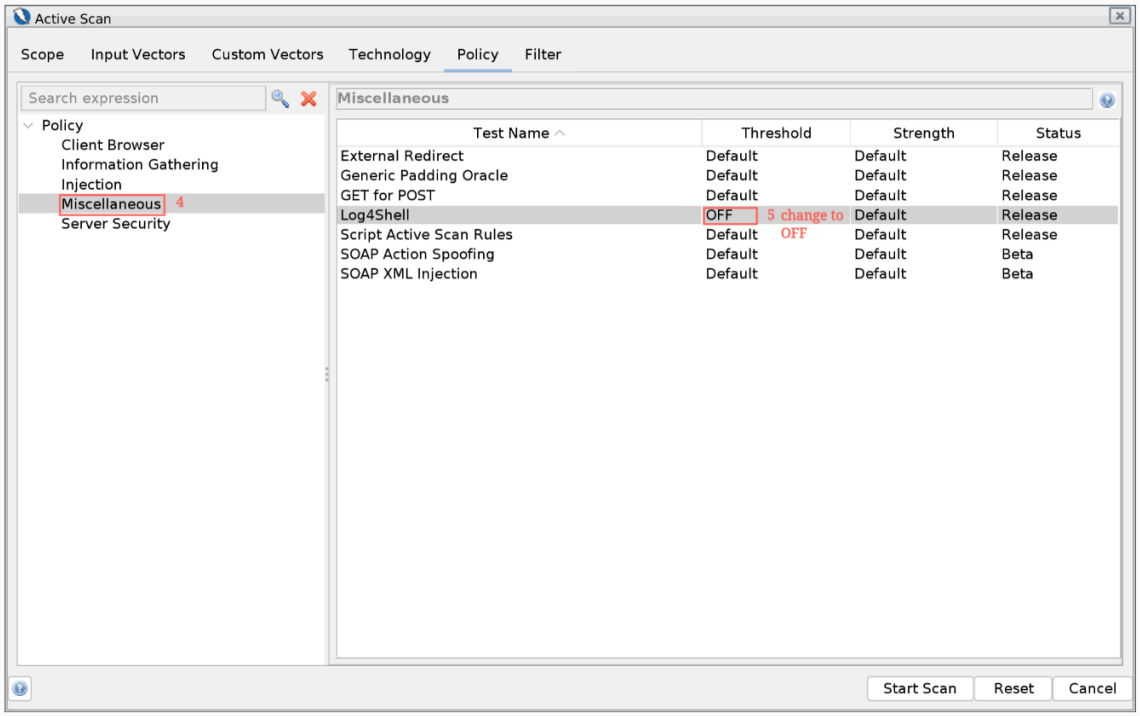
- Now we are all set, we can scan by following the same steps as before. See below.


Sites
Contexts
Default Context
Authenticated Scan
Right Click
Sites
http://localhost:30001
GET:/
GET:course.php(courseid)
POST:index.php()(password,username)
GET:participants.php(courseid)
GET:participants.php(courseid,search)
GET:static
static
GET:style.css
GET:user.php
Active Scan...
Remove From Scope
Delete
Delete
Export Context...
AJAX Spider...
Export URLs for Context(s)
Spider...


Active Scan
Scope
Filter
Input Vectors
Custom Vectors
Technology
Policy
Starting Point:
Context: Authenticated Scan
Select...
Policy:
Default Policy
Context:
Authenticated Scan
User:
Laksh
Recurse:
Show Advanced Options
Start Scan
Reset
Cancel

- If we start scanning at this point, then the scan will take about 40-45 minutes. To avoid that the additional step here is setting up active scan policies. To do that go to the "Policy" tab, and turn off tests as shown in the following 2 images.





- Post this, generate a report much like you did for part-1, except choose the right context.