OWASP ZAP Project

TASK 1 Introduction and overview of the Tool

The tool was designed by the Open Web Application Security Project and called has OWASP ZAP [OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation]

One of the best practices for protecting your web server and the clients accessing your websites is to find the vulnerabilities in your website
This task which can be automated with this tool "OWASP ZAP" from cross site scripting to sql injections covering all the top 10 vulnerabilities.

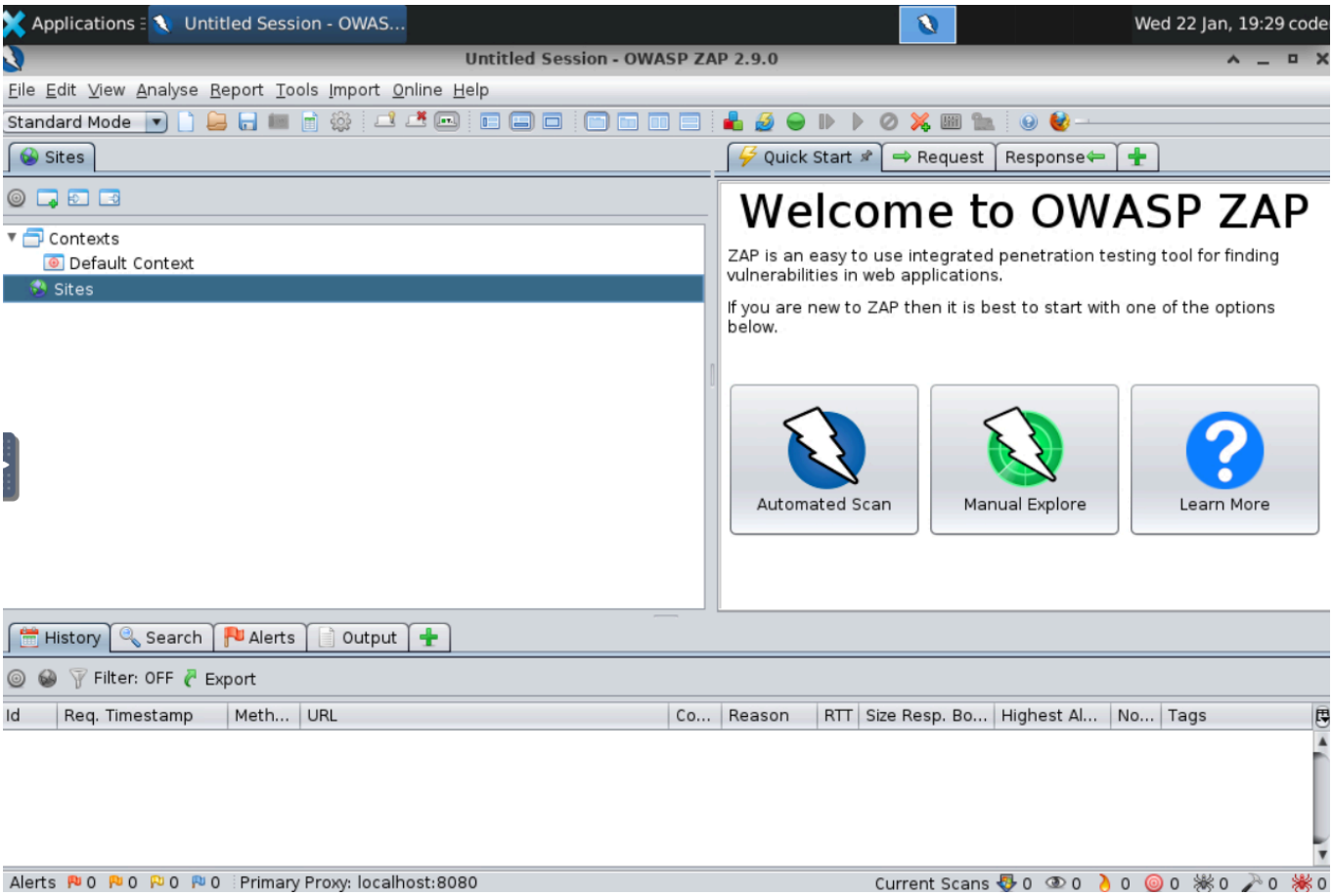
OWASP is a non-profit organization and online community that provides free content in the field of web security

It is good for web security testing and which includes the intercepting proxy, active and passive vulnerability scanners a spider web crawler a buzzer and an http request sender and brute forcer and much more
This also has a scripting engine that can be used to automate activities or to create new functionality

But everything has a flaw a until it is found so here it can also generate false positives or miss critical vulnerabilities in some cases

Remember Automated scanning tools should not be used as a replacement for manual vulnerability exploitation but rather be used in conjunction alongside manual vulnerability exploitation and backup to more manual methods.

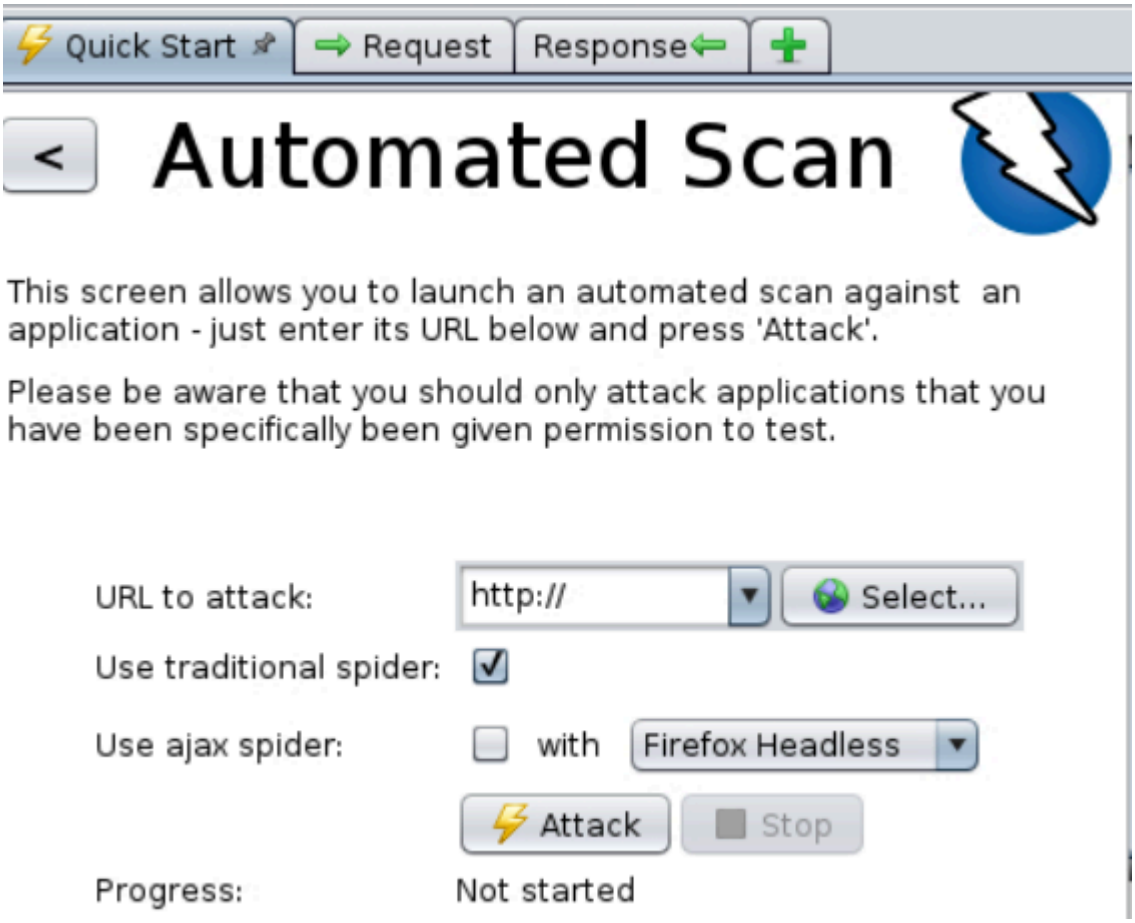
TASK 2 OWASP ZAP Layout and First Scan



This is the actual layout of the OWASP ZAP 2.9.0 version

we can see the sites tab which contains two: 1.Contexts which is a way of setting the url together and other 2: Sites which will be used for the websites that has been accessed and targeted by the ZAP

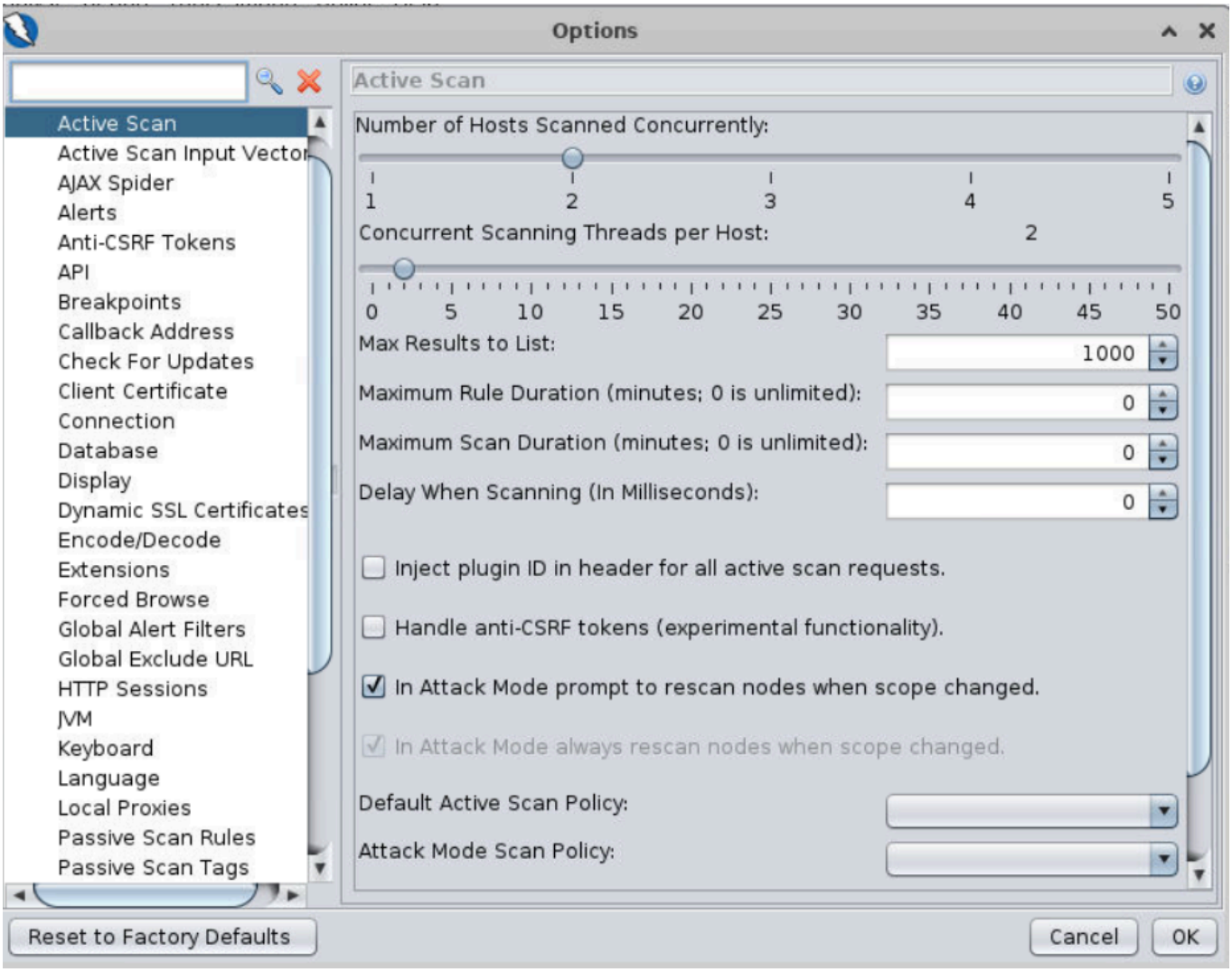
Quick start tab :
This is the easiest way to start using ZAP Which is for automated scanned tab when clicked we can see the url section which we need to provide for the tool or to the automated scan



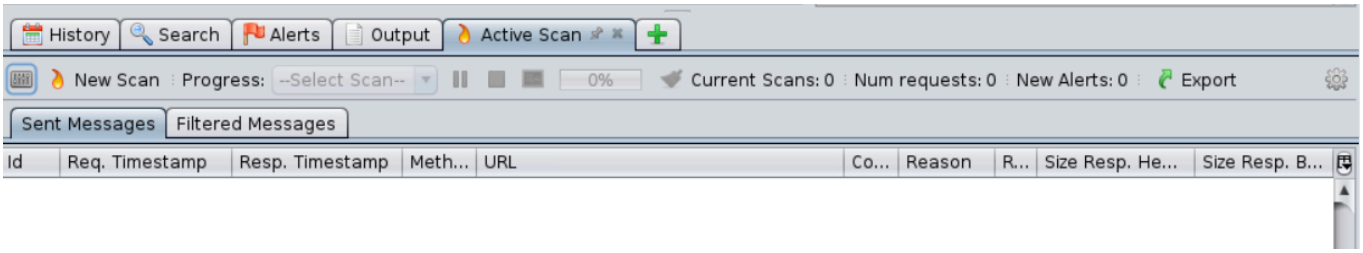
Along with this we can see other tabs which is
History, Search, Alerts, Output

History where we can see the results of the scan in live like what it is scanning the id, Req. Timestamp Method and URI, Code, Method, Reason, RTT , Size Resp.Body, Highest Alert, Note, Tags

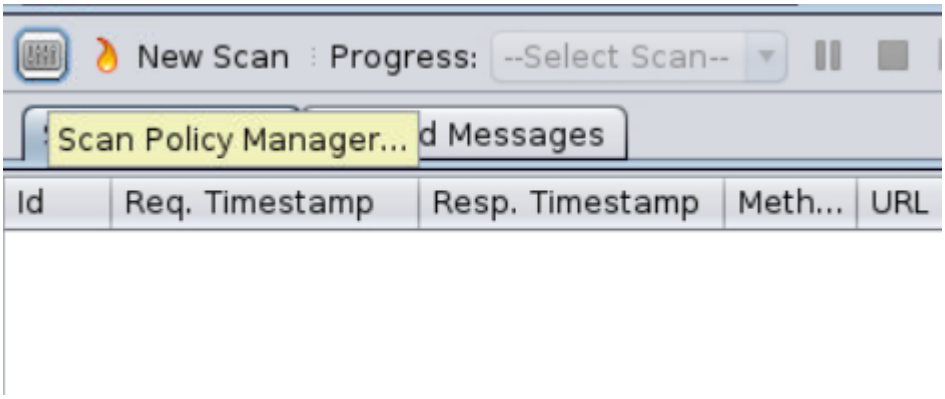
The Options button allows us to change the settings of the program



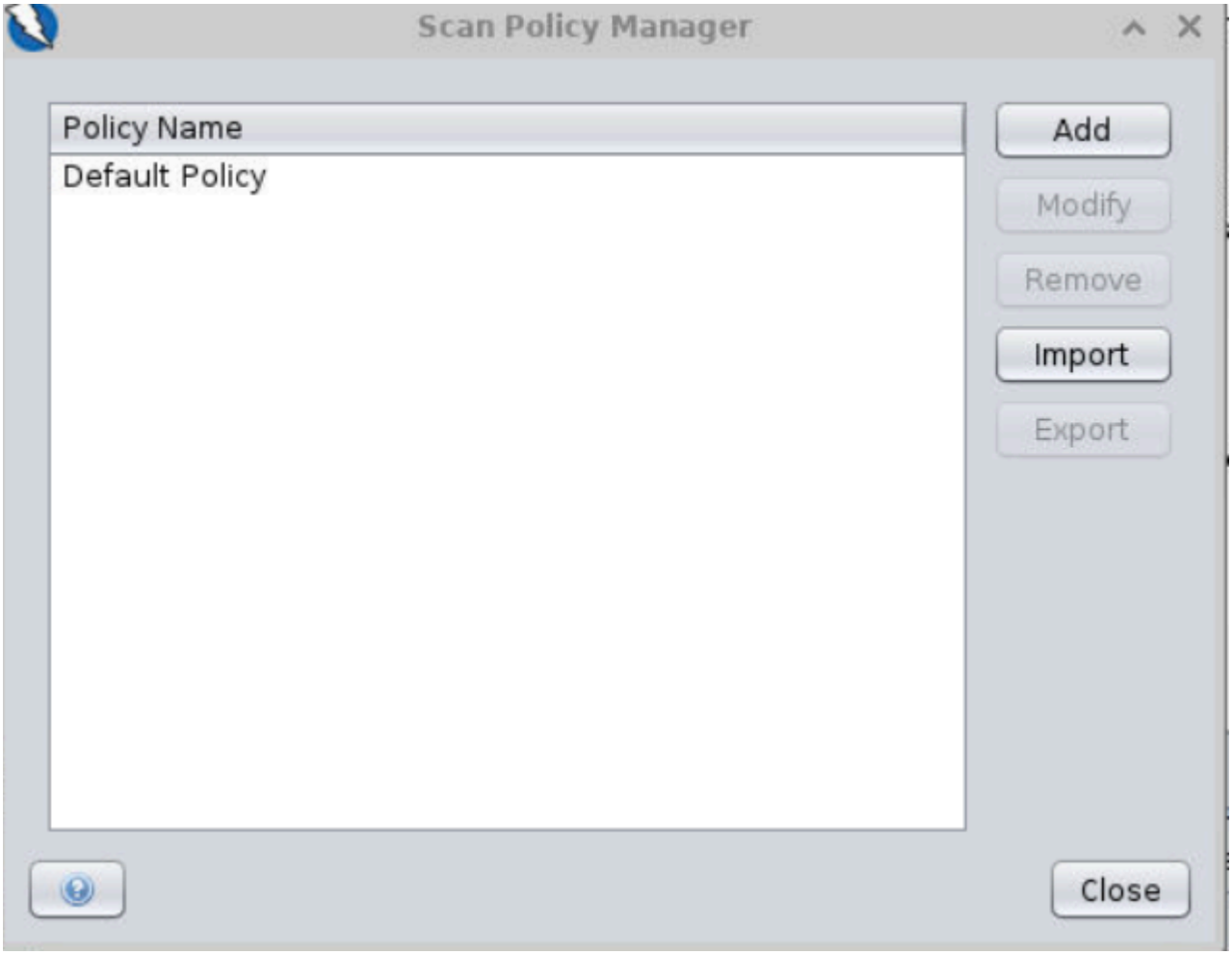
We can also modify the scan policy by adding the active scan tab by clicking the "+"

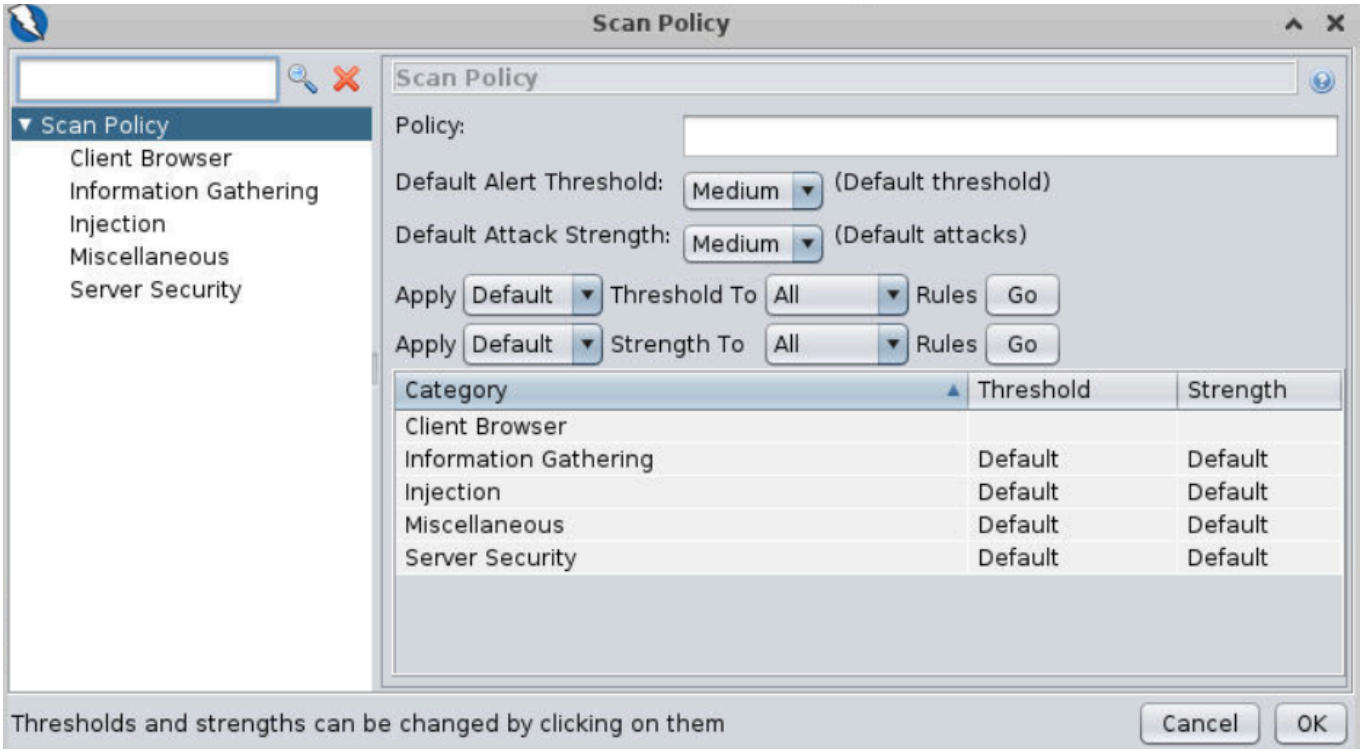


and then clicking to the scan policy manager



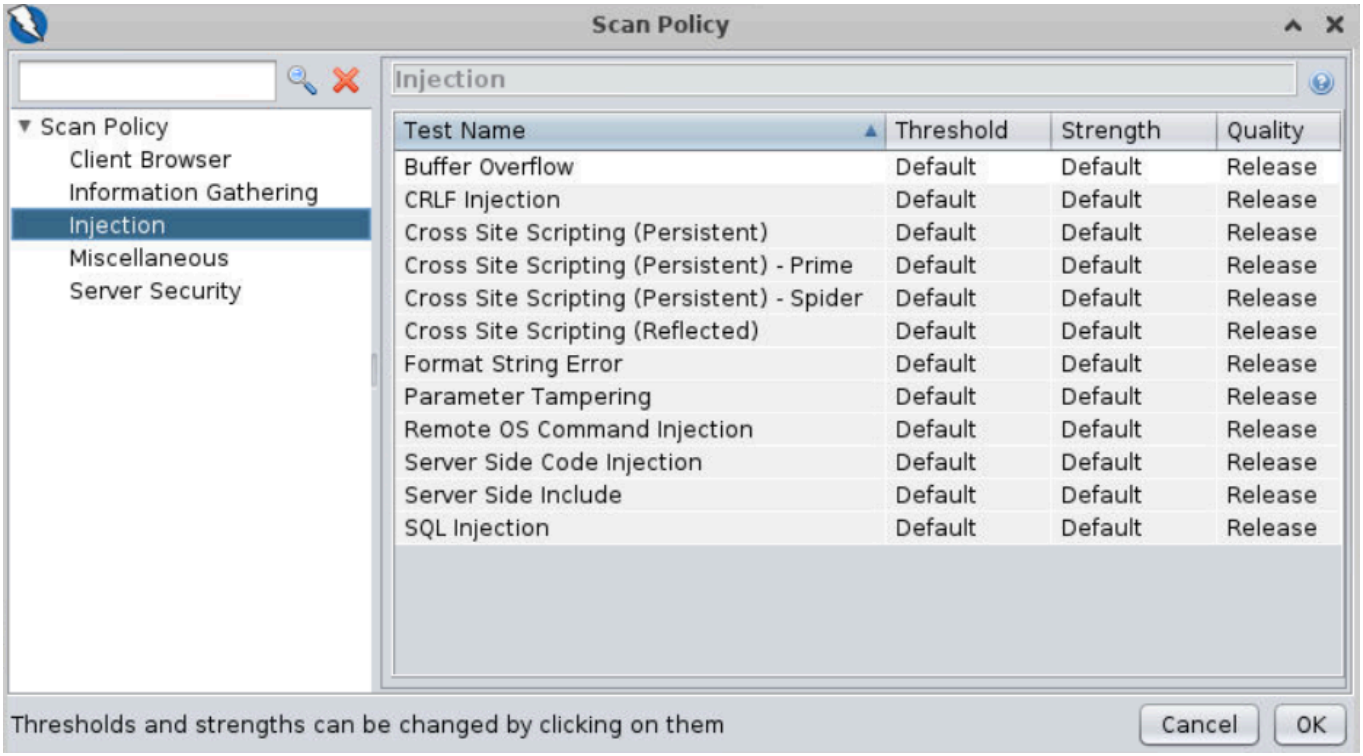
we will be presenting options with the scan policy button





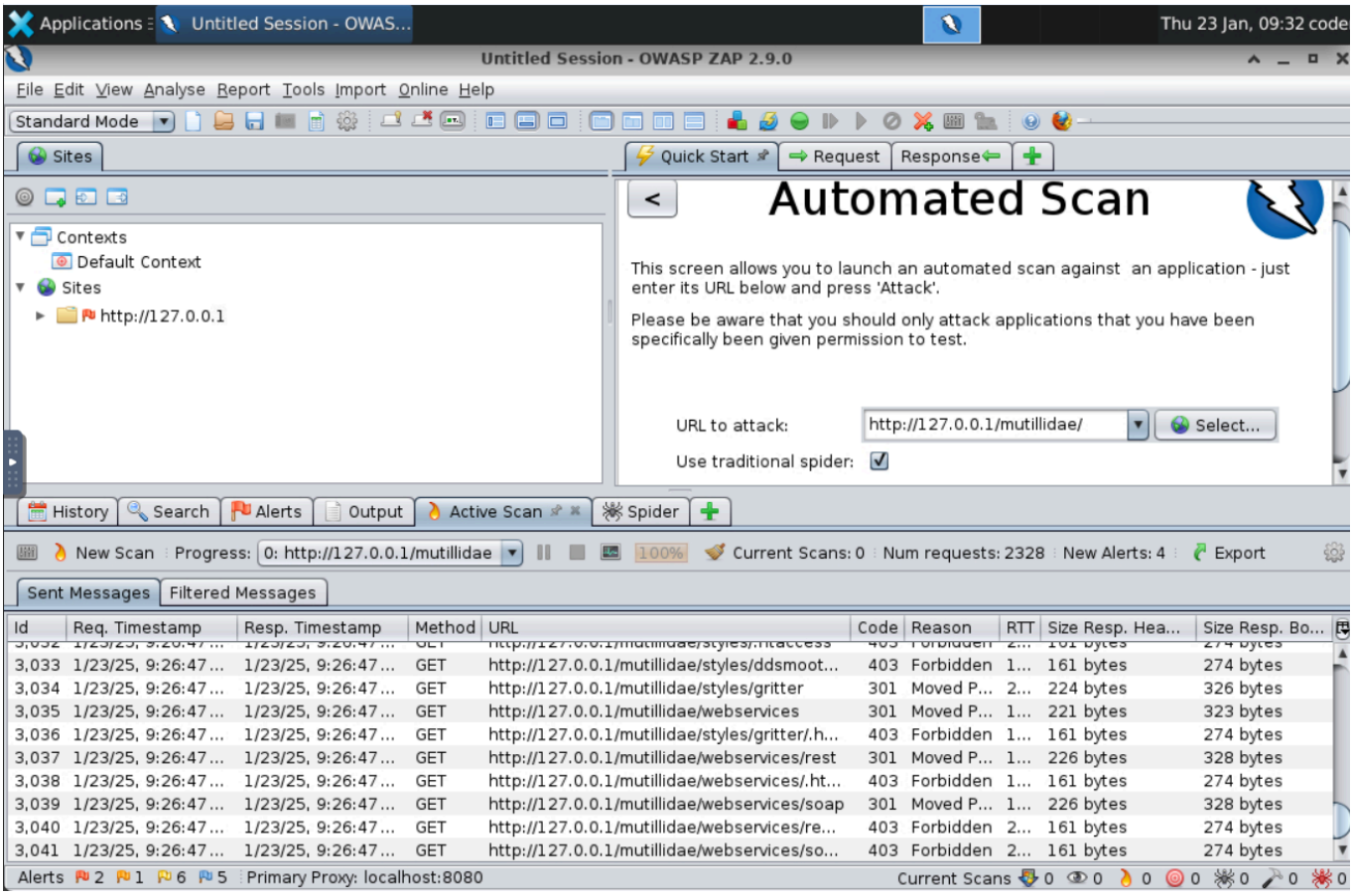
Adding a scan policy looks like this where we can customize the policies which we want to go

for and setting out the threshold and strength

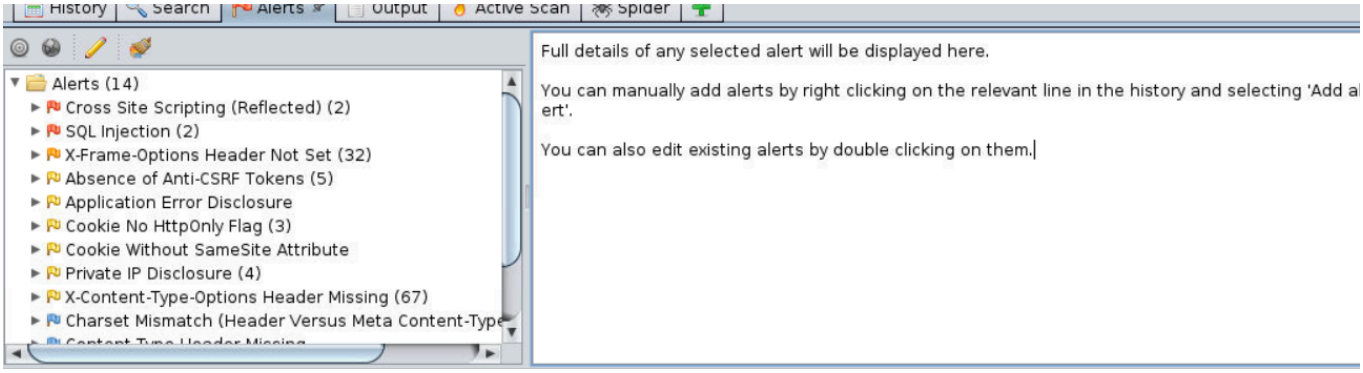


TASK 3 Analyzing the OWASP ZAP Scan Results and Generating Report

After the scan is done we can Get the report actually "cool right " so there is no need of doing a separate report and we can analyze it
we can see this in the sites tab



And in the below is the alerts tab where all the vulnerabilities are listed

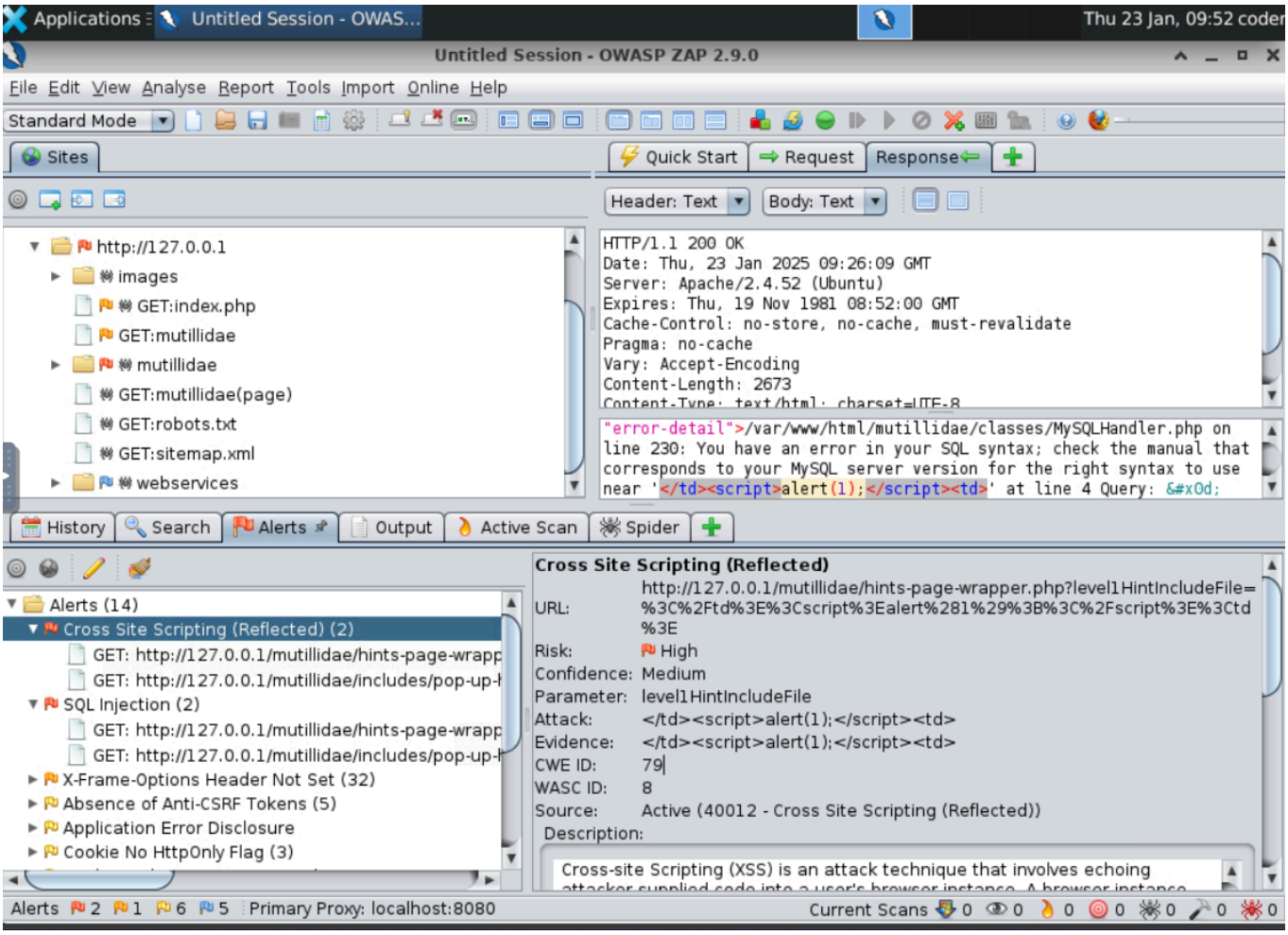


The alerts are listed has three different categories marking with different colored flags

1.High - Red flag

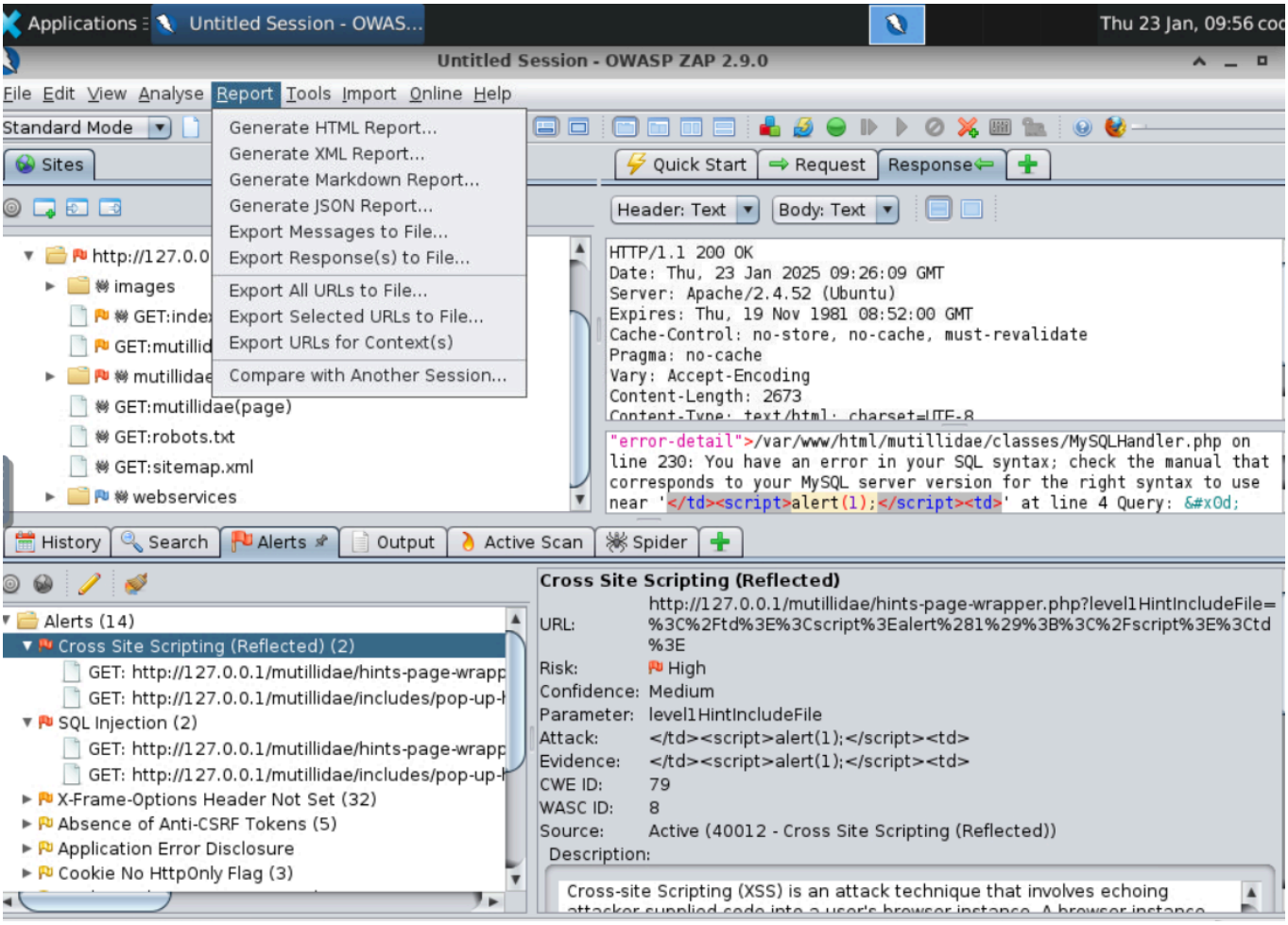
2.Medium - Orange flag

3.Low - Yellow flag



we can analyze the Vulnerabilities detailed

The Important thing which is the Reporting is also done by this tool has mentioned earlier

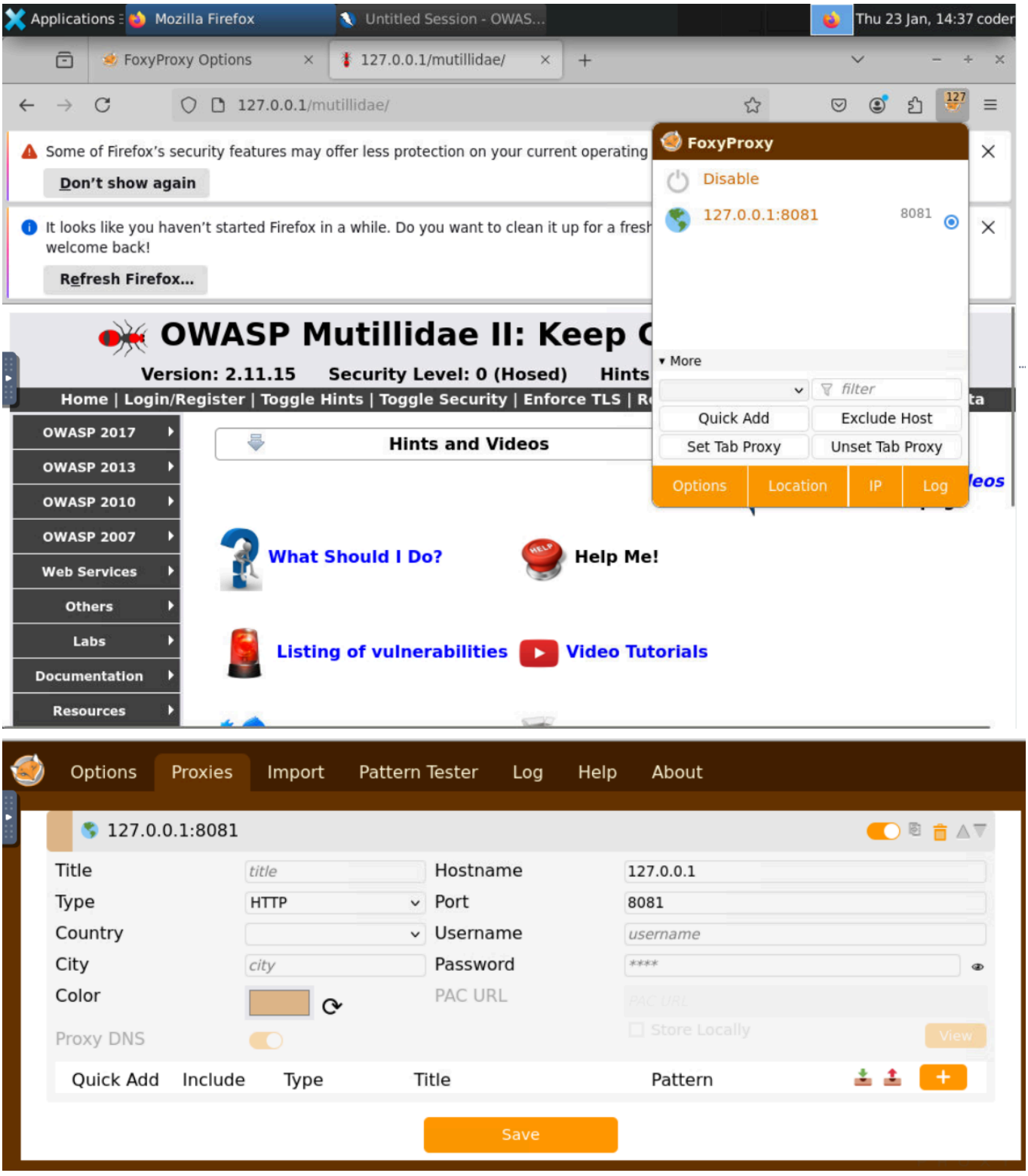


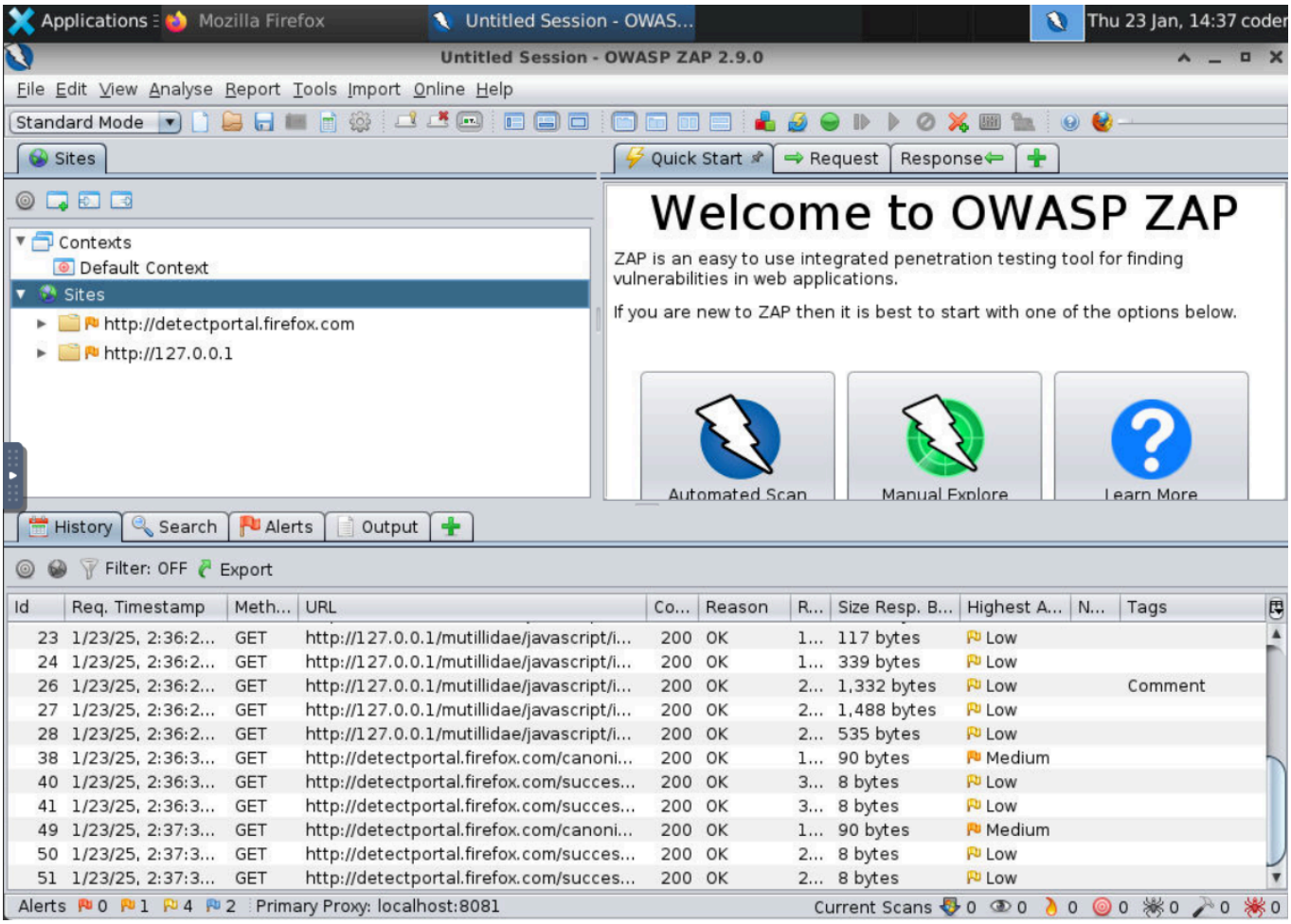
Saving has a Html file and then converting into to pdf and submitting to the application owners is a much important task in VAPT(Vulnerability Assessment and Penetration testing)

TASK 4 Setting Up Foxy Proxy in Firefox to use OWASP ZAP as a Proxy

This Feature is very Important for a Web Security Testing Tool
Foxy Proxy which enables us to intercept the traffic if i would say the request we wanted to send to the server will be not sent directly it is ,intercepted at us the address where the zap is listening "in this tool"
In order to
Owasp zap is considered an integrated non-transparent proxy and when using the proxy we need to configure the browser for the request to the ZAP tool

Two ways to configure the firefox browser manually or we can install a proxy Firefox add-on called FoxyProxy which requires an initial configuration

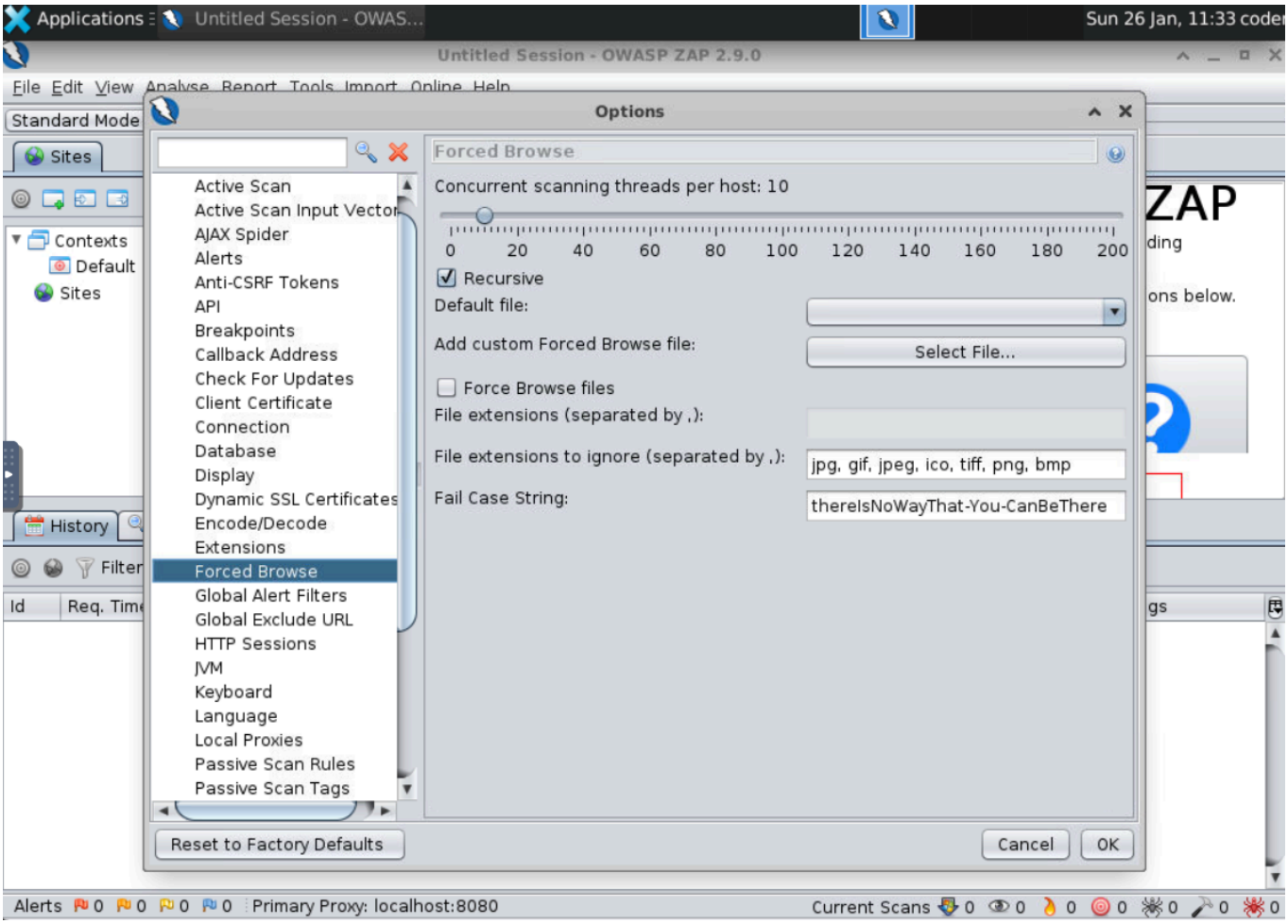

Applications
Mozilla Firefox
Untitled Session - OWAS...
Thu 23 Jan, 14:37 coder
FoxyProxy Options
127.0.0.1/mutillidae/
127.0.0.1/mutillidae/
Some of Firefox's security features may offer less protection on your current operating
Don't show again
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh
welcome back!
Refresh Firefox...
FoxyProxy
Disable
127.0.0.1:8081
8081
More
filter
Quick Add
Exclude Host
Set Tab Proxy
Unset Tab Proxy
Options
Location
IP
Log
OWASP Mutillidae II: Keep C
Version: 2.11.15
Security Level: 0 (Hosed)
Hints
Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
Others
Labs
Documentation
Resources
Hints and Videos
What Should I Do?
Help Me!
Listing of vulnerabilities
Video Tutorials
Options
Proxies
Import
Pattern Tester
Log
Help
About
127.0.0.1:8081
Title
title
Type
HTTP
Country
City
city
Color
Proxy DNS
Hostname
127.0.0.1
Port
8081
Username
username
Password
****
PAC URL
Store Locally
View
Quick Add
Include
Type
Title
Pattern
Save



TASK 5 Finding Files and Folders Using a Dictionary List Within OWASP ZAP

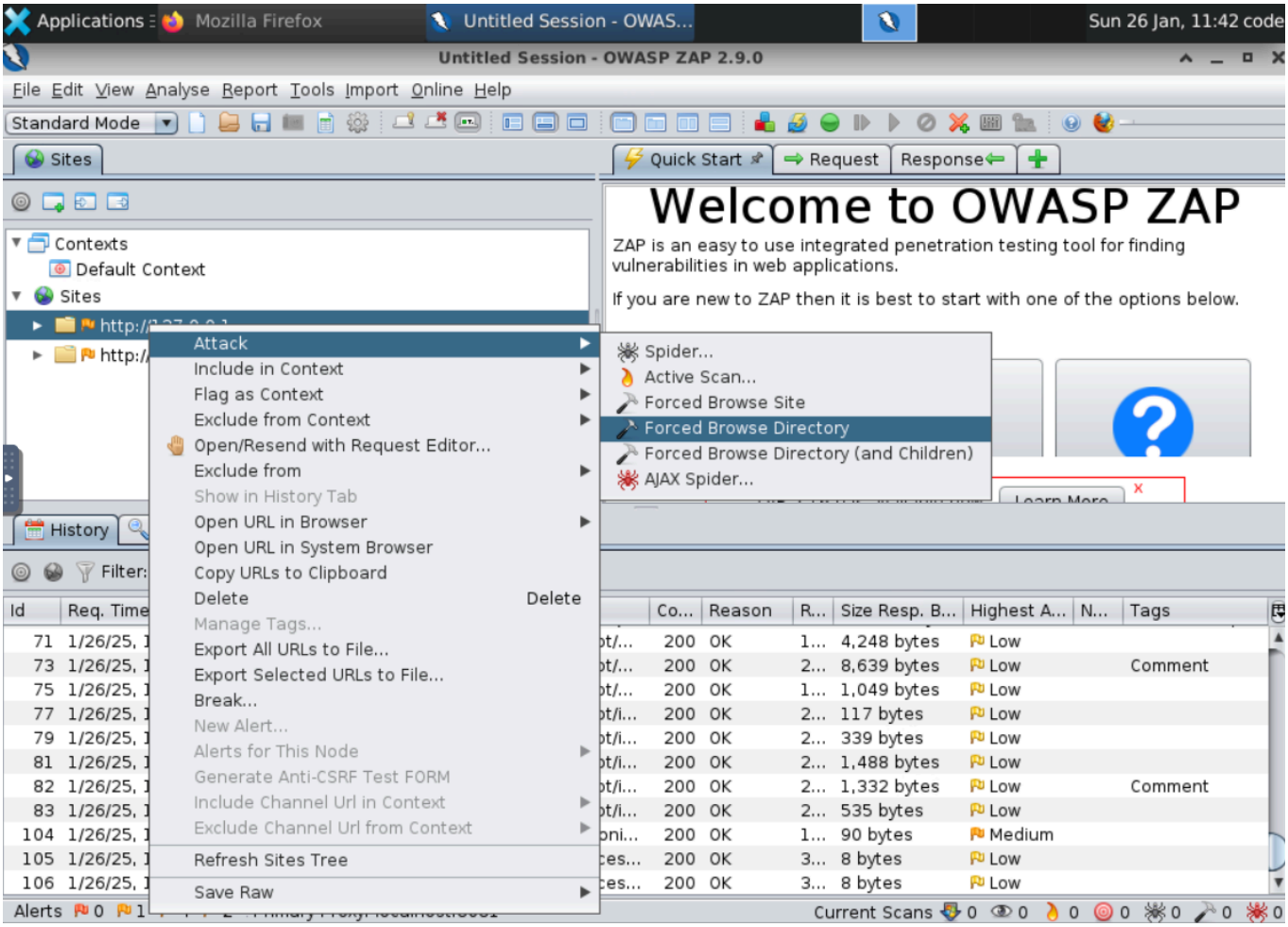
Finding files and folders of a web server using dictionary list

ZAP uses dictionary list of brute-force directories in a web app it tries to access all the directories and files listed used for attacking web authentications and discovering hidden web pages within a web application we can provide the Dic file or list that zap need to use



In options You can find the forced Browse option and then select the dictionary file which you wanted to use and check whether the froxy proxy is in on or not if not on it and enter the url you

wanted to so the forced attack

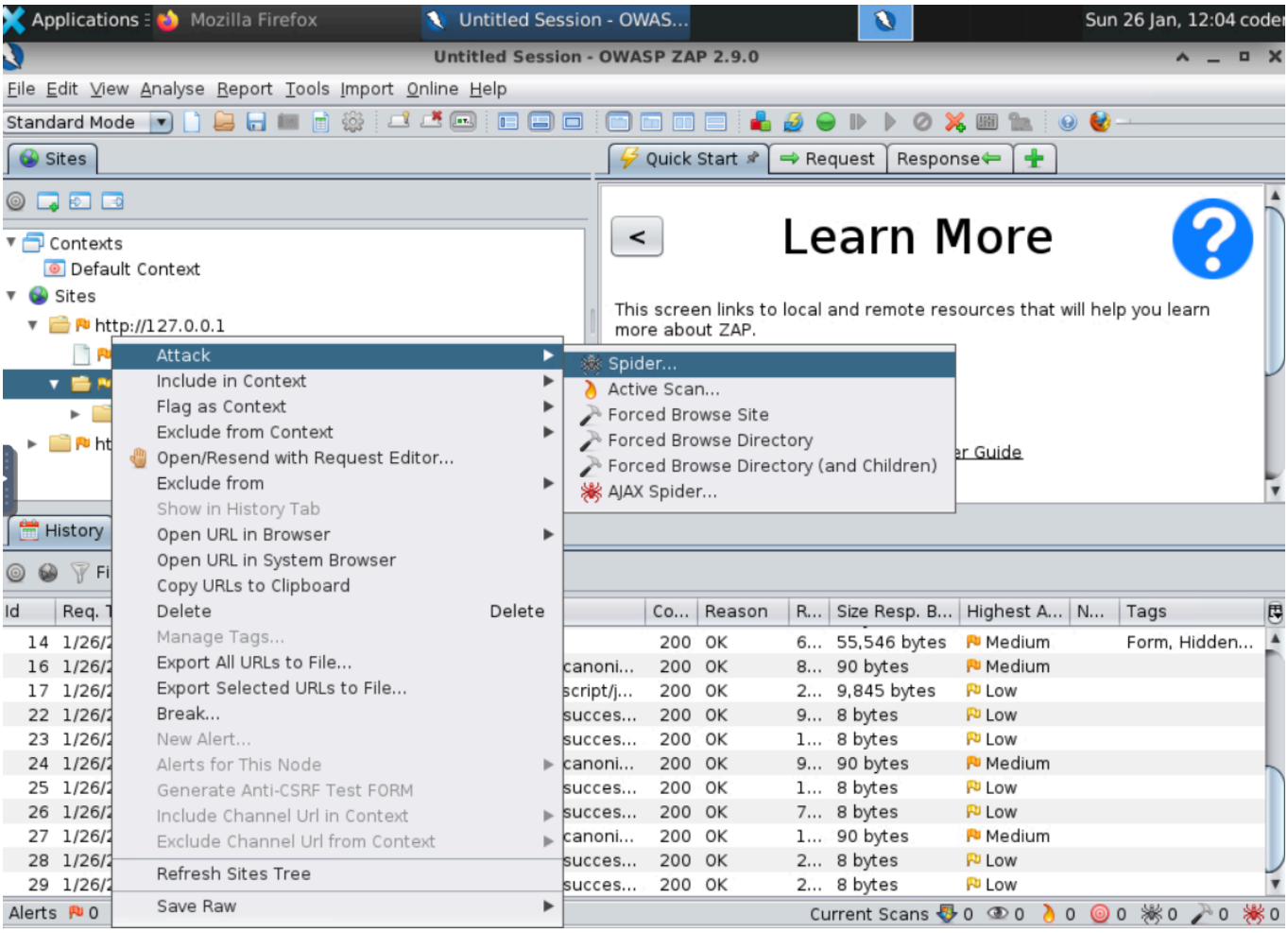


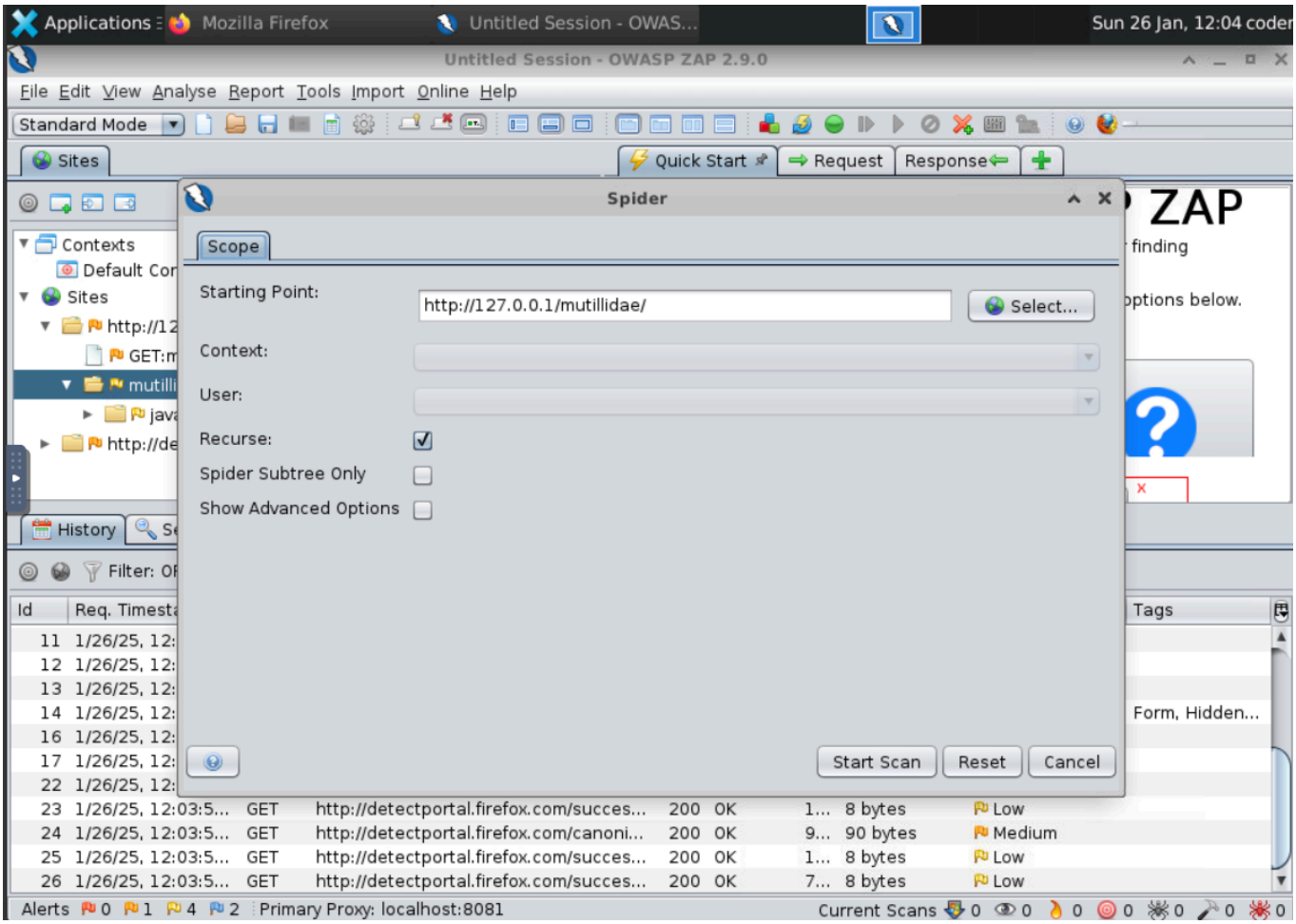
Using OWASP ZAP TO Spider Crawl a website to Find URL's and Links

Discovering how to use ZAP to crawl or spider a website to find URLs and Links
Web crawlers and spiders can be used to browse every link included in every web page included in the scope requested and keeps a record of every file displayed by it Zap can be used to automate and accelerate this task
ZAP spotter follows the formed responses redirects the URLs within the robots.txt and sitemap.xml files of a web server we can then save those results and analyze them offline This stores all the requests and responses for later analysis
Downloading a site in this way to directory in pc can give us a static copy of the information

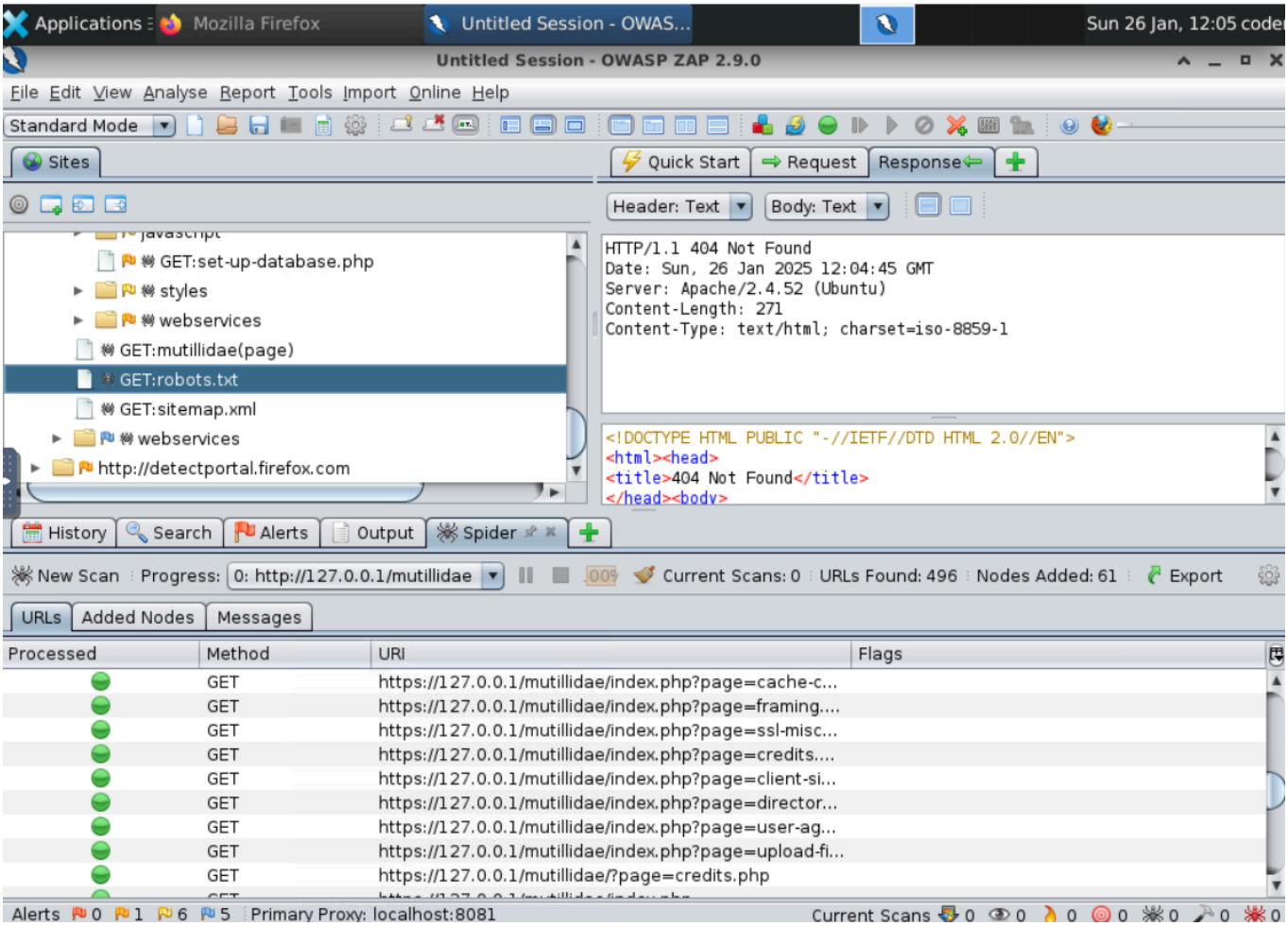
Others ways to download like that the static webpages is using wget and httrack but does not save the actual req and responses states of the server

With the spider integrated within OWASP ZAP it will record all the information


Applications
Mozilla Firefox
Untitled Session - OWAS...
Sun 26 Jan, 12:04
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
http://127.0.0.1
Learn More
This screen links to local and remote resources that will help you learn more about ZAP.
Attack
Include in Context
Flag as Context
Exclude from Context
Open/Resend with Request Editor...
Exclude from
Show in History Tab
Open URL in Browser
Open URL in System Browser
Copy URLs to Clipboard
Delete
Delete
Manage Tags...
Export All URLs to File...
Export Selected URLs to File...
Break...
New Alert...
Alerts for This Node
Generate Anti-CSRF Test FORM
Include Channel Url in Context
Exclude Channel Url from Context
Refresh Sites Tree
Save Raw
Spider...
Active Scan...
Forced Browse Site
Forced Browse Directory
Forced Browse Directory (and Children)
AJAX Spider...
History
Id
Req. T
Co...
Reason
R...
Size Resp. B...
Highest A...
N...
Tags
14 1/26/2 200 OK 6... 55,546 bytes Medium Form, Hidden...
16 1/26/2 canoni... 200 OK 8... 90 bytes Medium
17 1/26/2 script/j... 200 OK 2... 9,845 bytes Low
22 1/26/2 succes... 200 OK 9... 8 bytes Low
23 1/26/2 succes... 200 OK 1... 8 bytes Low
24 1/26/2 canoni... 200 OK 9... 90 bytes Medium
25 1/26/2 succes... 200 OK 1... 8 bytes Low
26 1/26/2 succes... 200 OK 7... 8 bytes Low
27 1/26/2 canoni... 200 OK 1... 90 bytes Medium
28 1/26/2 succes... 200 OK 2... 8 bytes Low
29 1/26/2 succes... 200 OK 2... 8 bytes Low
Alerts 0
Current Scans 0 0 0 0 0 0 0


Applications
Mozilla Firefox
Untitled Session - OWAS...
Sun 26 Jan, 12:04 coder
Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Spider
Scope
Starting Point:
http://127.0.0.1/mutillidae/
Select...
Context:
User:
Recurse:
Spider Subtree Only
Show Advanced Options
Start Scan
Reset
Cancel
Contexts
Default Cor
Sites
GET:m
mutilli
java
http://de
History
Filter: Of
Id
Req. Timesta
Tags
11 1/26/25, 12:
12 1/26/25, 12:
13 1/26/25, 12:
14 1/26/25, 12:
Form, Hidden...
16 1/26/25, 12:
17 1/26/25, 12:
22 1/26/25, 12:
23 1/26/25, 12:03:5... GET http://detectportal.firefox.com/succes... 200 OK 1... 8 bytes Low
24 1/26/25, 12:03:5... GET http://detectportal.firefox.com/canoni... 200 OK 9... 90 bytes Medium
25 1/26/25, 12:03:5... GET http://detectportal.firefox.com/succes... 200 OK 1... 8 bytes Low
26 1/26/25, 12:03:5... GET http://detectportal.firefox.com/succes... 200 OK 7... 8 bytes Low
Alerts 0 1 4 2
Primary Proxy: localhost:8081
Current Scans 0 0 0 0 0 0 0

By scanning You can analyze the results and requests and responses

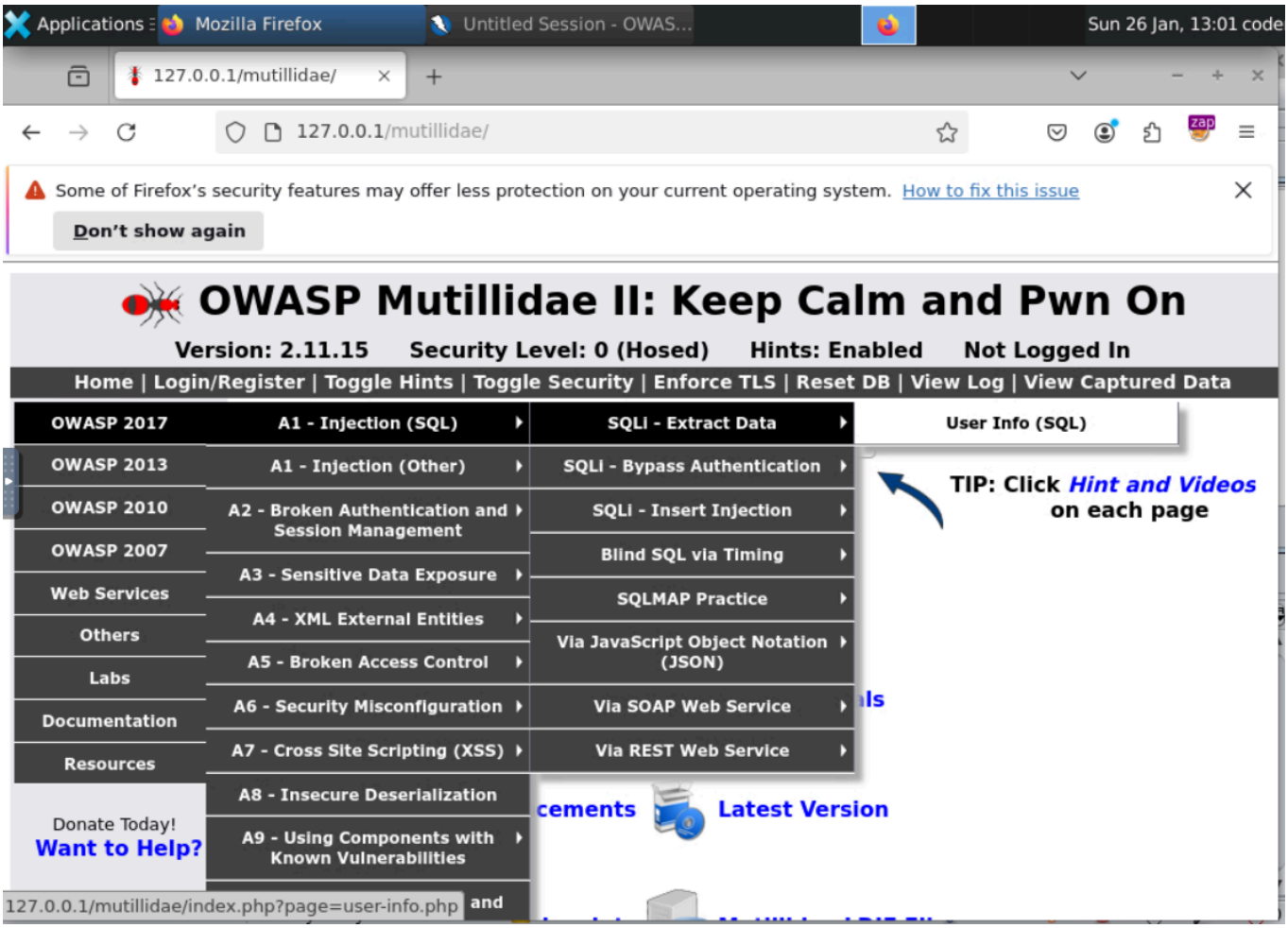


We can use this for pentesting like repeating the request that modified data and we can perform active and passive vulnerability scans

Using OWASP ZAP for Viewing and Altering Requests

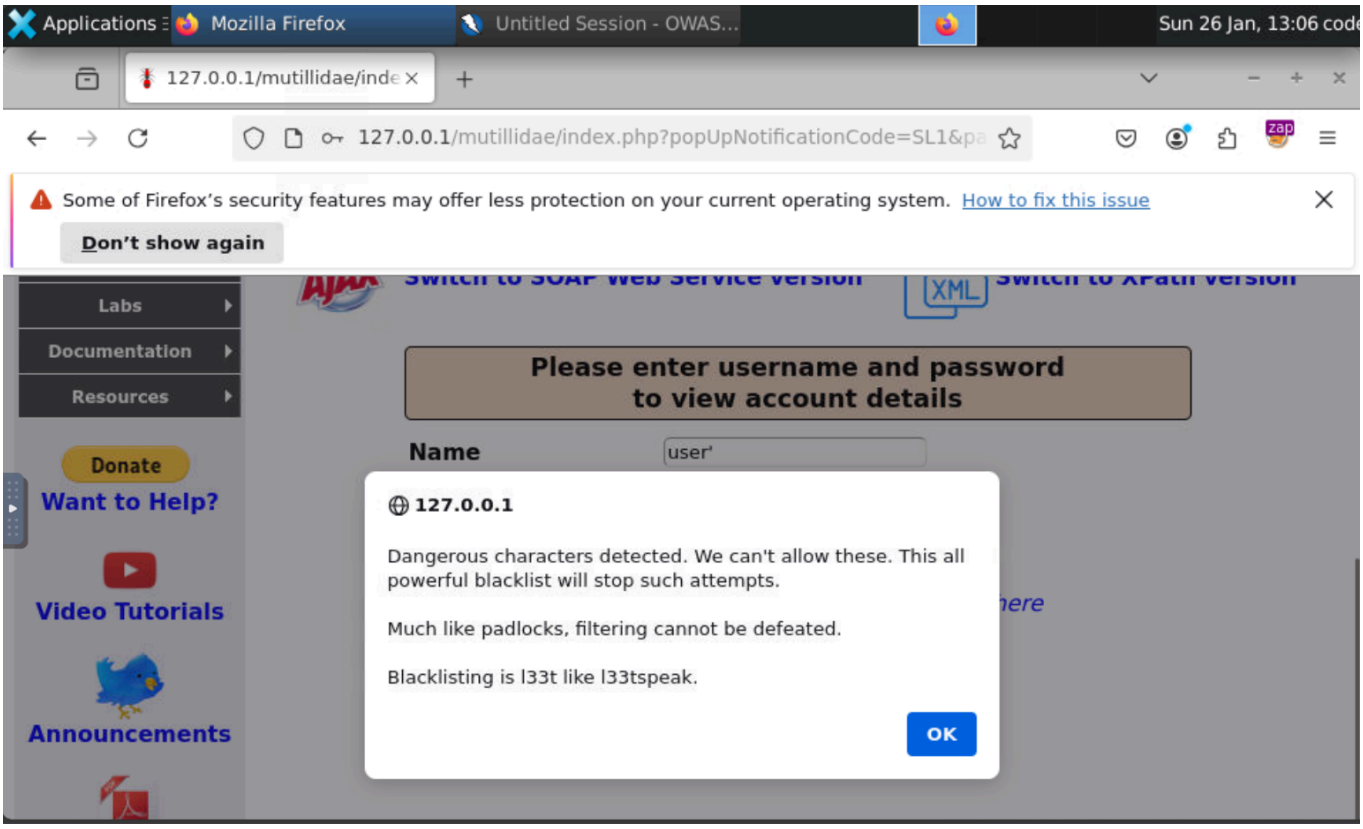
ZAP is very flexible for modifying the requests, it can change the request method from GET to POST and save the req-response pair to be processed by other tools

For example let us use this tool to modify a valid req and make it invalid with a little bit of malicious SQL injection and then send to server and provoke unexpected behavior from it basically bypassing a client validation



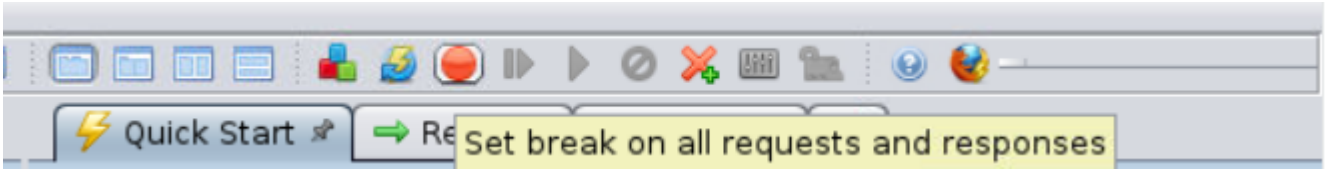
We are having this mutillidae which is a built in vulnerability application for practicing web pentesting

Raising the security level and testing the sql injection

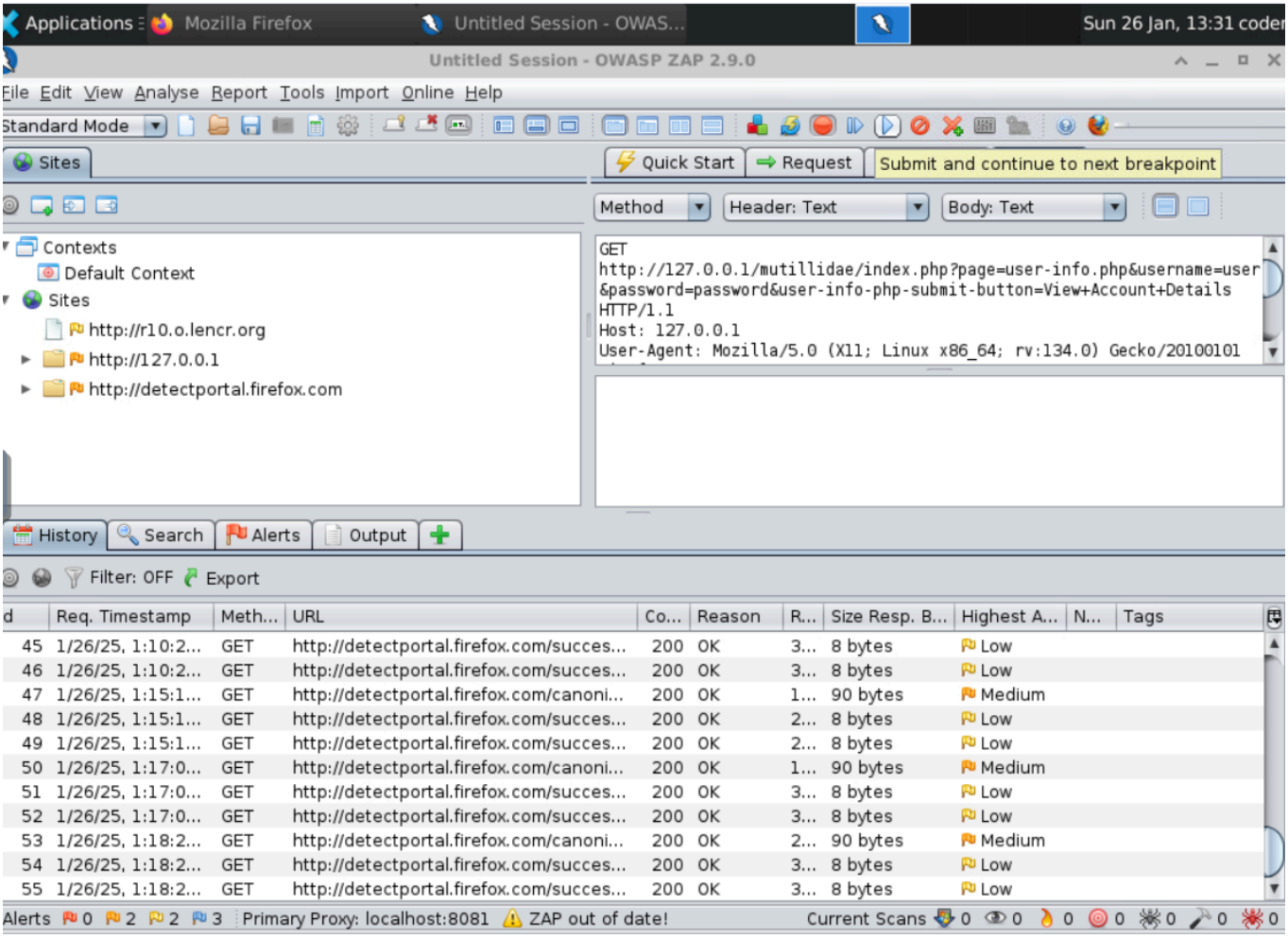


We can see the popup which is because of the client side validation to bypass this we need to break the request from going to the server by ZAP and change the Request we cannot see the req in our zap so we need to to bypass

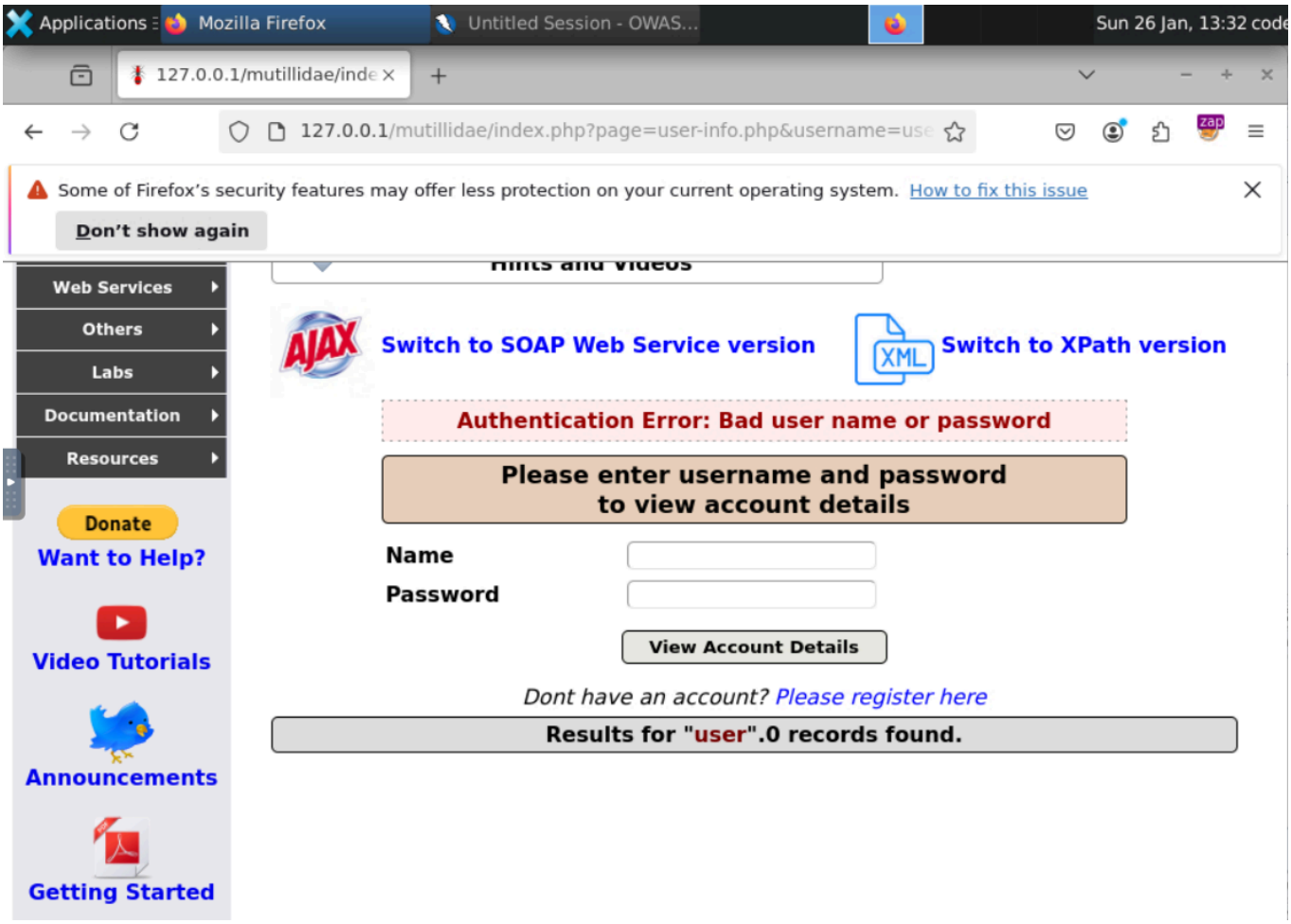
To do this we need to create a valid req and then intercept it with the ZAP proxy and we need to enable the request interception breakpoint within the ZAP



We can see a green button but hover over it it changes to red which is for setting up break on all req and responses

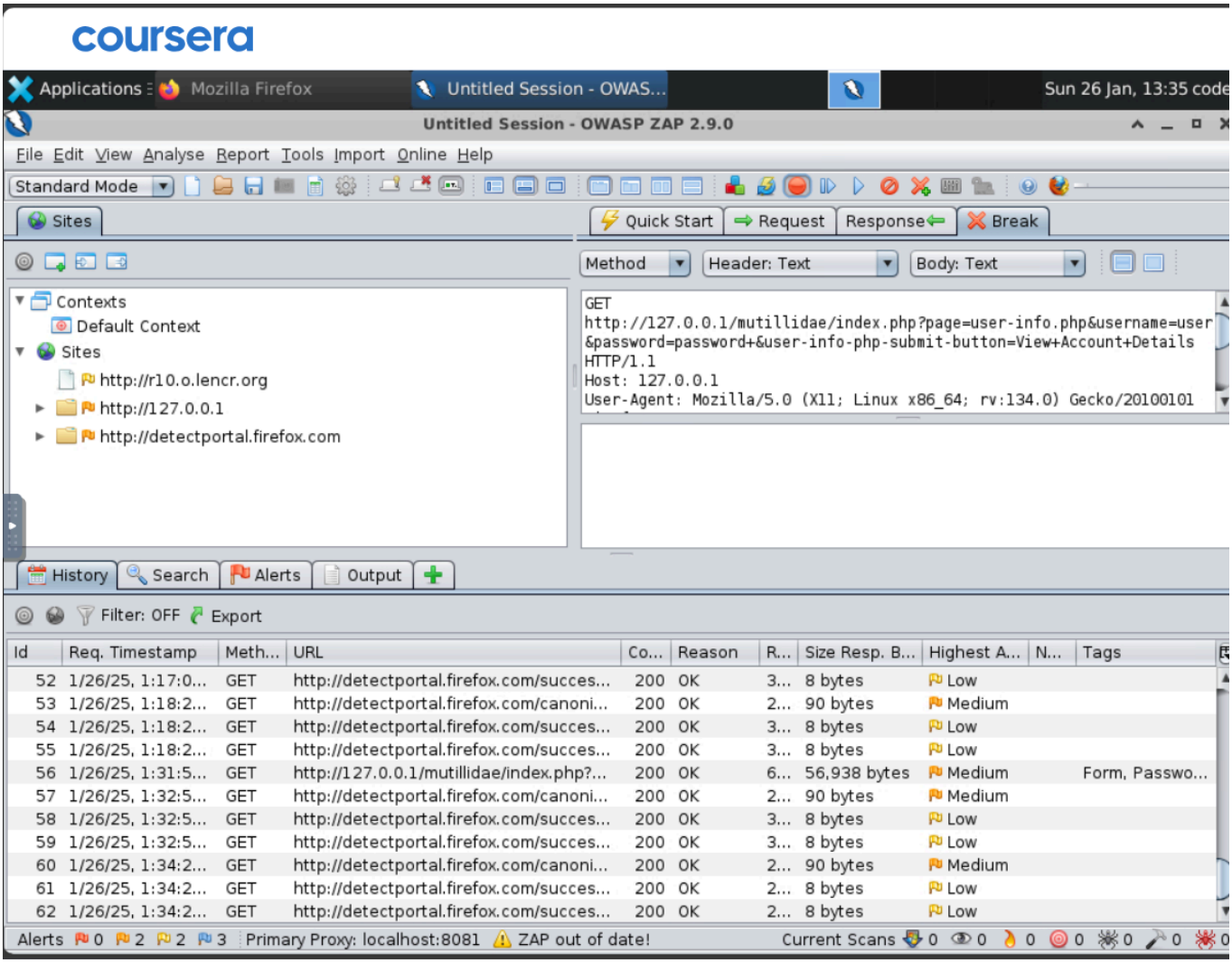


By pressing the play back button the req sends to the server



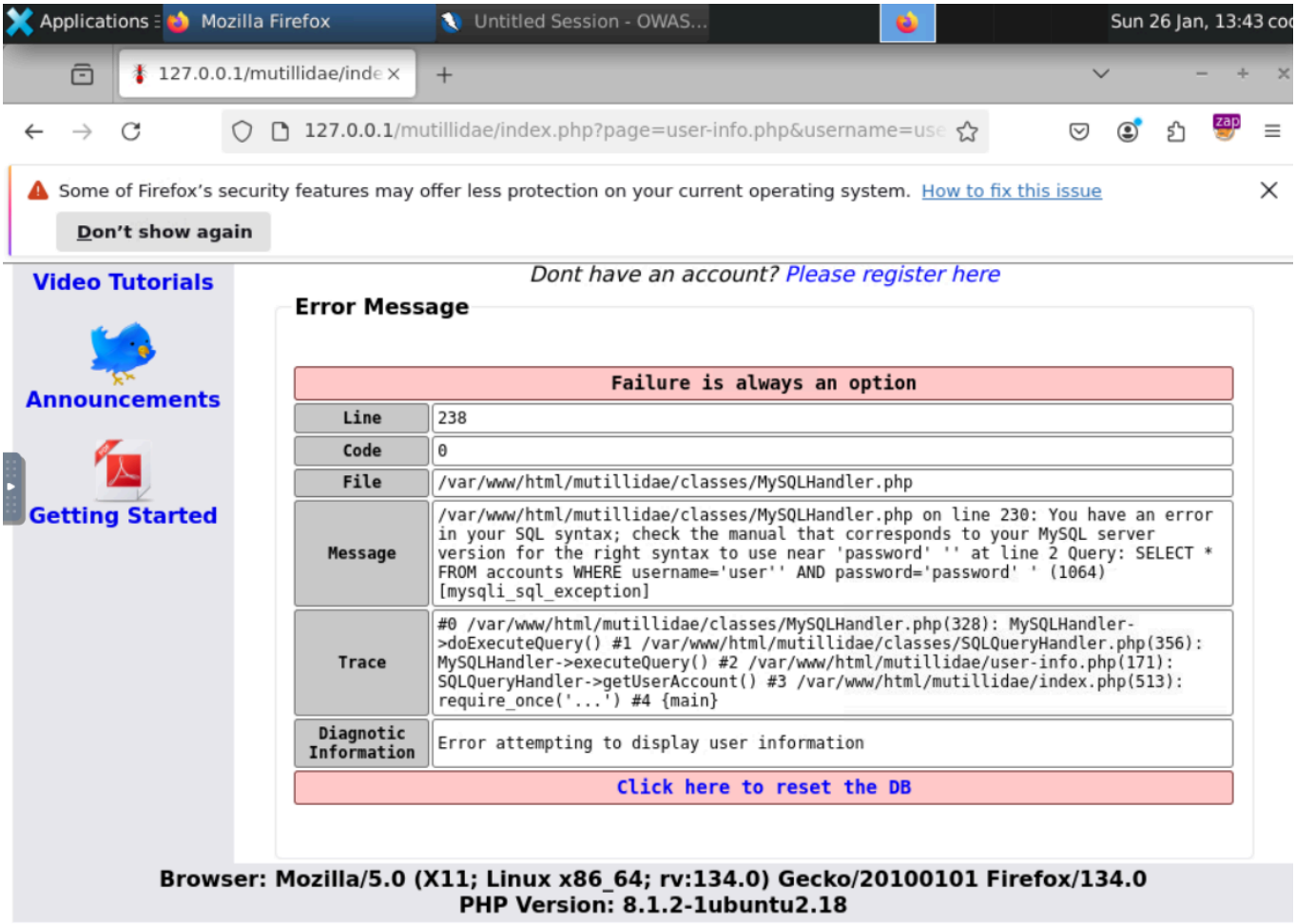
we can see a authentication error stating a bad username or password

Now again enter the valid name and password and do not press for view account details
Go to the ZAP and set the breakpoint and then send the req by pressing the view account details



Here we have intercepted the request which is bypassed the client validation by the application but have not sent to the server because we have stopped it

now unsetting the breakpoint and playing on the req and return with injecting special characters



we can see a new error this is because the server was unable to process the input correctly but we bypassed the client validation which stopped earlier however this is also a client validation but we bypassed some of the client validation
we can say that the web app cannot process the unexpected server side request correctly

By Using this we can understand how the web application works

Conclusion

OWASP ZAP a web security testing tool has various benefits not only the tasks done by me This tool is a Great tool to do penetration testing and reporting the web applications from intercepting the traffic and finding the links and URLs of the target web application and a spider to crawl the website and finding the directories and altering the requests and analyzing the responses and checking for vulnerabilities