Practical – 9

Demonstrate Application Injection using Zed Attack Proxy.

Q. What is Zed Attack Proxy?

Zed Attack Proxy is an open-source security software written in Java programming language and released in 2010. It is used to scan web applications and find vulnerabilities in it. It was started as a small project by the Open Web Application Security Project (OWASP) and now it is the most active project maintained by thousands of individuals around the globe. It is available for Linux, Windows, and mac in 29 languages. It can also be used as a proxy server like a burp suite to manipulate the request including the HTTPS request. Daemon mode is also present in it which can later be controlled by REST API.

Features:

-
- Passive Scanner
- Automated Scanner
- Proxy Server
- Port Identification
- Directory Searching
- Brute Force Attack
- Web Crawler
- Fuzzer

Q. Why do we use Zed Attack Proxy?

Zed Attack Proxy is used to detect vulnerabilities present on any web server and try to remove them. Here is some big vulnerability that could be present in the web server:

- SQL injection
- Cross-site scripting (XSS)
- Broken access control
- Security miss-configuration
- Broken authentication
- Sensitive data exposure
- Cross-site request forgery (CSRF)
- Using components with known vulnerabilities.

Some Important Terminologies:

Proxy Server:

It is a server that acts as a mediator for clients who want to go through the request and want to alter them.Cyber Security

Spider:

It is a type of information gathering process in which the application in this case ZAP will go through the whole web page and try to find out all the links and other important details.

Passive Scan:

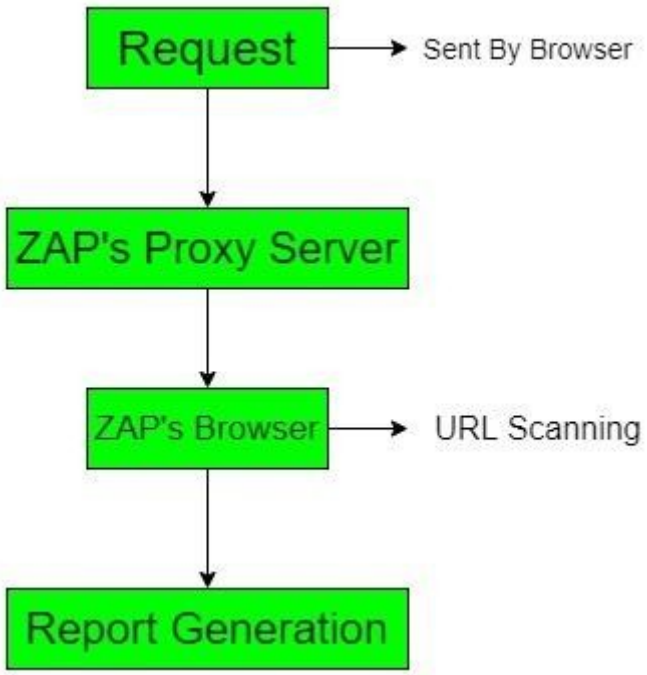
In this type of scanning the vulnerability is detected without getting in direct contact with the target machine.

Active Scan:

In this, the vulnerability is detected by getting in direct contact with the target machine which makes it very easy to be detected by the administrator.

Working Process:

First we set up the proxy server with any browser. The browser sends website data to the proxy server and then the browser inside the ZAP processes the request and perform attacks and generates the report.

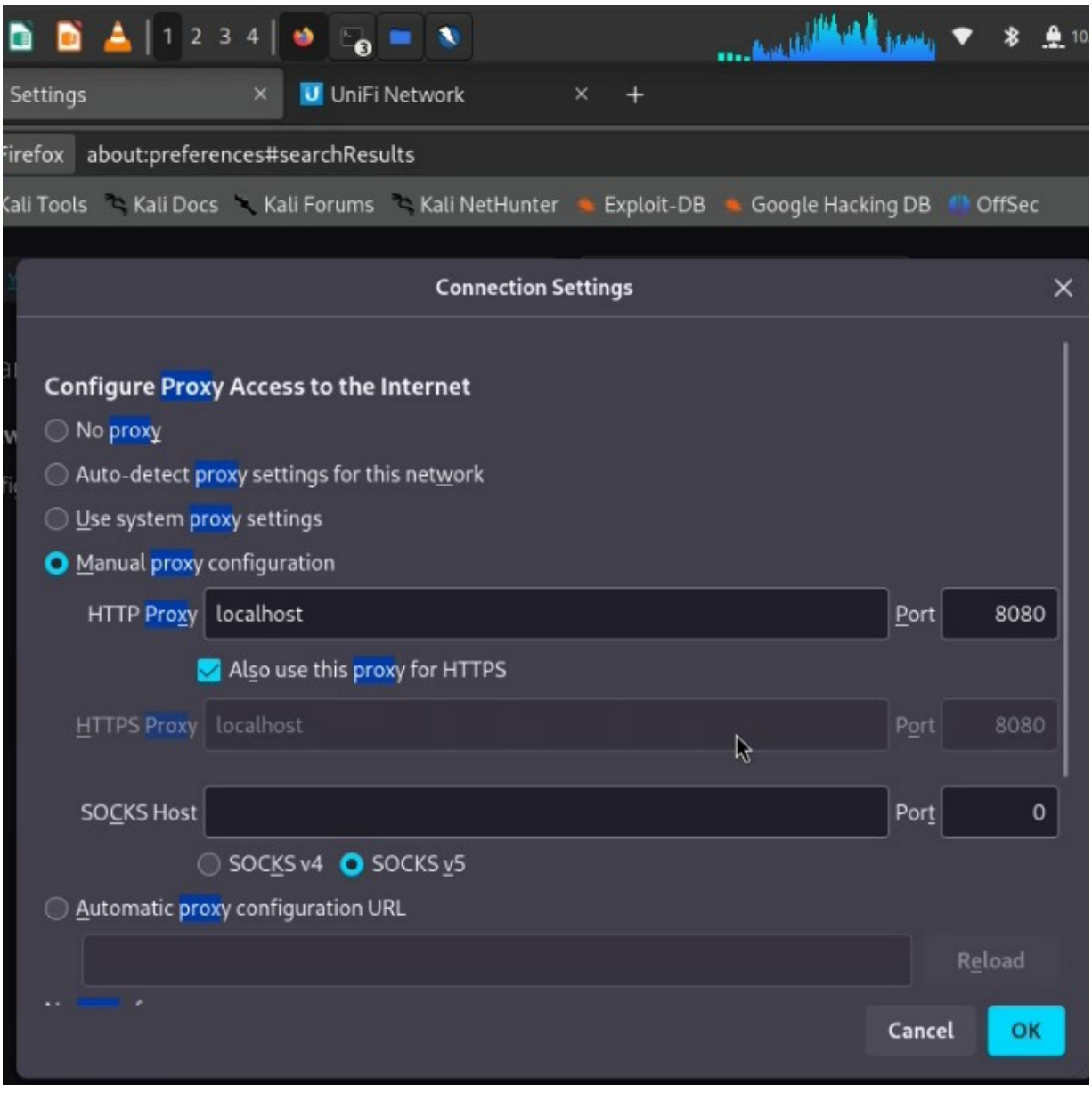


Note :- In Kali Linux ZAP is pre installed

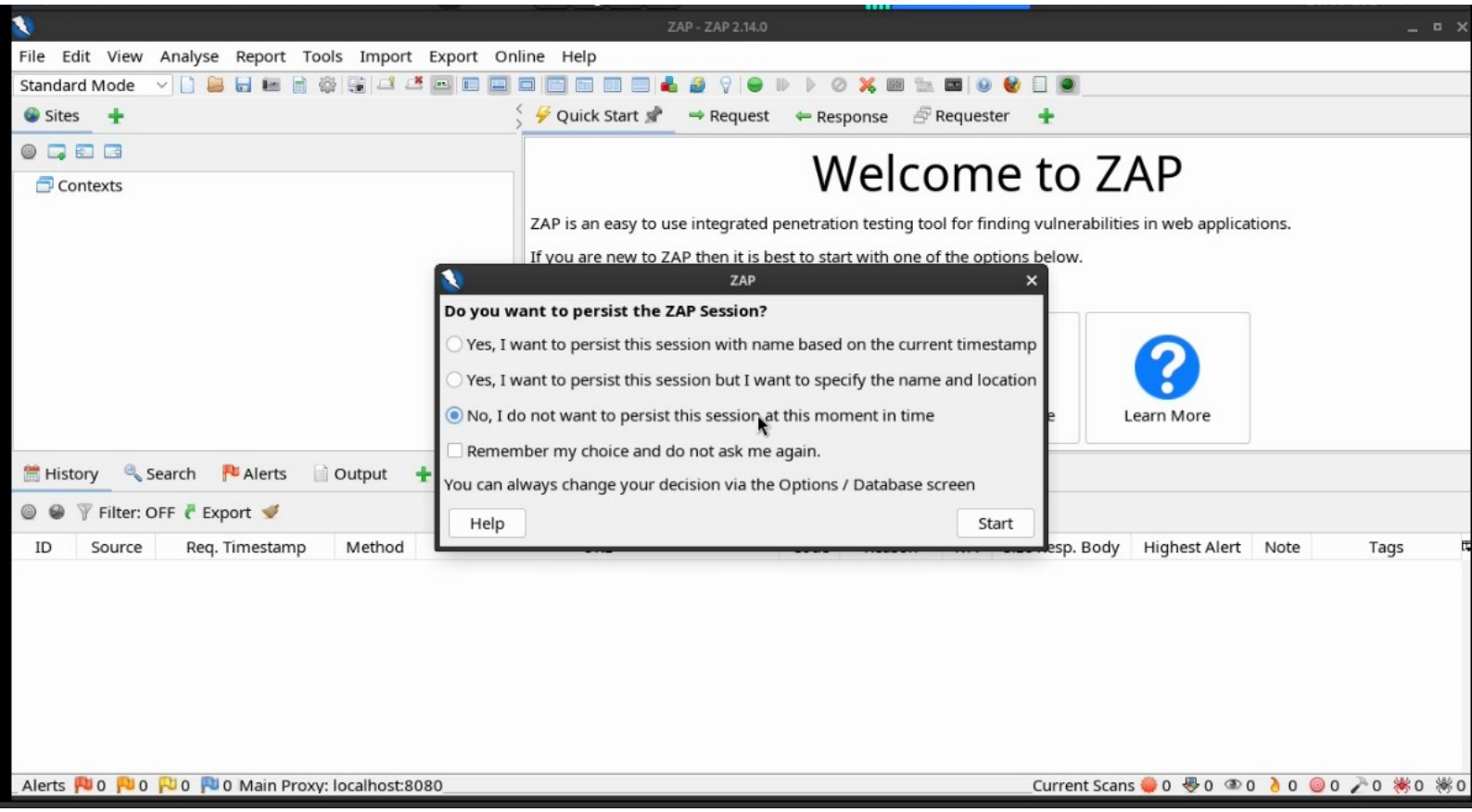
Step 1 :- Open ZAP Using Terminal it can also be opened without terminal bysearching it in Application Menu

command to open using terminal is :- owasp-zap

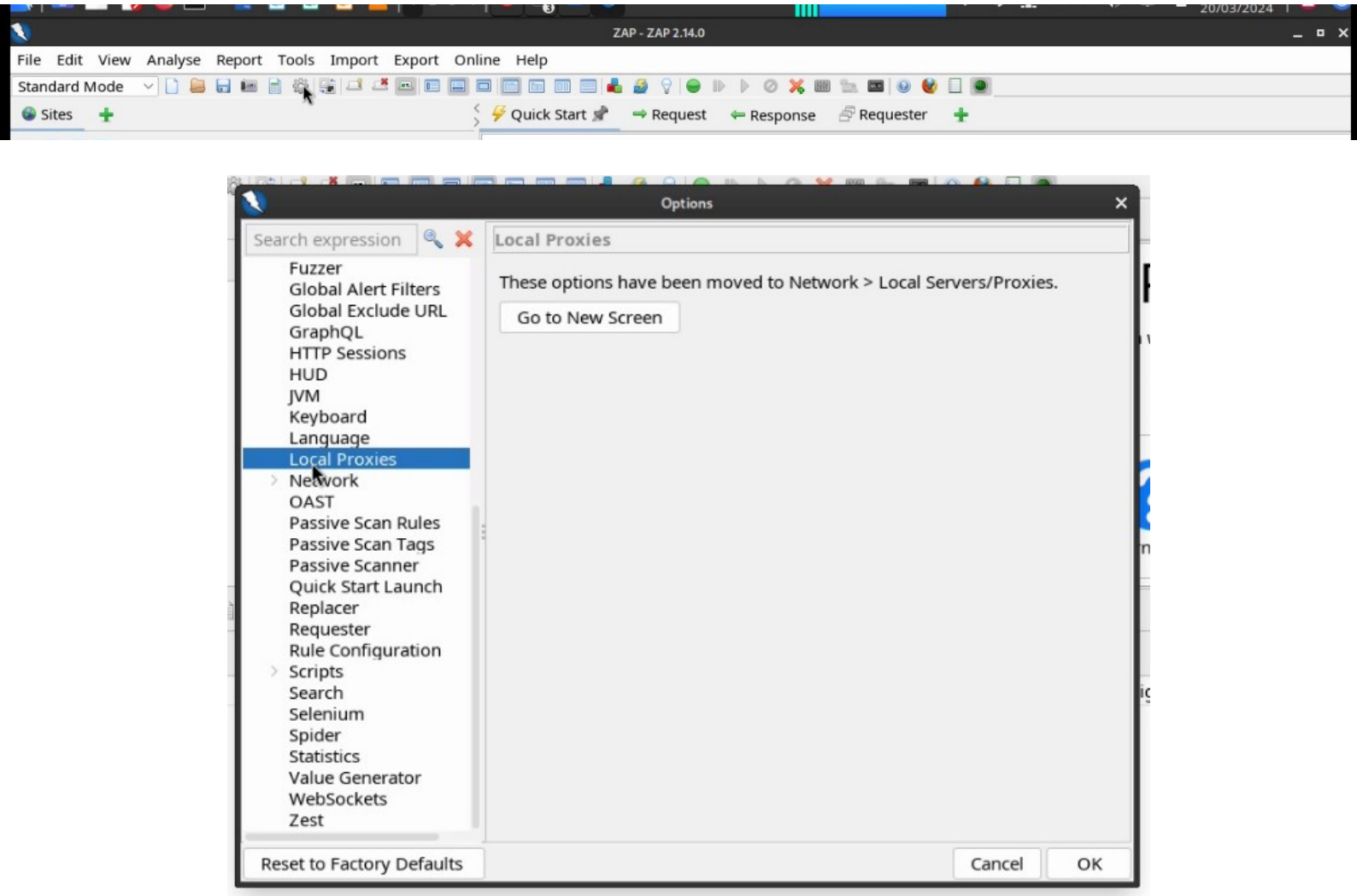
Step 2 :- Till ZAP opens open your browser go to **Settings** in search box type **“proxy”** and do following configuration but keep settings open after doing it



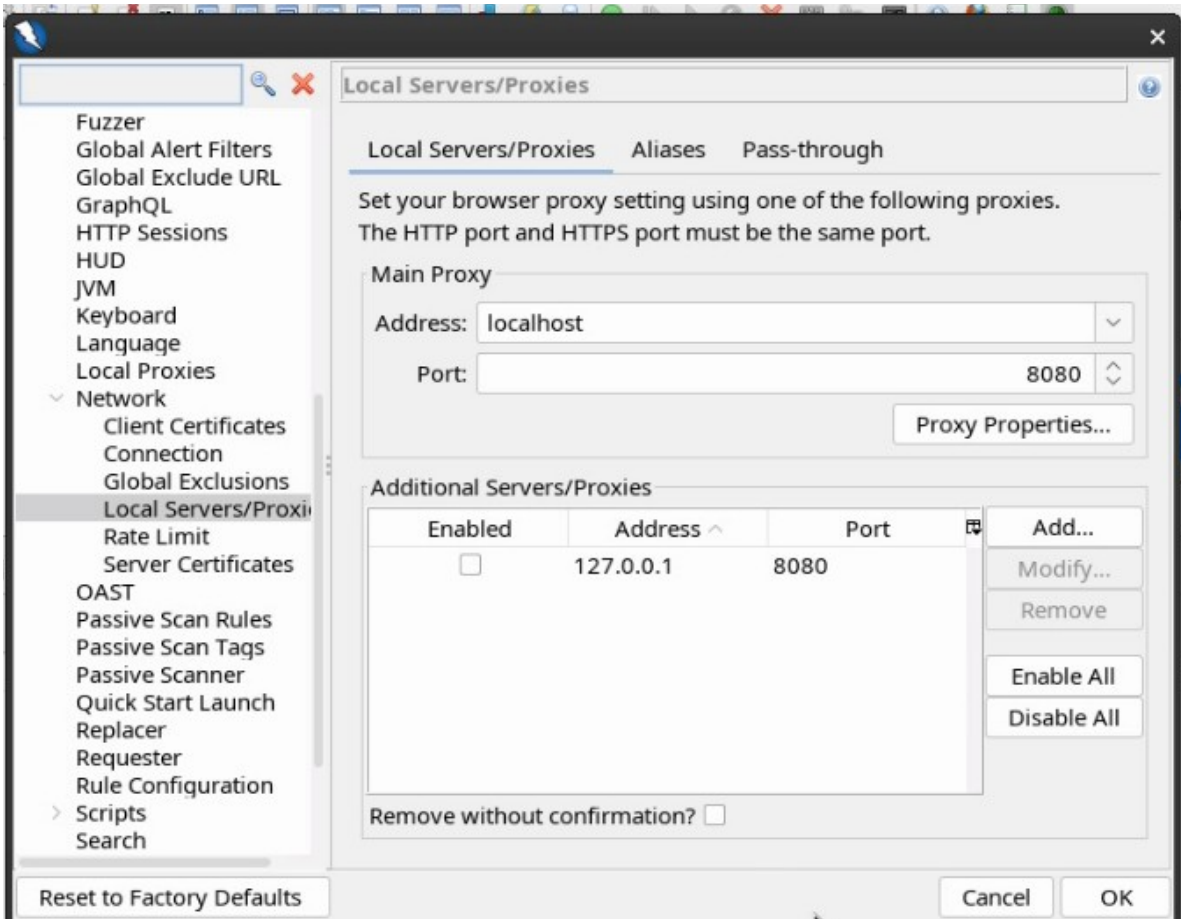
step 3 :- After ZAP opens select 3rd option as followes

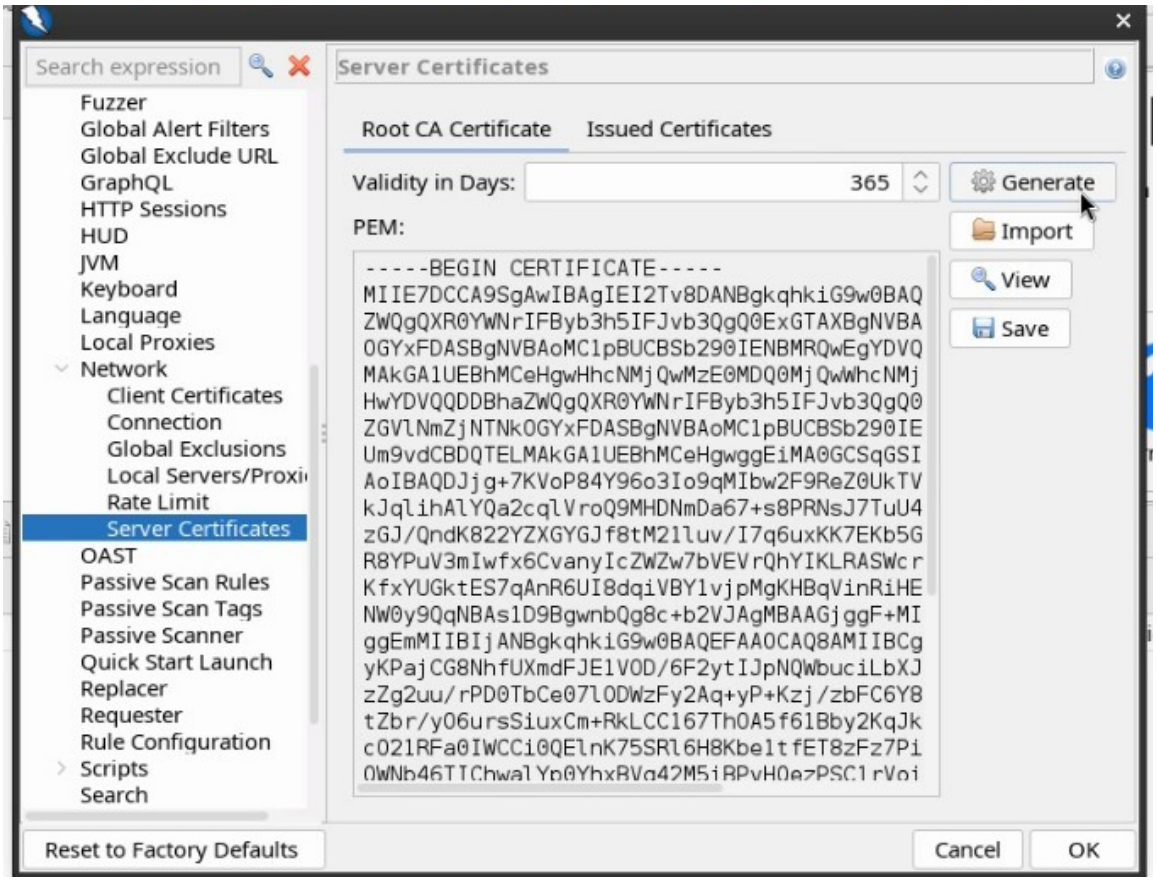


Step 4 : Do following configurations.



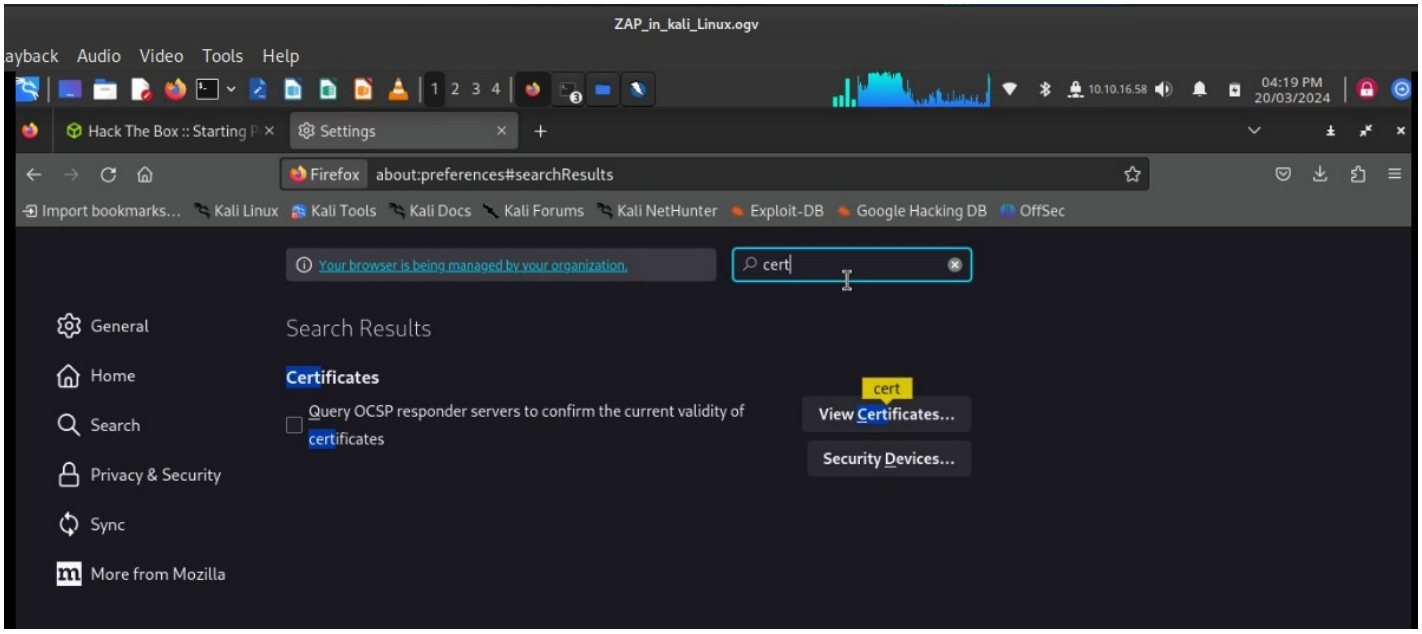
Click Go to New Screen

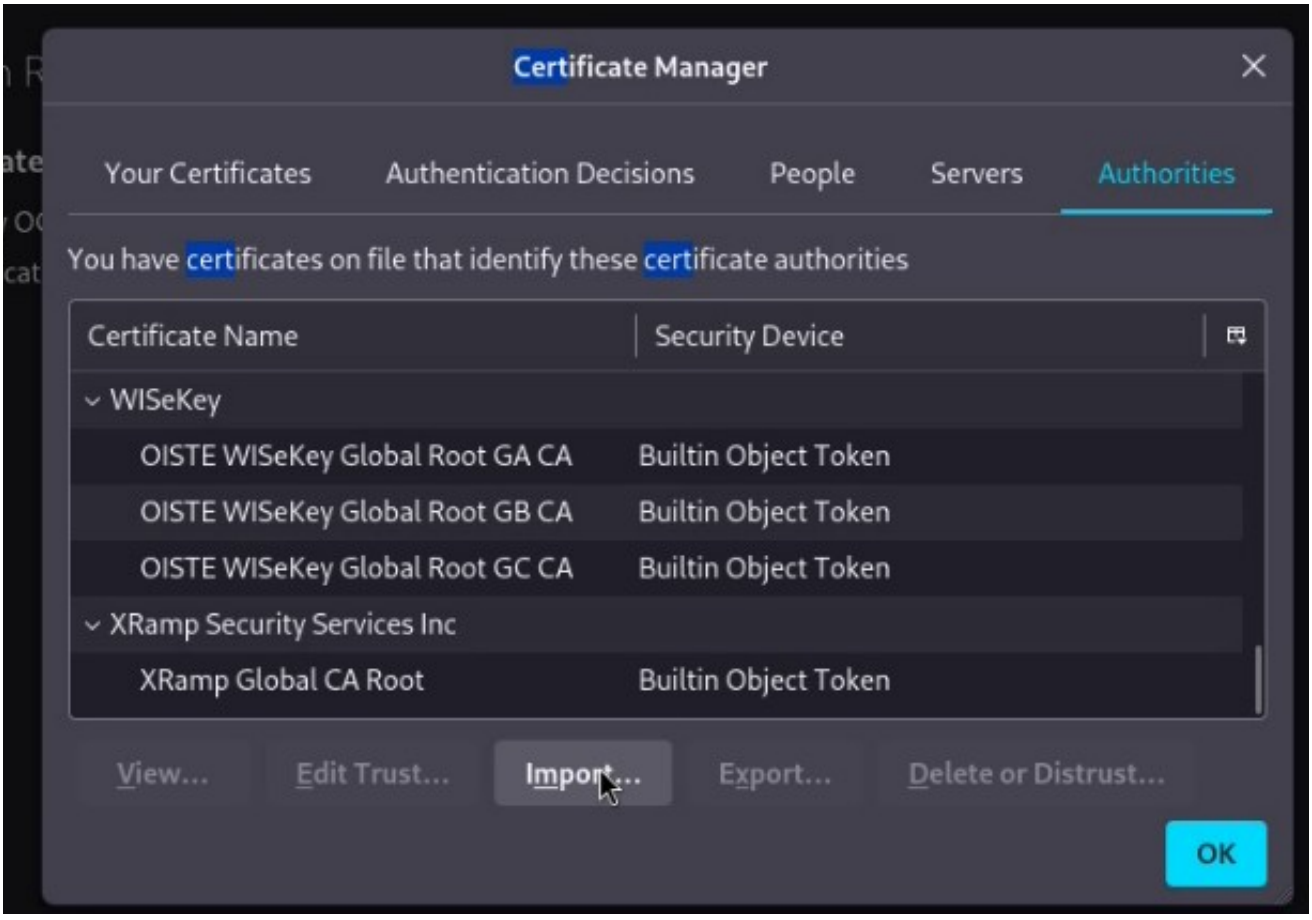


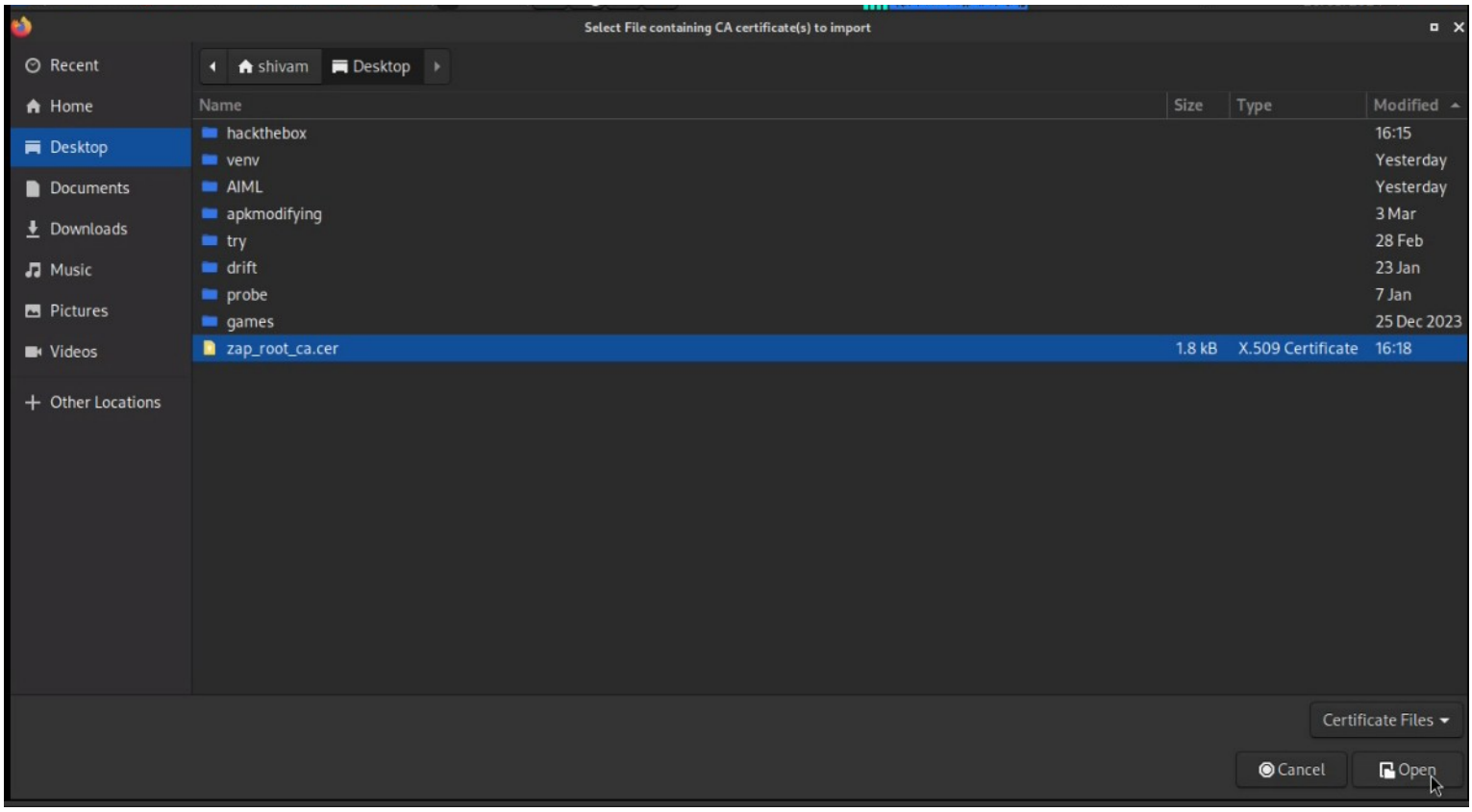


Go to Server Certificates in Network & Click Generate and then Save it.

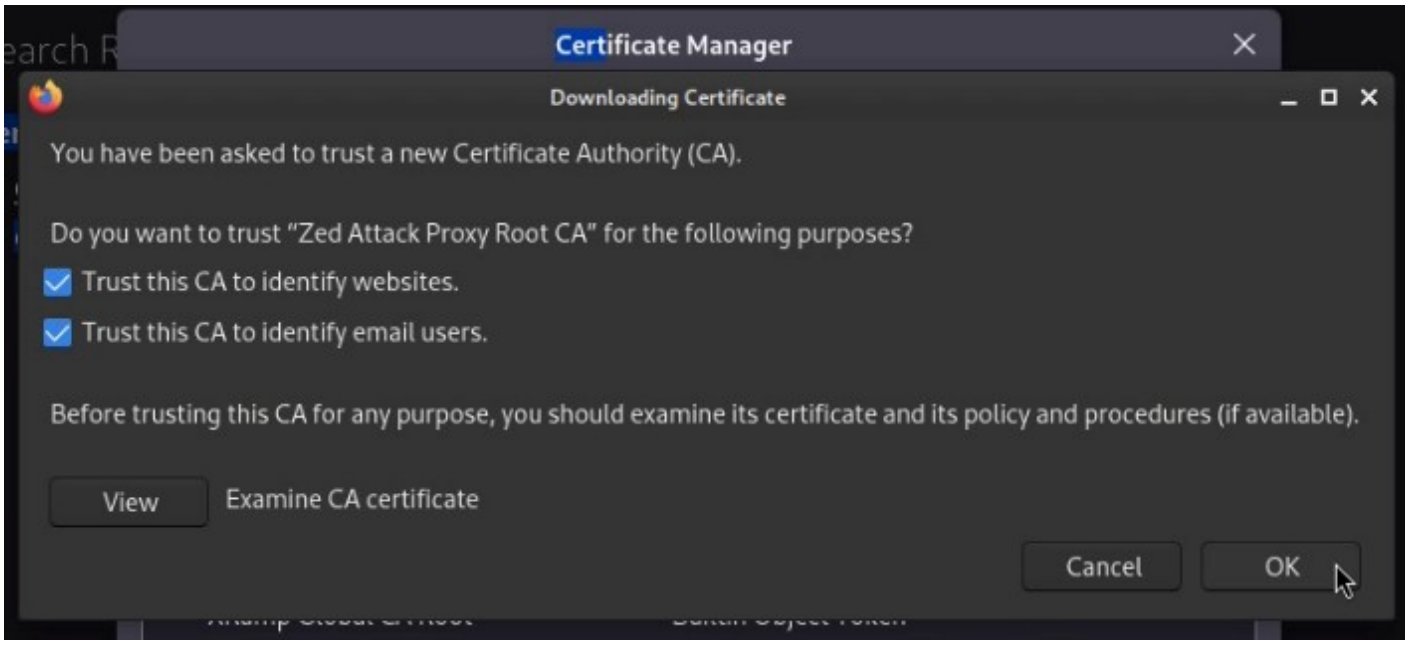
Step 5 :- In Browser Settings Type **“certificates”** in search box and add the zap certificate which we saved in previous step





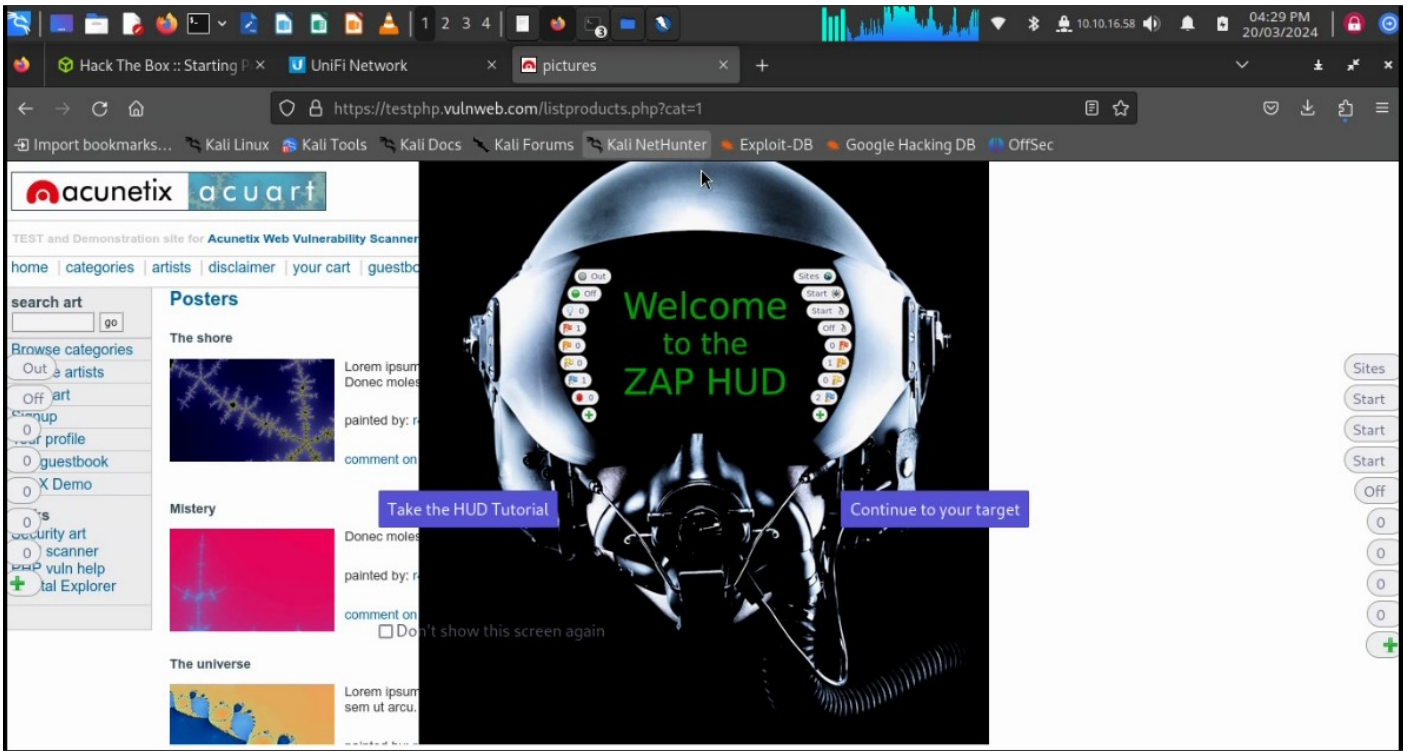


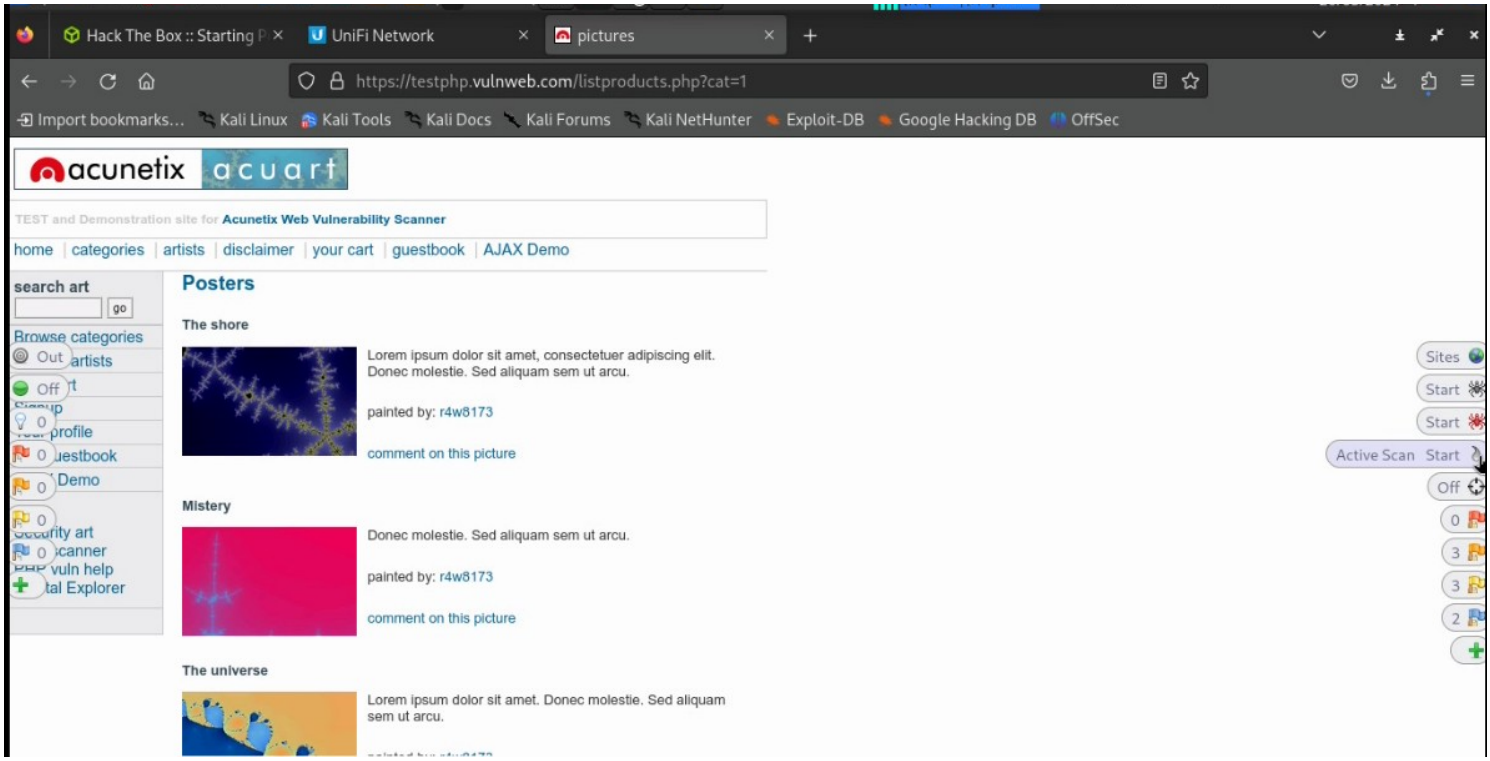
Open the saved certificate after clicking Import



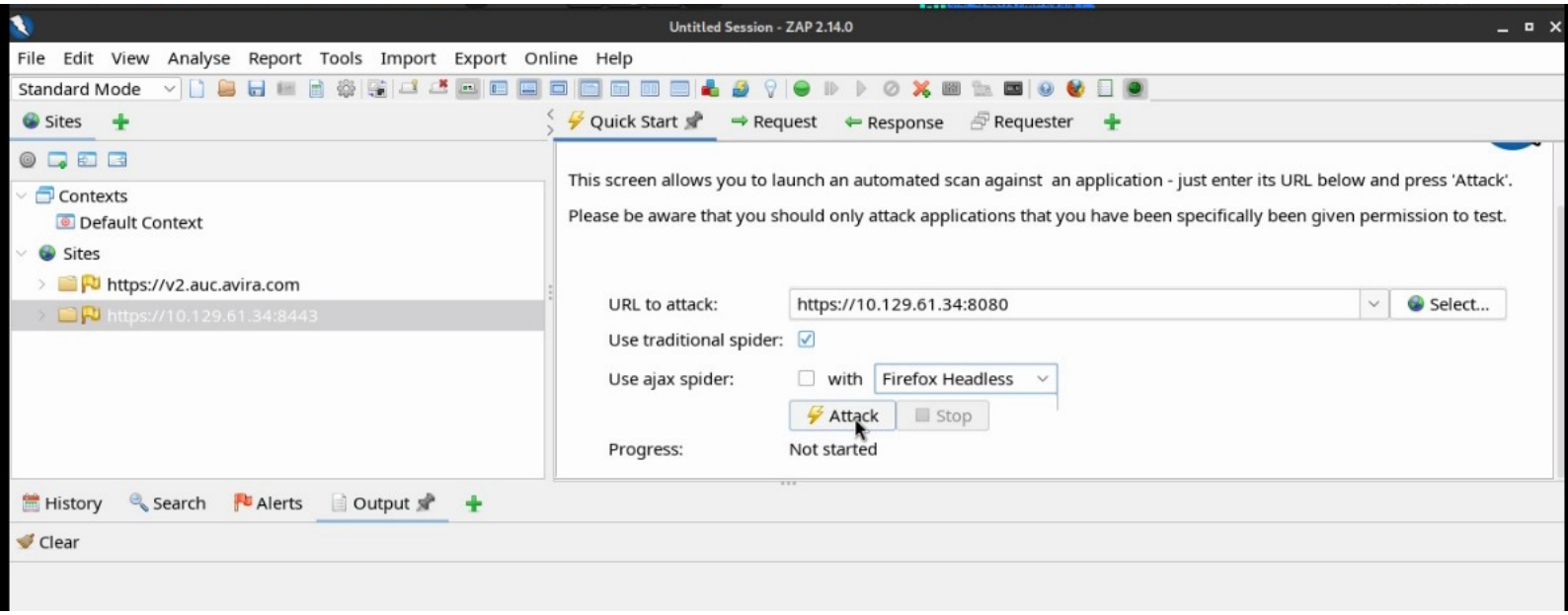
Trust the certificate and then click OK then close Certificate manager by clicking OK

Note :- When you now browse any page like above given link you will see HUD of ZAP in browser Choose to Continue to your target and start an Active Scan

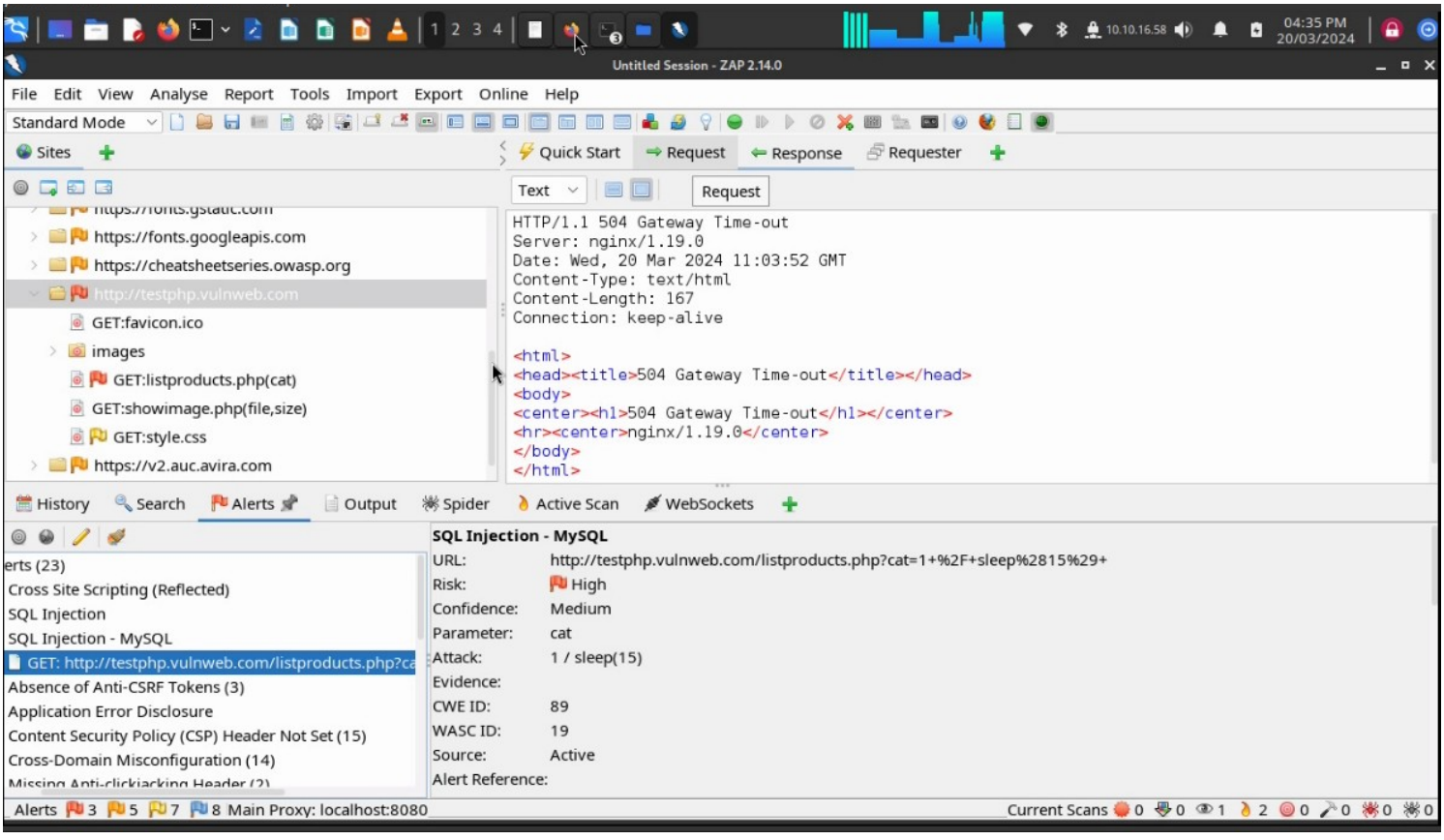




If HUD Don't start you can add that site in Automate Scan in ZAP and click Attack option



The Zap & its HUD has one RED FLAG symbol which shows Alerts i.e. alerts of vulnerabilities present in site



Hence our ZAP is completed