

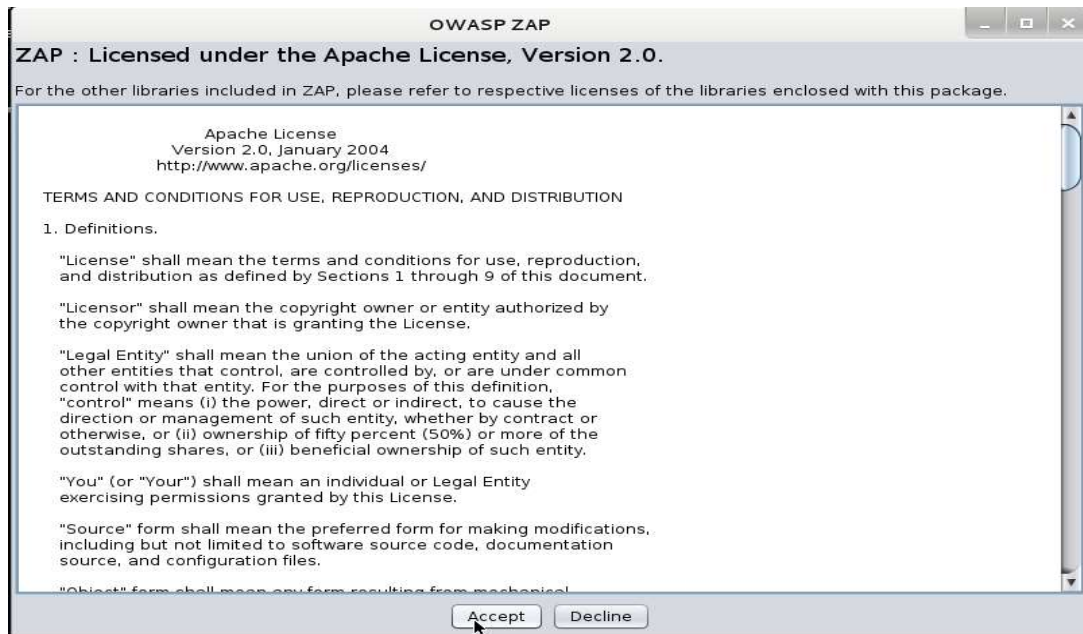
## Practical – 9

### Aim: Demonstrate Application Injection using Zed Attack Proxy

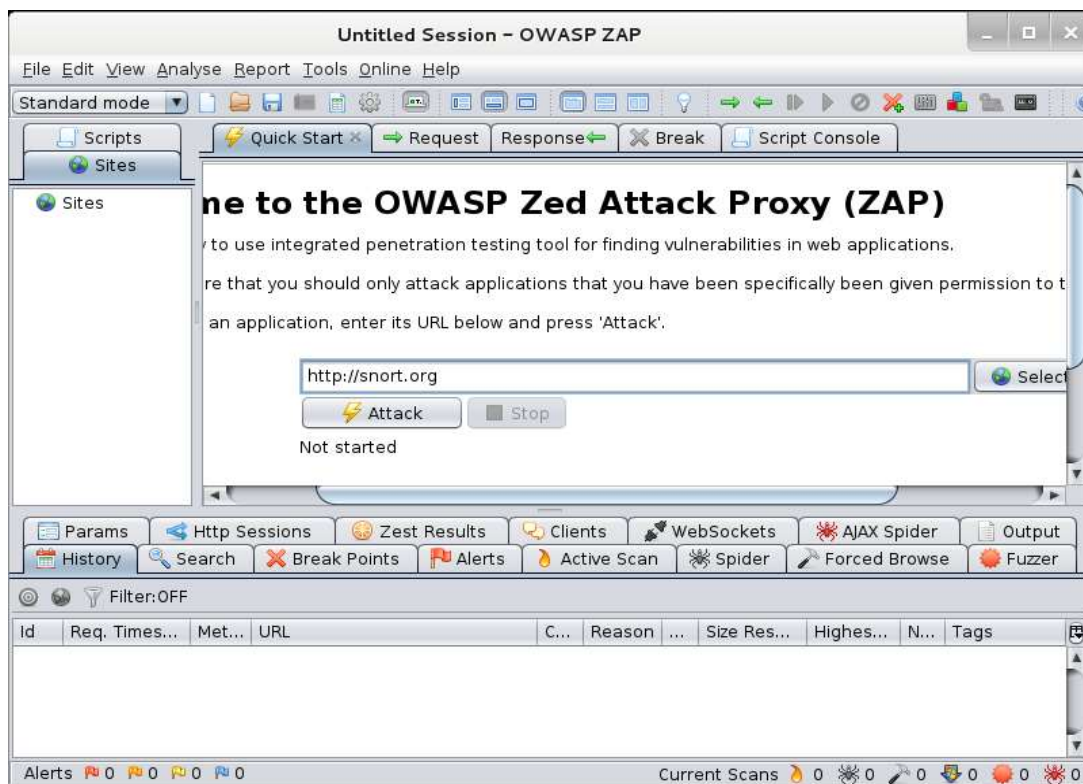
- OWASP ZAP is a web application penetration testing tool that has some great features. It is a very easy to use scanner that allows you to do manual or automatic website security checks. In this tutorial we will learn how to use the automatic attack feature.
- This open-source tool was developed at the Open Web Application Security Project (OWASP). Its main goal is to allow easy penetration testing to find vulnerabilities in web applications. It is ideal for developers and functional testers as well as security experts.
- **Zed Attack Proxy Features**
  - Intercepting Proxy
  - Automated Scanner
  - Passive Scanner
  - Brute Force Scanner
  - Fuzzer
  - Port Scanner
  - Spider
  - Web Sockets
  - REST API
- **Start OWASP ZAP:**  
Applications>Web Applications > Web Application Proxies >owasp- zap.



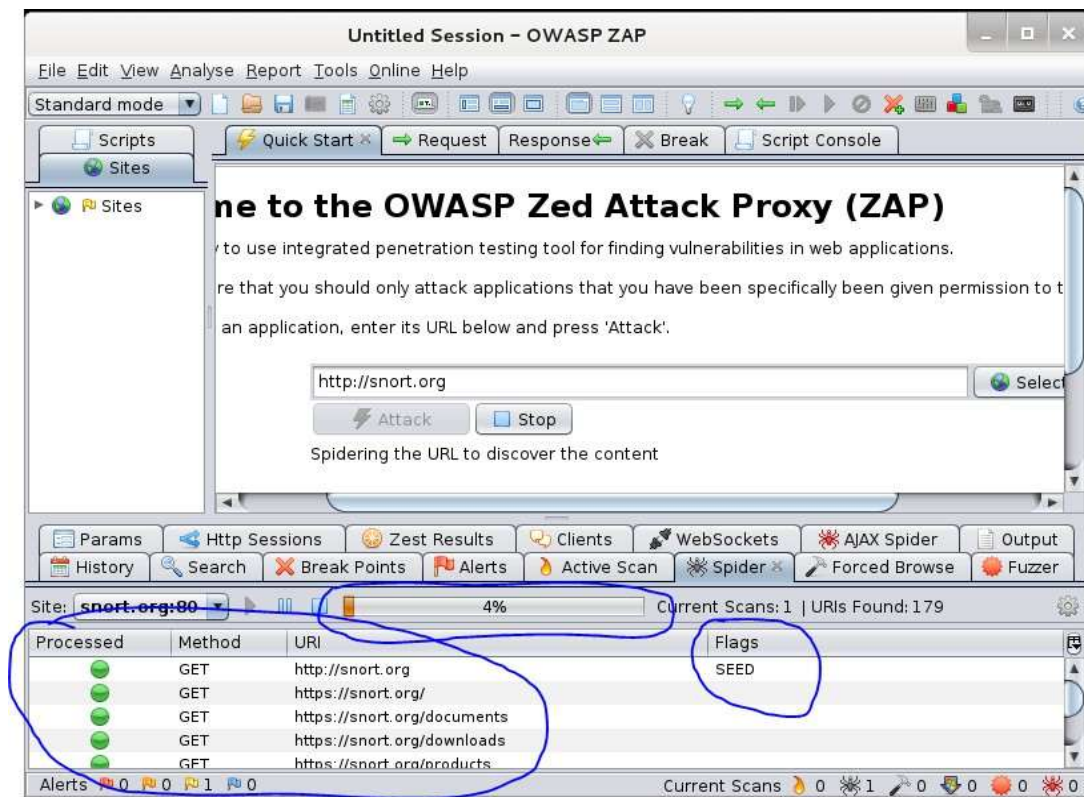
After clicking on owasp-zap it ask for license agreement and we have to accept it.



Now it shows the main window of owasp-zap tool in which user have to insert **ip address** or **URL** for scanning.



After inserting URL click on “Attack”



The scanning process is started with the click and it shows the scanning status and current status in spider section.

It will also list any security issues it finds and place them under the “Alerts” tab. Clicking on the tab will show the following alerts:



We can also examine the alerts which are listed in the alert window and it shows all the details about the URL path risk reliability Parameter attack evidence etc.

