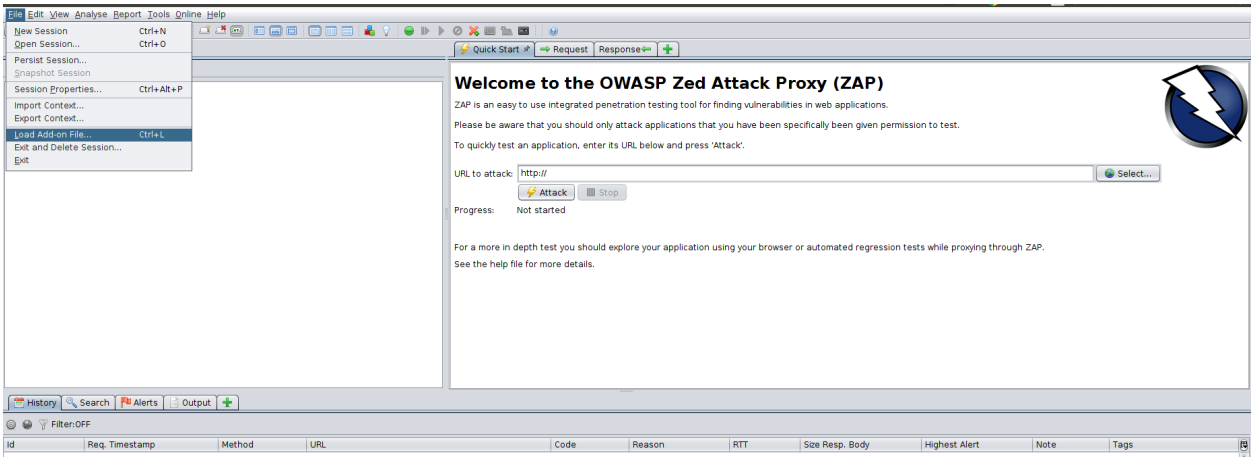
Using Retire.js with ZAP to identify vulnerabilities in JavaScript libraries

Prakhash Sivakumar Follow
Sep 7, 2016 · 2 min read

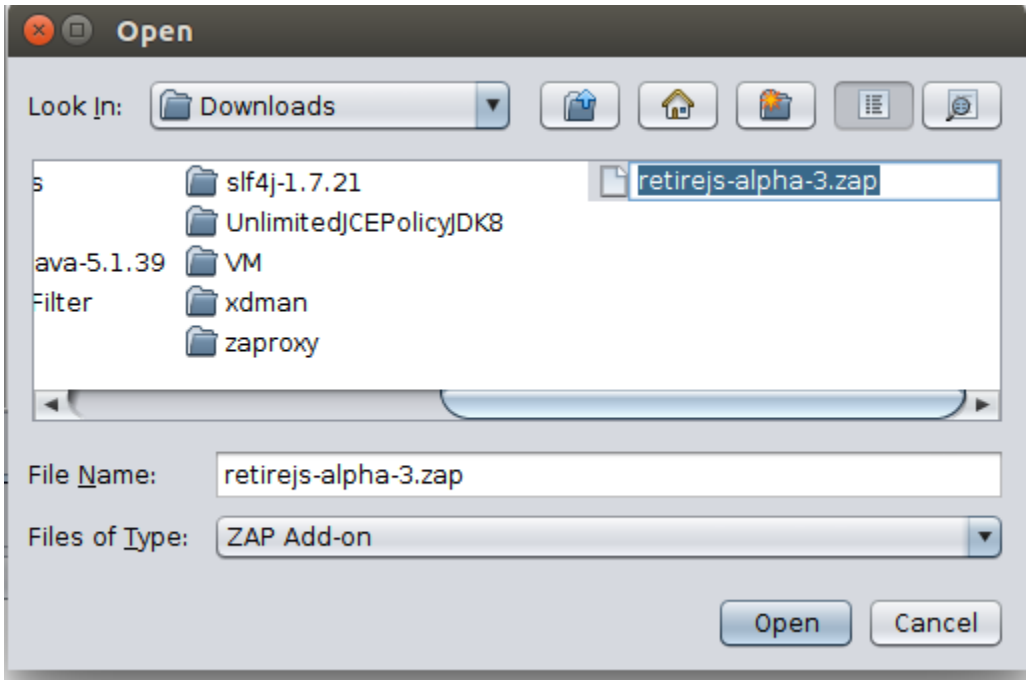
Download the Retire add-on for ZAP from here.

1. Go to **File -> Load Add-on File** and load the add-on to the ZAP



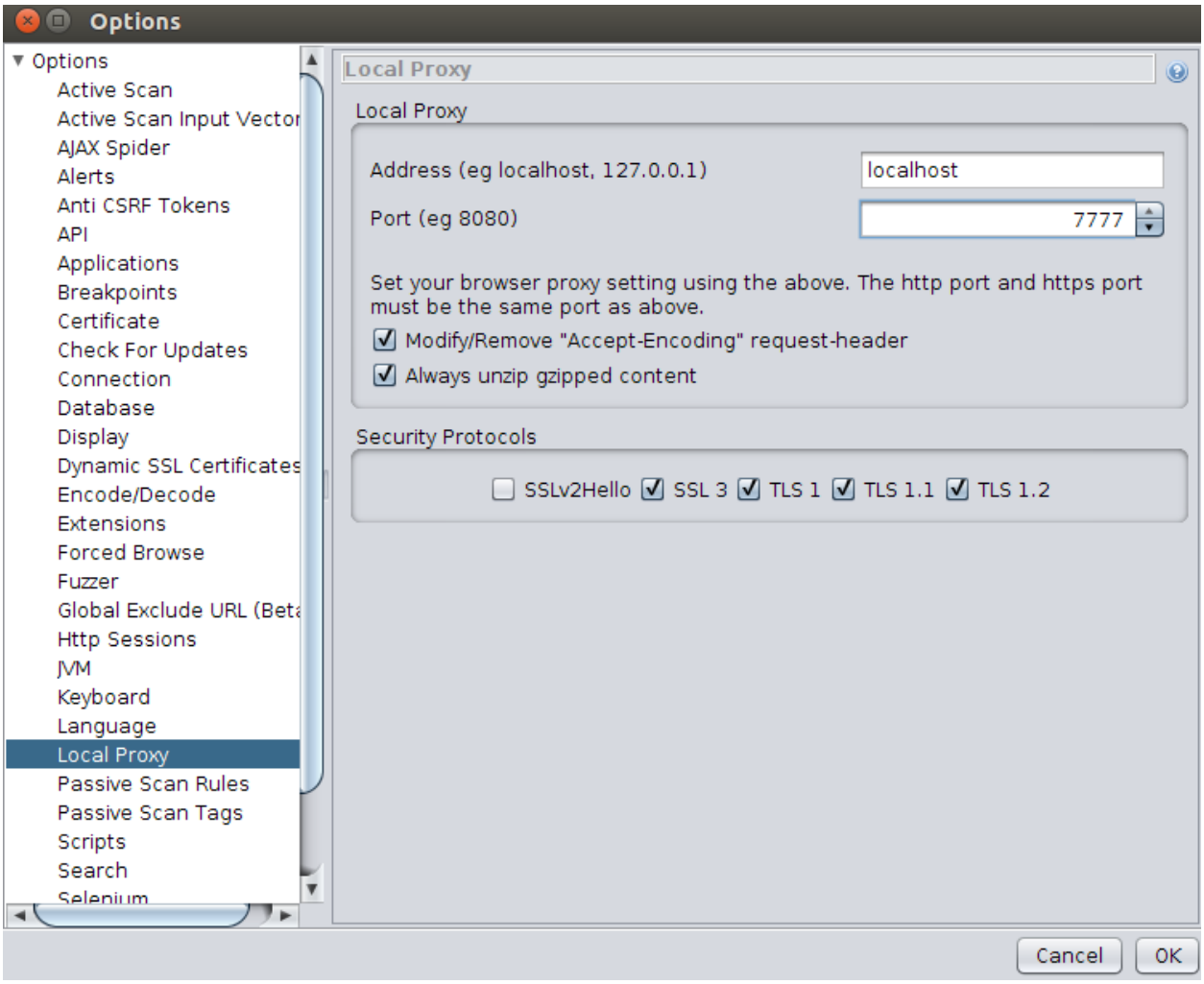
2. Currently the alpha version of retirejs is released by the community for the ZAP, Click onthe **retirejs-alpha-3.zap** and update the ZAP with the add-on by click open.(You won't be able to observe any UI changes after adding the add-on but you can verify the update by

checking **/home/<NAME>/.ZAP/plugin** folder.)



Configuring ZAP Proxy to Trace Browser Traffic

3. Go to **Tools → Options → Local Proxy** and set the hostname/ip address and the port number for the proxy. *(In this example, the port is set to 7777 which is selected randomly)*

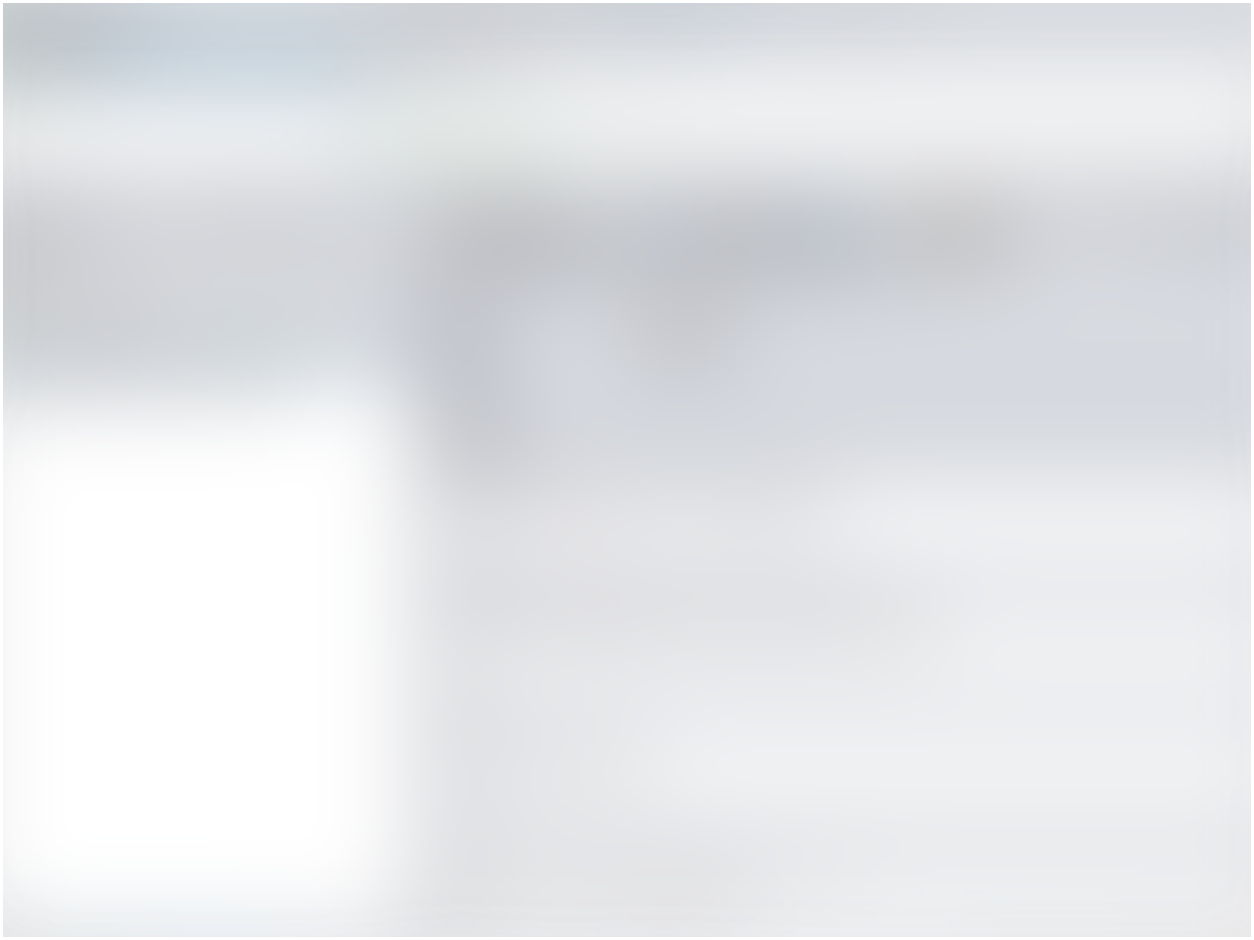


4. Now ZAP tool is ready to capture the traffic going through the above set port number. Next step is to configure the browser to send traffic through this port number so ZAP tool can trace them. In Firefox, go to **Edit → Preferences** and in the **Advanced** options, click on **Settings** under the **Network** tab.

Select the **Manual proxy configuration** and set the hostname/ip and the port number.

5. Now, go to Firefox and access the your application. You will see the traffic goes through ZAP proxy.

Continue the scanning, you will observe the reported JavaScript vulnerabilities under the **Alerts** tab



References

[1] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
[2] http://retirejs.github.io/retire.js/