Steps:

1. Install OWASP-ZAP UI from (URL: <https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>)
2. Install pip and then python from (URL:

<https://en.wikipedia.org/wiki/Pip_(package_manager)> )

1. Install python-owasp-zap by typing command

pip install python-owasp-zap-v2.4

1. Install Docker or Docker Toolbox for Windows from (URL: <https://docs.docker.com/engine/getstarted/step_one/>) which can be useful for Continuous Integration and running shell scripts. Docker for Windows runs as a native Windows application and uses Hyper-V to virtualize the Docker Engine environment and Linux kernel-specific features for the Docker daemon.
2. Configure browser to ZAP – i.e., Go to Network – LAN Settings and enable Use a Proxy Server by typing Address: localhost, Port: 8090.
3. Start ZAP in daemon mode by going to OWASP/Zed Attack Proxy directory and using command - “ *./zap.sh -daemon -port 8090 -host localhost -config api.apikey = '****APIKEY****' &* “ so that ZAP will listen/Proxy the URL’s  
   **APIKEY** will be generated in OWASP-ZAP UI tool Under Tools-Options-API and enable Autofill API key in the API UI. API key is required to generate report.
4. Go to regression tests directory and start regression test-suites. For e.g. Start nightwatch or selenium or any other automated regression tests. For nightwatch its just typing command - “*nightwatch*”   
   ZAP will proxy all the URL’s regression tests will be exploring.
5. Once done, go to ZAP Scan python scripts directory and Run spider & scan automated scripts to generate the vulnerability report.

**Files:**

zap\_spider\_scan\_report.py : Contains Python Script to spider, scan and generate report mentioned in step 8.

zap\_automate.sh : Shell script to execute steps 6 to 8.