Get Started: ZAP ASVS Scripts

In-depth instructions and demonstration can be found on Vimeo.

Clone the Repository

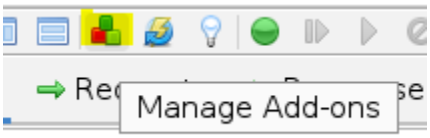
Link to our Repo: https://github.com/YaleUniversity/ZAP_ASVS_Checks

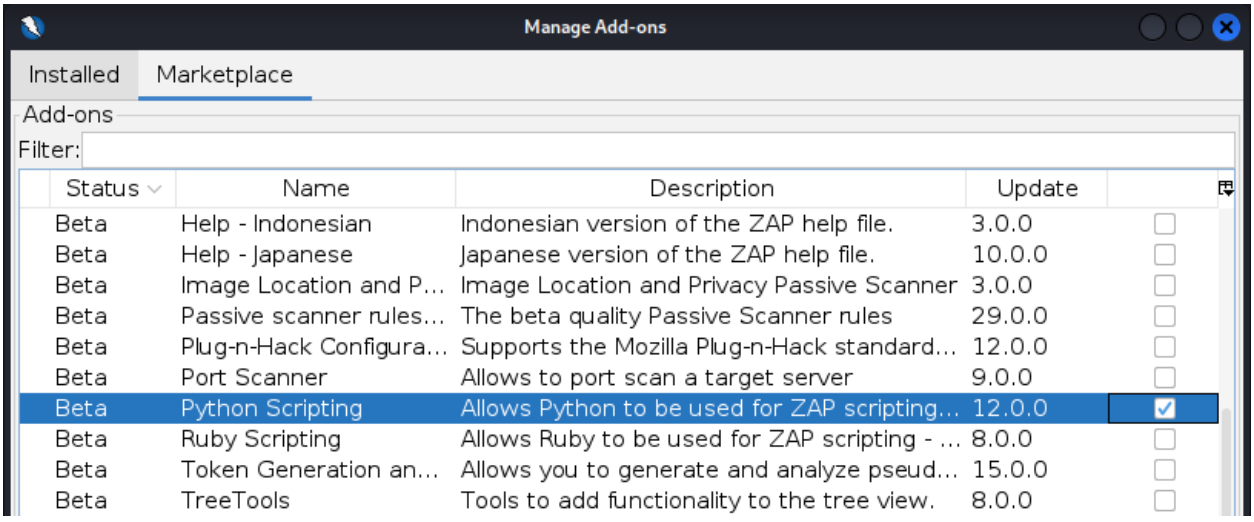
To clone the repo, enter the following command in your terminal

```
git clone https://github.com/YaleUniversity/ZAP_ASVS_Checks.git
```

Install Jython

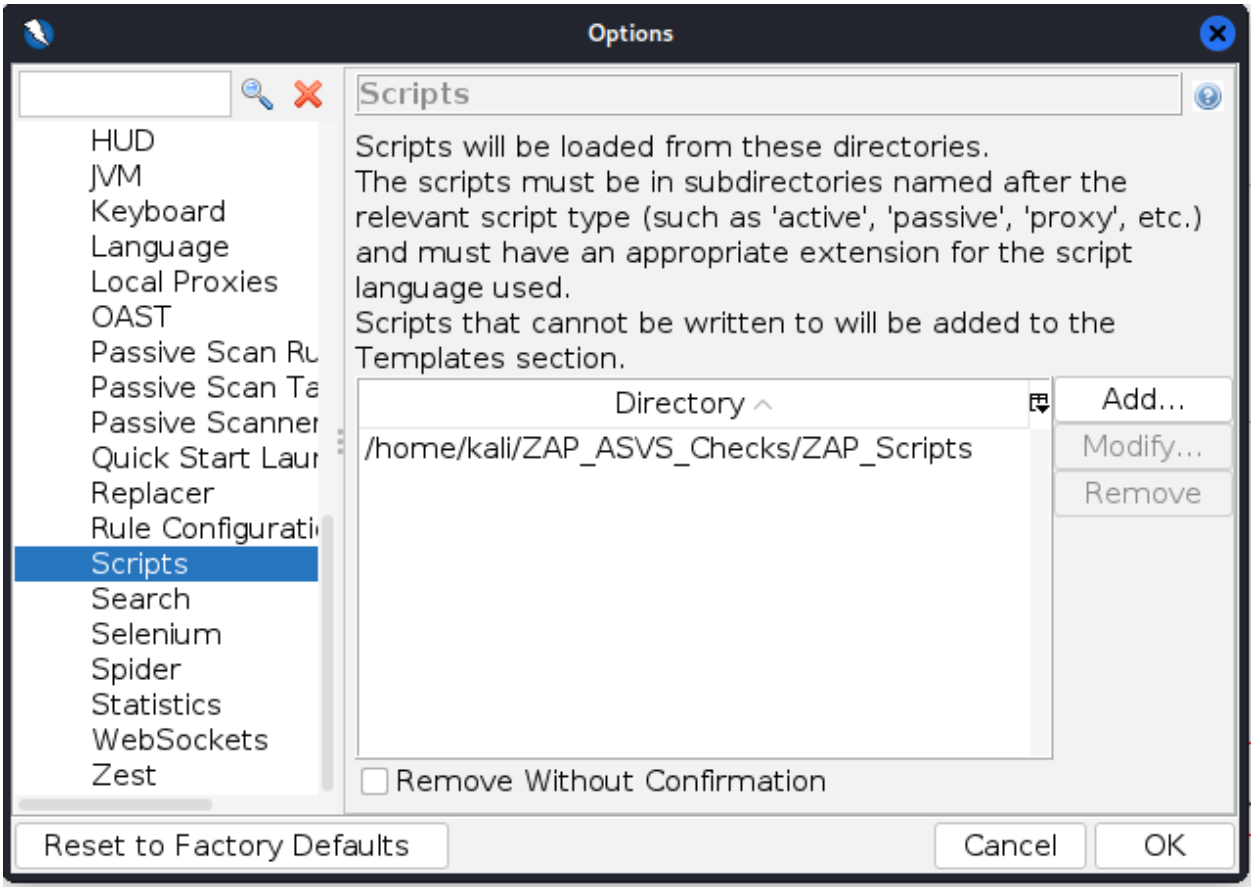
From the Zap Marketplace (tri-color squares icon), install the python scripting add-on. Once installed, you can ensure it was installed properly if the Jython tab appears in the Options menu located in Tools > Options.





Import Scripts

From Tools > Options > Scripts select Add. Choose the file path on your machine for the ZAP_Scripts folder. For example, my path is /home/kali/ZAP_ASVS_Checks/ZAP_Scripts

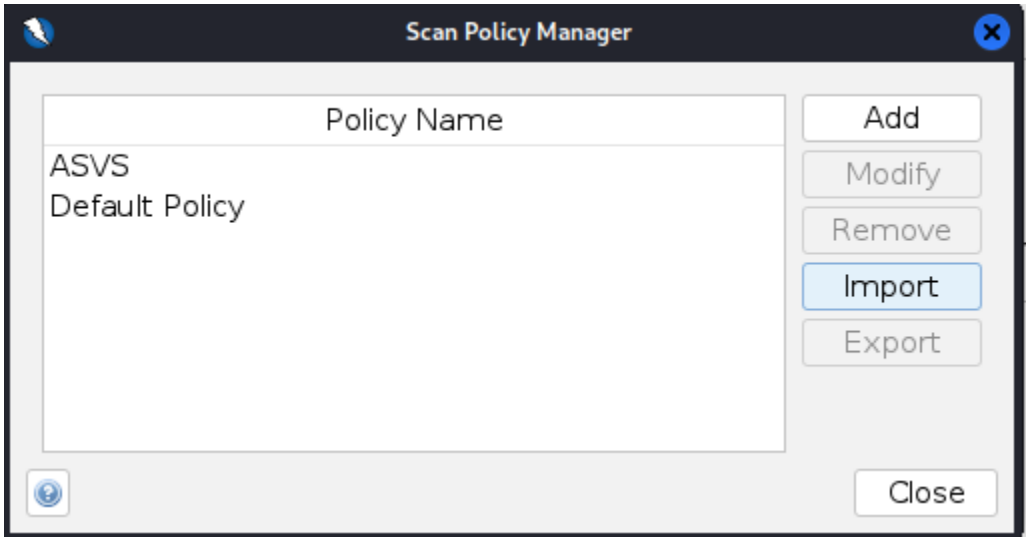


Configure Passive Scan Rules

From Tools > Options > Passive Scan Rules, Apply Off Threshold to All Rules and select Go. Then, Set the Script Passive Scan Rules and Vulnerable JS Library Threshold to Medium.

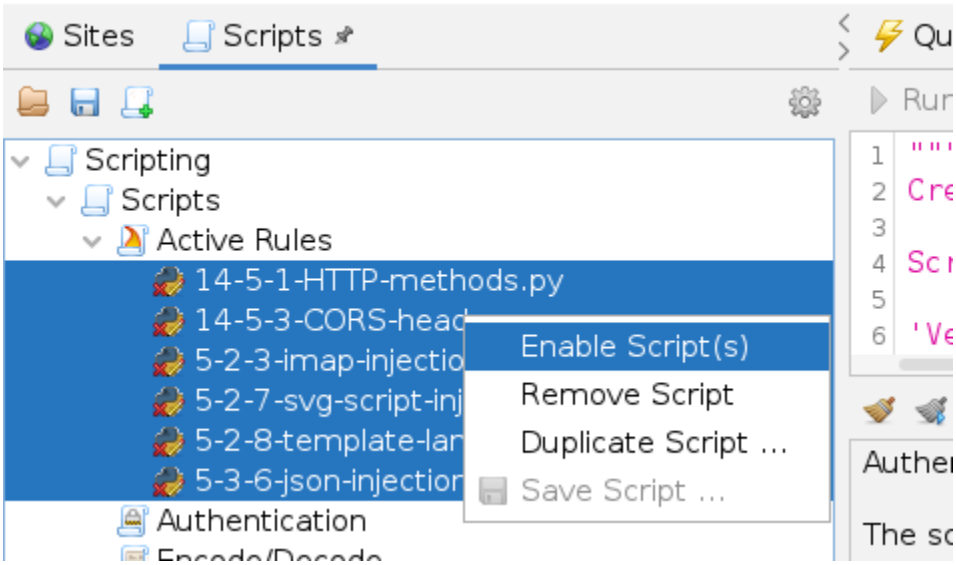
Add Active Scan Policy

From the Analyse Tab, select Scan Policy manager. Select Import and choose the ASVS.policy file from the downloaded repository. Once imported, the menu should look like this.



Enable Scripts

Click the green plus sign next to the Sites Tab to open the Scripts menu. For each section, Active, Httpfuzzerprocessor, Passive and Standalone, right-click each script and select Enable Script.



Suggested Scan

To get the full use of the scripts, it is suggested to use the following ZAP functionalities in this order.

1. Traditional Spider – To map resources in application and passively scan
2. Ajax Spider – To map resources in application and passively scan
3. Active Scan with ASVS Policy – To inject payloads from Active scripts
4. Standalone Script – To reformat alerts to match ASVS naming convention
5. Optional: Fuzzer scripts to test for default accounts, password security and unique session token generation.