Dynamic Scanning with OWASP ZAP for Identifying Security Threats

Prakhash Sivakumar Follow
Sep 27, 2016 · 12 min read

———————————————————————————————

1. Increase JVM Heap Size for Running ZAP

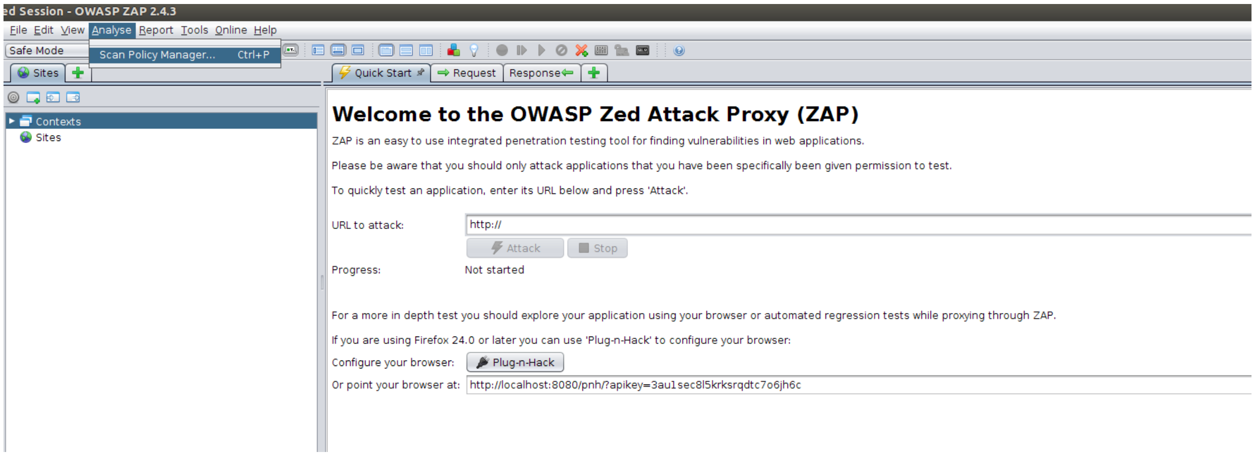
The heap size is defined in the **zap.sh** *(for linux)* and **zap.bat** *(for Windows)* files. Default value is set to **Xmx512m** *(if available free memory is above 1,500 MB)* and increase the value appropriately based on the memory availability of your system. *(At-least 4GB is recommended)*

In addition to that, ZAP scan is a long running process. Therefore it is better to run ZAP in a cloud instance or in a dedicated server to avoid any interruptions.

2. Fine Tune ZAP Tool with Pre-Configured Policy

ZAP tool should be fine tuned before running a scan for obtaining better results. For this, you can even use your own policy file for ZAP in which contains the settings to fine tune ZAP. A sample policy file is shown in [1]

Go to **Analyze → Scan Policy Manager** in ZAP.


ed Session - OWASP ZAP 2.4.3
File Edit View Analyse Report Tools Online Help
Safe Mode
Scan Policy Manager... Ctrl+P
Sites
Quick Start
Request
Response
Contexts
Sites
Attack
Stop
Plug-n-Hack

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://

Progress: Not started

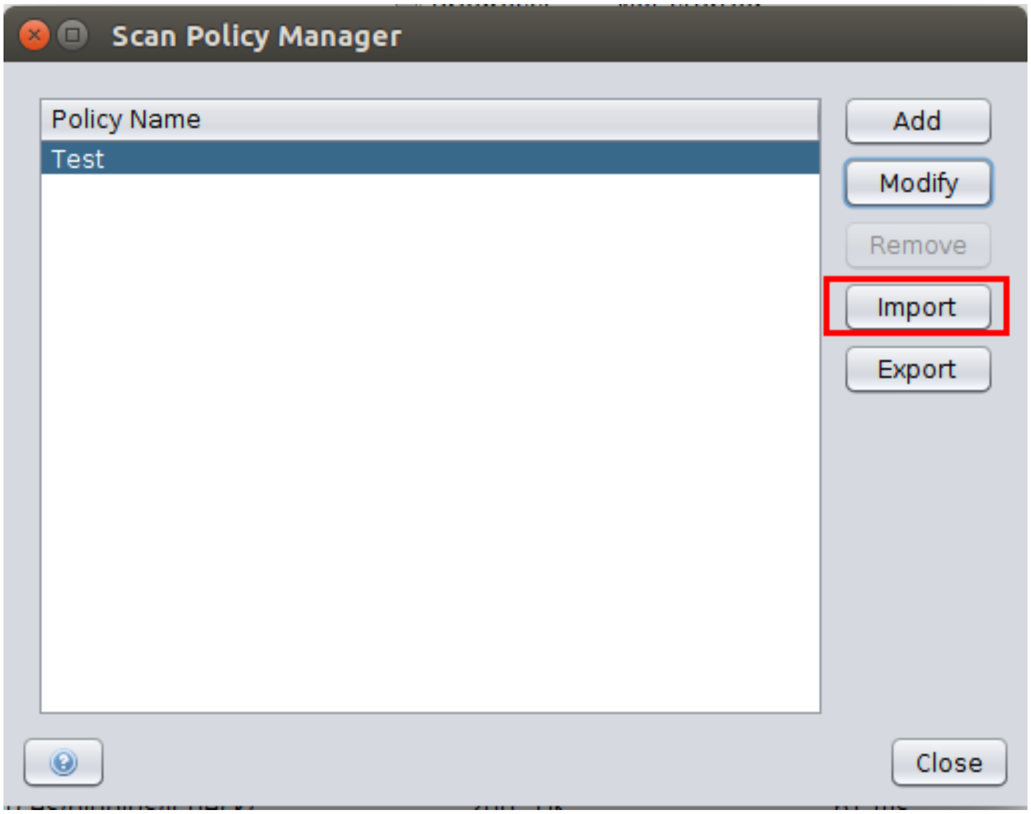
For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

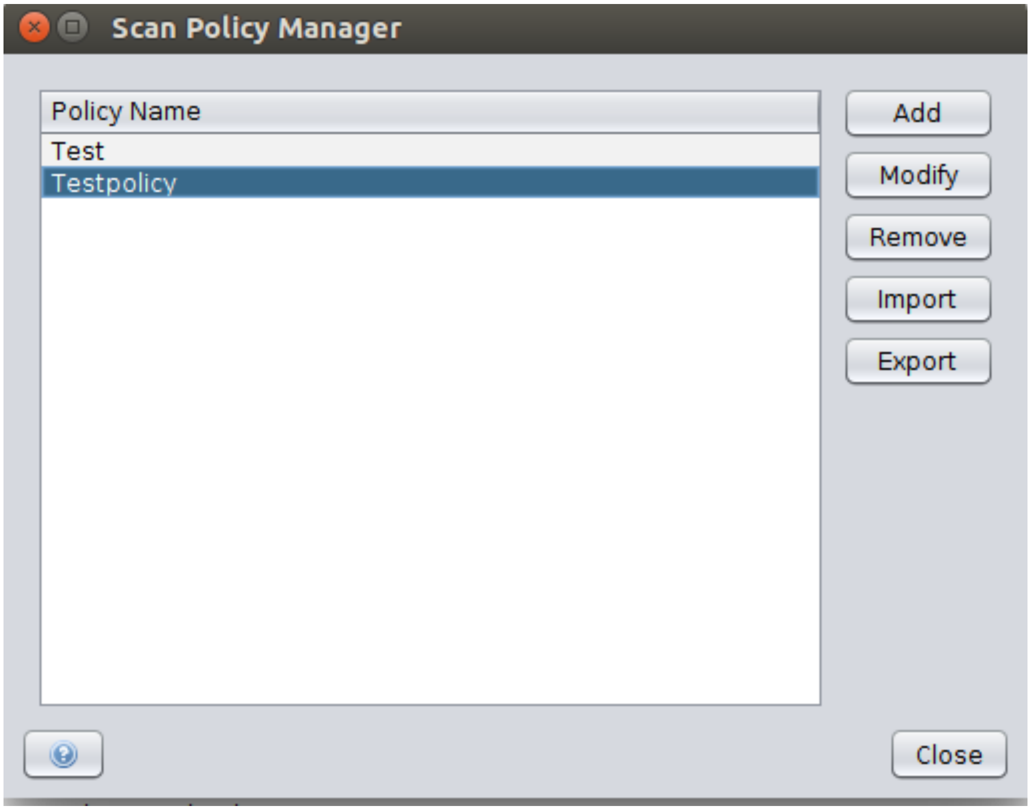
Configure your browser: Plug-n-Hack

Or point your browser at: http://localhost:8080/pnh/?apikey=3au1sec8l5krksrqdtc7o6jh6c

In the **Scan Policy Manager** window, click on **Import**.



Browse and select the Policy file.



Policy Name
Test
Testpolicy

Since the policy file is imported correctly, you can use this later when you run the spider and the scan.

3. Configuring ZAP Proxy to Trace Browser Traffic

Rather than providing the URL of your application and attack the URL with ZAP, it is much more effective if we record the UI actions we do on the application and let ZAP tool capture the traffic which can then be used for performing attacks.

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)*

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.

If any exception for **localhost**, **127.0.0.1** or the hostname of the application you are trying to scan is given in **No Proxy for:** text box, remove them so ZAP can detect the traffic flow of that as well.

Now, go to Firefox and access the application. Now the application URL should be opened in the browser. Also it should be listed in ZAP under the sites.

Select the Mode of the scan as **Protected Mode**. With this, you can choose which sites to be used for attacking.

4. Excluding the Application Logout from Spider

When we run the ZAP scan with an active user session, if ZAP executes the action to logout from the application in the middle of the scan, the actions that should be performed with a logged in user session would not be performed after that *(because active session is removed with logout action)*. In order to avoid that, we need to exclude the logout action from the Spider.

For that, first login to your siteand then logout so that the logout action is traced by ZAP. Then, find the **GET:Your_Logout_Action** and right click on it and exclude from Spider.

Then in the **Session Properties** window, it will show the URL regex that ZAP is going to exclude in the spider. Click **OK**.

5. Perform UI Actions Manually (or using Selenium)

With the above steps, ZAP is tracing the sites that you visit in the browser. Next step is to manually perform UI actions in the browser so that ZAP traces all the actions which we can then use for attacking.

On the URLs ZAP discovered, it can perform attacks to find possible issues. We can improve the coverage of the scan by manually performing all actions in the browser so that ZAP discovers each flow that it can try attacking.

You can also automate this by having selenium scripts for all UI actions. After setting the ZAP to act as the proxy, you can run selenium scripts so that in the browser, it automatically plays the actions you would do manually. For every action, ZAP will discover the URLs.

6. Removing Unnecessary Sites from Scan

When the ZAP is acting as the proxy, all the URLs that the browser calls will be traced under the **Sites** in ZAP. We need to remove external websites and select only your applications scope for scan.

Right click on the **Site** that should be included in the scan and select **Include in Context -> New Context** .

Then it will show the **Session Properties** window with the regex for including the URL patterns in the scan. Provide a name for the context so that we can identify the site uniquely when we have multiple sites added as different contexts.

Once the site is added to the Context for scan, the icon image for each entry under the tree of the site will be changed showing that it is added to the context.

Under the Sites list, you can click on the **Show all URLs** button to view only the sites that are added to the contexts. All other sites will be hidden from the Sites panel with this option.

Once you have added the site/s to the context, you can filter the scan results *(after running a scan)* easily. In the History tab, **Show only URLs in Scope** filters the results and shows only the URLs that belong to the context.

When searching also you can search URLs that belong only to the context with the **Search all URLs** option enabled.

You can also filter the alerts that belong only the contexts you have added with the **Show all URLs** option enabled.

7. Globally Excluding URL Patterns

When the ZAP tool starts crawling the site, it will increase the network traffic heavily. We can reduce the traffic by excluding the URL patterns globally so that ZAP will ignore such URLs when crawling. For example if we exclude URLs of .mp4 video files, ZAP tool will not download mp4 video files which saves network bandwidth.

Go to **Tools -> Options** and select **Global Exclude URL** option. By default there are some patterns already added to ZAP. You can select all of them for exclusion. Additionally, if there is any URL pattern you need to exclude, you can add the regex for the URL as a new entry.

8. Creating the Logged in User Session

When running the spider to crawl the site, we have to let ZAP discover the URLs that are accessible only by logged in users as well. For that, we need to create a logged in user session in ZAP so that same as a logged in user can browse the URLs in web browser, ZAP will be able to crawl through those URLs.

Click on **Show All Tabs** in the toolbox so that it will display all the tabs.

Go to the **Http Sessions** tab. If there are already created sessions listed, you can remove them.

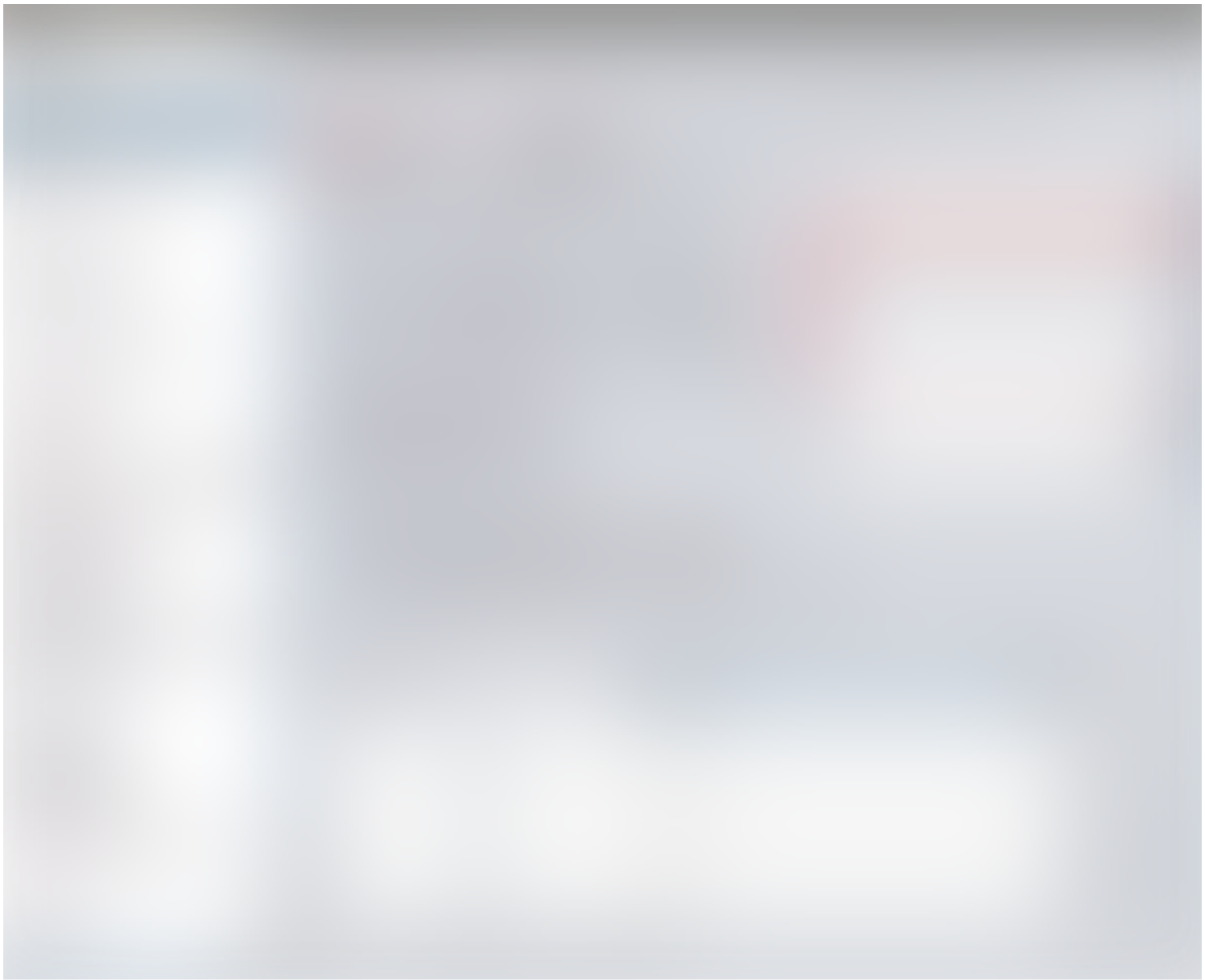
Now while ZAP proxy is tracing the traffic, go to the browser and login to the site you need to scan. *(When ZAP performs the scan, it will attack to the URLs with the associated privileges of the user you logged in)*. Once you login, the session ID should be listed in the **HTTP Sessions** tab. Right click on the session and **Set as Active**.

Above should be done only if the authentication to the site is tracked via the **SESSIONID**.

9. Configuring and Running AJAX Spider

When you have multiple sites added to the context and when you need all the sites to have the same configuration, you can set them globally. Go to **Tools -> Options** and select **AJAX Spider**.

Set the maximum crawl depth, maximum crawl states and maximum duration to **0** so that the AJAX Spider will go on crawling completely without any limitation.

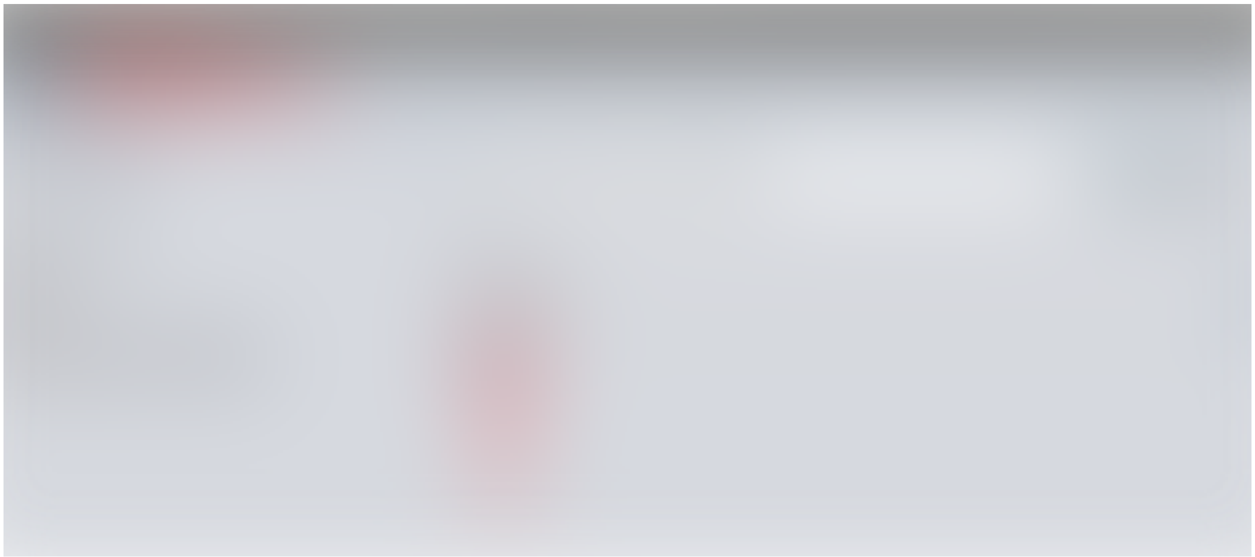


You can choose the browser to be used for crawling by the AJAX spider. If your browser is not listed in the dropdown, go to **Tools -> Options** and in the **Selenium** option, browse and provide the selenium driver for the particular browser. *(You can download the selenium driver for the particular web browser from internet)* . Once you have provided the driver, in AJAX Spider configuration's browser dropdown the browser will be listed.

If you have multiple sites added to the context, but need to have separate ajax spider configuration for a particular site, you cannot use global settings. In such case, right click on the particular site and go to **Attack -> AJAX Spider**.

Also you need to select **Protected Mode** *(from the dropdown in toolbox)* for running the AJAX spider so that it will crawl through the sites added to the context and will skip any URL that is out of scope.

Select **Show advanced options** in the **Scope** tab which will make the **Options** tab visible.



In the **Options** tab of AJAX Spider, you can set the configuration specific to this particular site.

Once the configuration is set, you can **Start Scan**.

Before starting the scan, you need to make sure that you have an active user session set in ZAP *(Follow the steps in* ***Creating the Logged in User Session*** *section)* so that AJAX spider can crawl URLs that are accessible by the logged in user.

10. Running Spider

The global configuration for Spider is in **Tools -> Options** under **Spider** option which is applicable to all the sites added to the context.

You can set the maximum depth to crawl to **5**. At this point we have already run the AJAX Spider and discovered most of the URLs with crawling. Therefore crawling more up to a depth of 5 levels would provide sufficient coverage.

When you have multiple sites added to the context and need to have separate Spider configuration for a particular site, you cannot use Global Settings. In such case, you can right click on the site and go to **Attack -> Spider**.

In the **Spider** window, select **Show Advanced options** and go to the **Advanced** tab

Since we have run the AJAX Spider previously, it should have crawled most of the URLs of the Application. Therefore having only **5** as the maximum depth to crawl would be sufficient to complete crawling and covering the URLs of the Application.

With above configuration, start the scan to complete URL discovery.

11. Removing False Positives before Scanning

Before running the Active Scan, we can configure the Session Properties such that when reporting alerts, it would avoid known false positive URLs.

Go to **Files → Session Properties** and under the particular context, select **Alert Filters**.

The click on **Add** button to define the URLs that we have already identified to be reporting false positive alerts.

In the **Add Alert Filter** window, select the type of **Alert** and set it as a **False Positive** in the **New Risk Level** dropdown. If the URL is a direct URL, it can be given in the **URL** textbox. If there are multiple URLs following the same pattern, select the **URL is Regex?** checkbox and define the regular expression for the URL. Finally **Confirm** the alert filter.

The alerts generated for these URLs would be ignored by ZAP during the scanning time and also would not appear in the identified security vulnerabilities.

12. Running Active Scan

When you have multiple sites in the context and need to have similar active scan configuration for all the sites, you can use the global settings. Go to **Tools -> Options** and select **Active Scan**.

As the default active scan policy and attack mode scan policy, select the Testpolicy file which you imported in section ***Fine Tune ZAP Tool with Pre-Configured Policy***.

When you have multiple sites added to the context, but need to have specific active scan configuration for a particular site, you can right click on the particular site and go to **Attack -> Active Scan**.

It will show the **Active Scan** window. Select **Show advanced options** and go to **Policy** tab.

As the **Policy**, select the TestPolicy file which you imported previously.

Finally start the scan. Note that you need to have a logged in user session when running the active scan. *(follow the steps in **1.8 Creating the Logged in User Session**)*

Then the scan will begin and you can see the progress in **Active Scan** tab.

13. Removing False Positives Before Report Generation

Once the **Active Scan** is completed and the alerts are generated, if there are false positive alerts, they can be removed appearing in the reports generated. For that, go to the **Alerts** tab and double click on the particular alert that should be marked as a false positive.

Then the **Edit Alert** window will appear. In the **Confidence** dropdown, select **False Positive**.

14. Generating Reports

Once the **Active Scan** is complete, you can generate the reports for exporting the results of the scan. Go to **Report -> Generate HTML Report** from the menu.

Then it will prompt where to save the report. Once you provide a file path, it will export the ZAP scan report. By examining the report, you will be able to identify possible security threats and get them fixed.

References

[1] https://gist.github.com/anonymous/240783a9dd4aa963a6b5101ac17b0bdf
[2] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project