Getting Started

Prerequisites

This guide assumes that you have OWASP ZAP installed and are able to access the graphical user interface (as opposed to using ZAP in headless mode).

Configuration

OWASP ZAP has by default enabled scripts and scan rules that should be disabled if you would like to receive a report which would include only alerts triggered by scripts testing OWASP ASVS controls. That includes action such as:

- Creating a context for your domain, so only the domains that are specified by you are scanned and no others.
- Disabling passive scan rules that are not part of the test
- Creating a policy for active scan scripts, in which only the scripts provided will be executed

Create a context for your domain

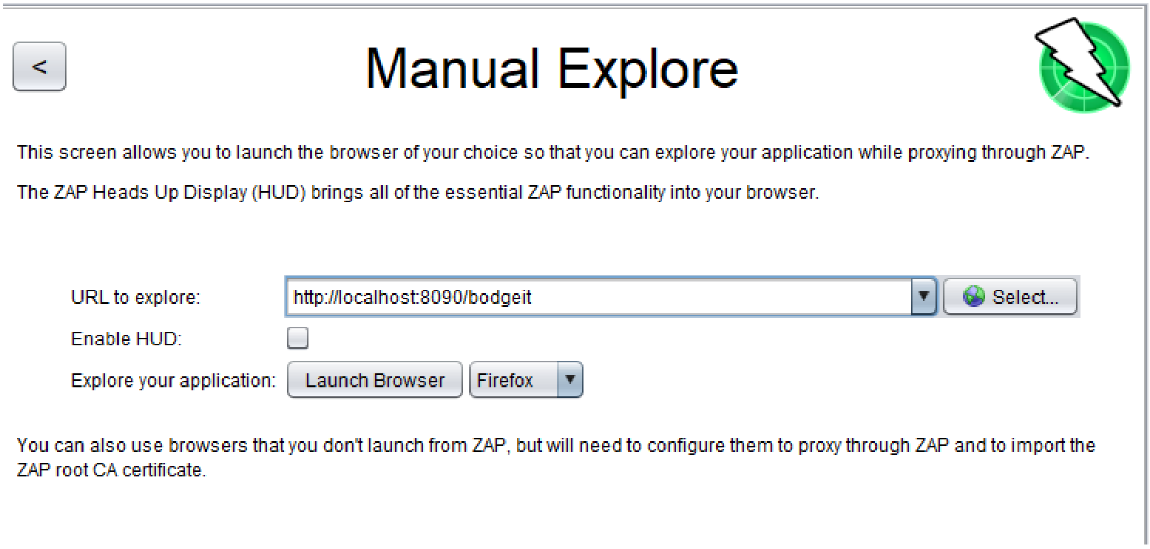
A context in ZAP defines how ZAP will work with certain websites. With specifying several contexts, you may separate issues that affect your website from issues that come from the third-party providers. This has to be look upon with a grain of salt - while the issue might have been found with a resource coming from a 3rd party provider, the issue may lay in how the resource is implemented on your website. When doing a scan of a website (especially using a spider or an active scan), configuring a context is a must - there you define:

- scope - which websites to scan and which should explicitly be excluded
- authentication and users that should be used for authentication
- session management

A properly configured context will make the spider and scan only target the websites in scope, without attacking ones that may belong to third party. If authentication and session management is configured, the spider and the scanner will be able to automatically authenticate if a session token has expired or the spider accidentally logged out - this will provide a better coverage of the tested site.

The easiest way to configure a context is after you have accessed the target domain with a built-in browser or preconfigured one.

1. Go to Manual Explore, input target application name and press 'Launch browser'.



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: http://localhost:8090/bodgeit

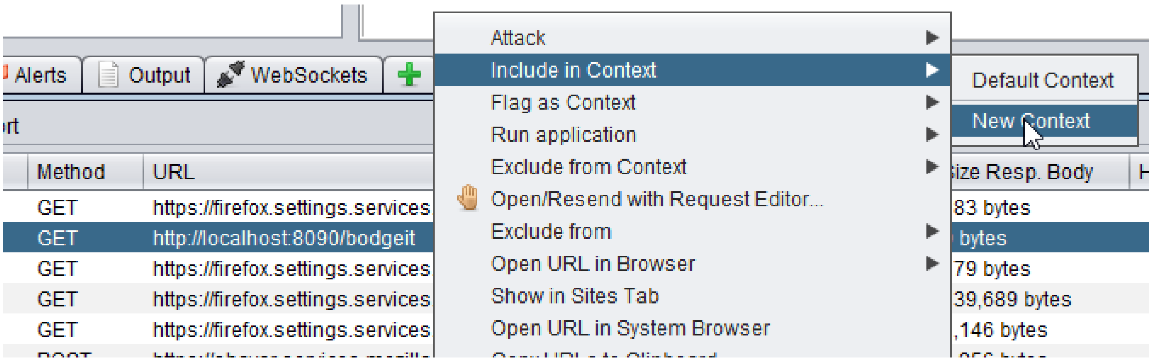
Enable HUD: □

Explore your application: Launch Browser Firefox

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

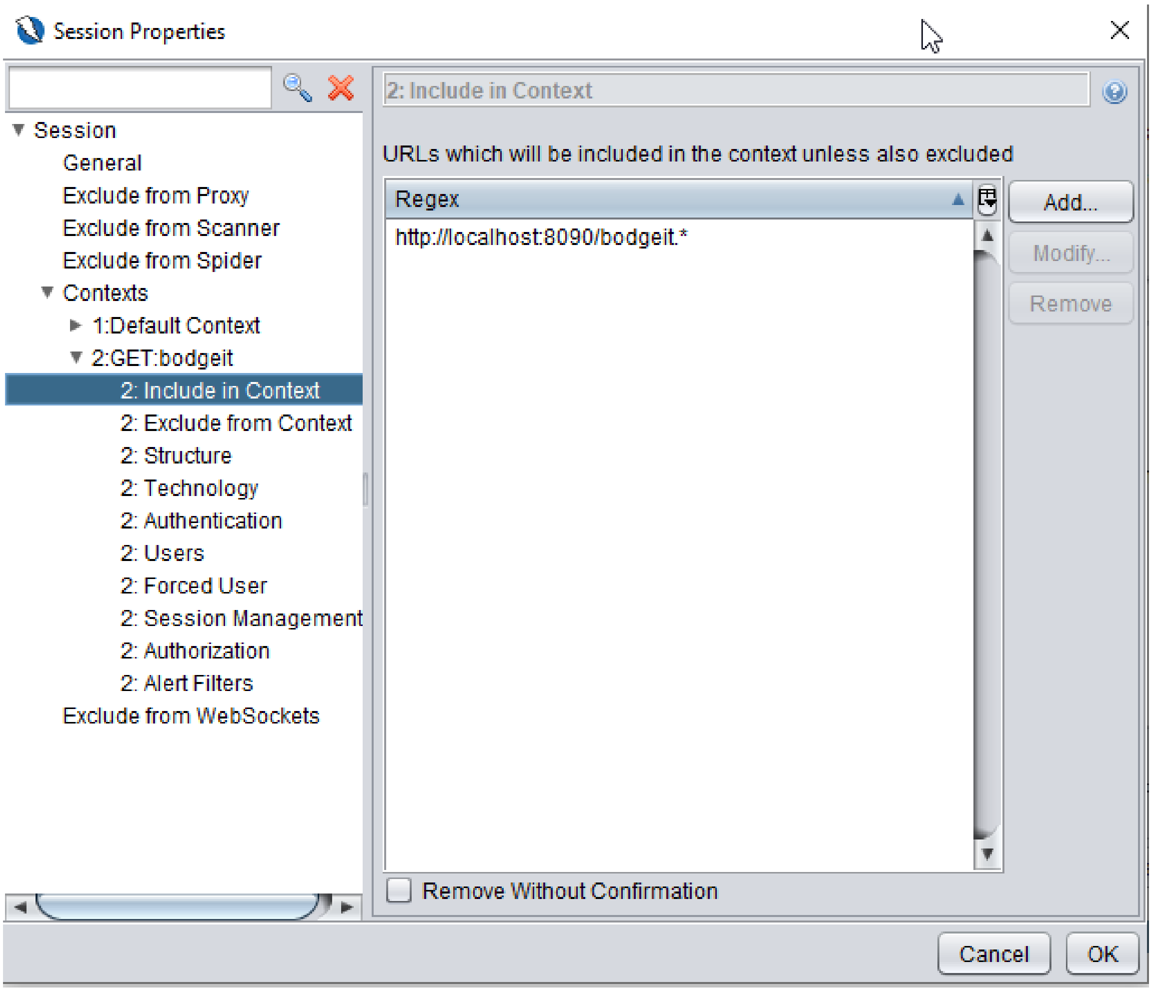
Wait for the browser and the application to load. You can click around to create some traffic, then close the browser and go back to ZAP. In the Sites tree you will see several domains.

2. On Sites tree, choose your target and left click on it and choose Include in Context > New Context OR left-click on the entry in the History tab and choose Include in Context > New Context



Method	URL	ize Resp. Body
GET	https://firefox.settings.services	83 bytes
GET	http://localhost:8090/bodgeit	bytes
GET	https://firefox.settings.services	79 bytes
GET	https://firefox.settings.services	39,689 bytes
GET	https://firefox.settings.services	,146 bytes

3. A pop up box will appear where you can configure your new context. There has been added a wildcard to the address, which means that everything that comes after bodgeit will be in scope. If there are any other sites that you would like tested you may add them here.



2: Include in Context

URLs which will be included in the context unless also excluded

Regex
http://localhost:8090/bodgeit.*

□ Remove Without Confirmation

4. Exclude the subdirectories from target website or addresses that you wish not to be targeted.

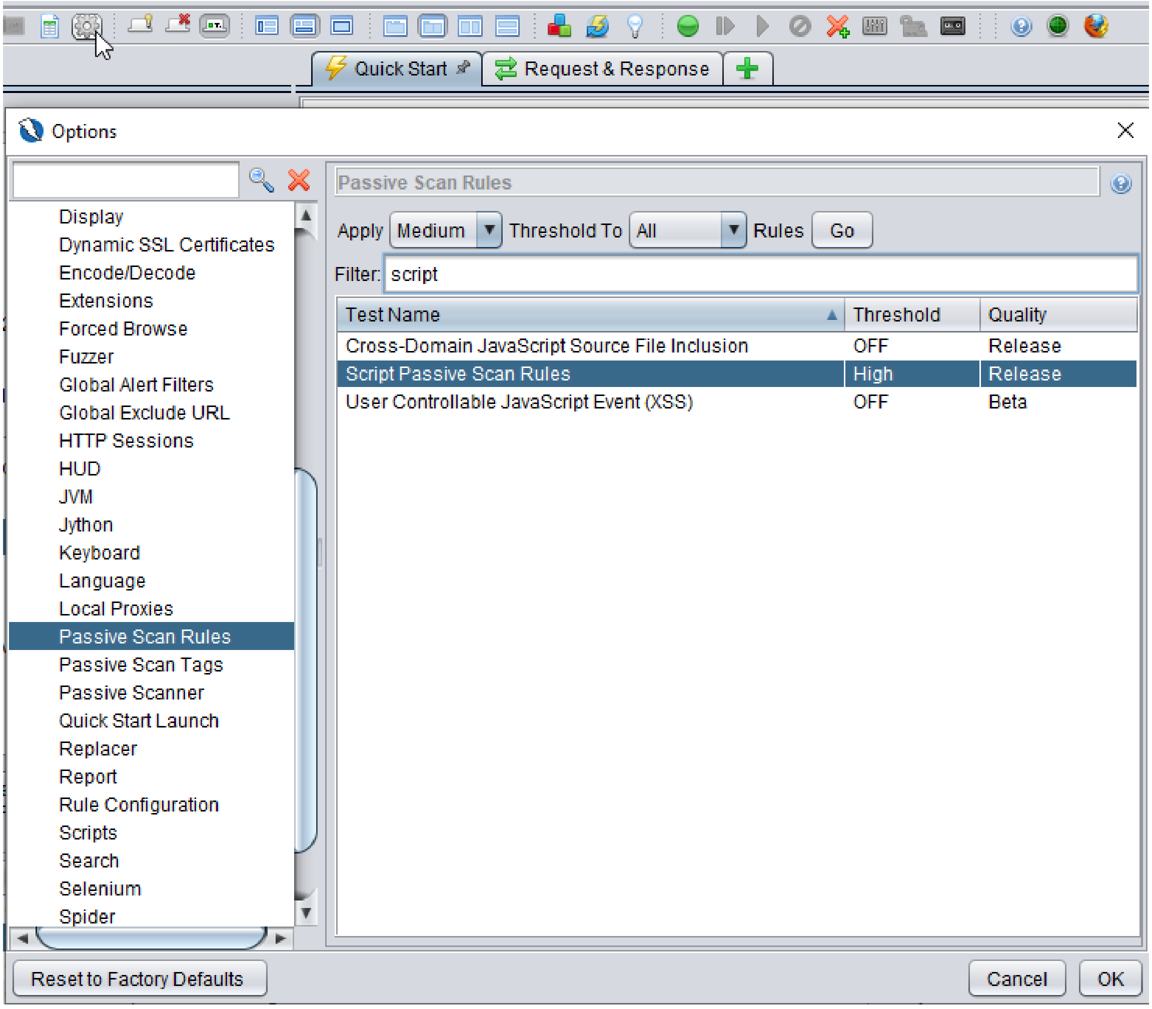
5. If you wish to configure authentication and session management, you may do it here. Refer to videos on ZAP's website for configuring those: https://www.zaproxy.org/videos/ and articles such as: https://dzone.com/articles/scripting-authenticated-login-within-zap-vulnerabi They are a brilliant resource if you would like to get up to speed with using ZAP.

6. *Now that we are done with configuring the context you can apply it in history tab by clicking the red target button. Next we want to configure*

the passive scan rules to use only the enabled scripts and to only scan the target in scope

Passive Scan rules

1. Click Options icon, go to Passive Scan Rules and choose 'Apply OFF Threshold to All'. Then filter for script and apply High threshold to script passive scan rules



Apply Medium Threshold To All Rules

Filter: script

Test Name	Threshold	Quality
Cross-Domain JavaScript Source File Inclusion	OFF	Release
Script Passive Scan Rules	High	Release
User Controllable JavaScript Event (XSS)	OFF	Beta

2. Go to Passive Scanner and check 'Scan only messages in scope'

3. ZAP scripting engine supports several languages. To install them go to Marketplace and search for scripts. Feel free to install as many as you want. You may also want to install Community scripts in Aplha and Beta release. After you have installed these add-ons, they will appear in the installed tab. Click Marketplace icon, search for OWASP ASVS passive scan rules and install Jython extension. Install also RetireJS add-on.

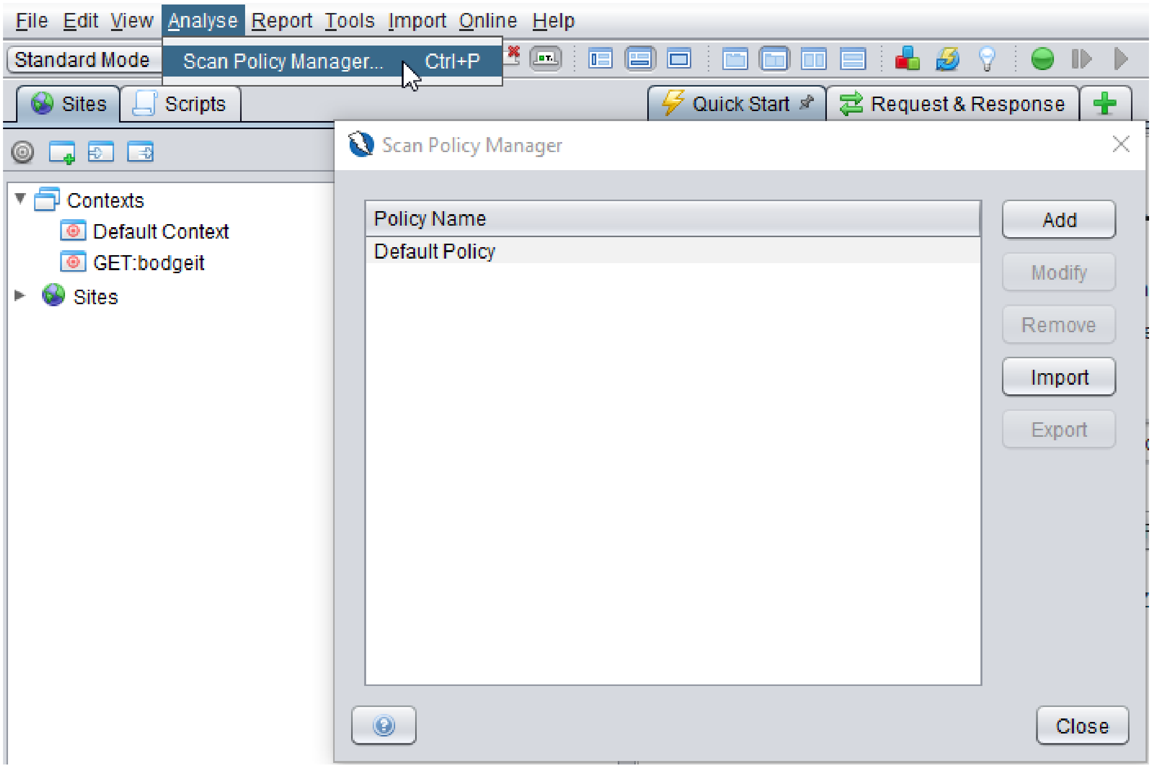
4. Check in Options > Passive Scan rules. Search for "Script Passive Scan rules" and set Threshold is to 'Medium'. Search for "Vulnerable JS library" and set Threshold to 'Medium'.
5. Click the green plus next to 'Sites' tab > click 'Scripts' > choose 'Passive Rules' > enable all scripts that came from this repository (or only the ones that you would like to test)
6. Go to Quick Start > Automated Scan and input the address of the domain you wish to scan.
7. Tick 'Use traditional spider' and click the 'Attack' button. If you wish for more coverage of your website, tick 'Use ajax spider' and choose one of the browsers you have installed. The spider shouldn't take longer than a few minutes to run. If you have enabled the ajax spider it will take longer.
8. In the lower right corner you will see several symbols, including an eye. Wait until the number goes down to zero - that means that passive scanning has finished. Depending on the size of your application, it may take a long time, so set it aside for an hour just in case.
9. Go to Report > Generate HTML report. If you prefer the folder in any other format, choose other options - Markdown, XML, JSON. If you have chosen HTML report, you will be presented with the report will all the controls.

You can see all the alerts that were raised by the scripts in the alerts tab. Then if you wish to generate a report of all these alerts, you can do so by going to Report > Generate HTML report.

Active Scan

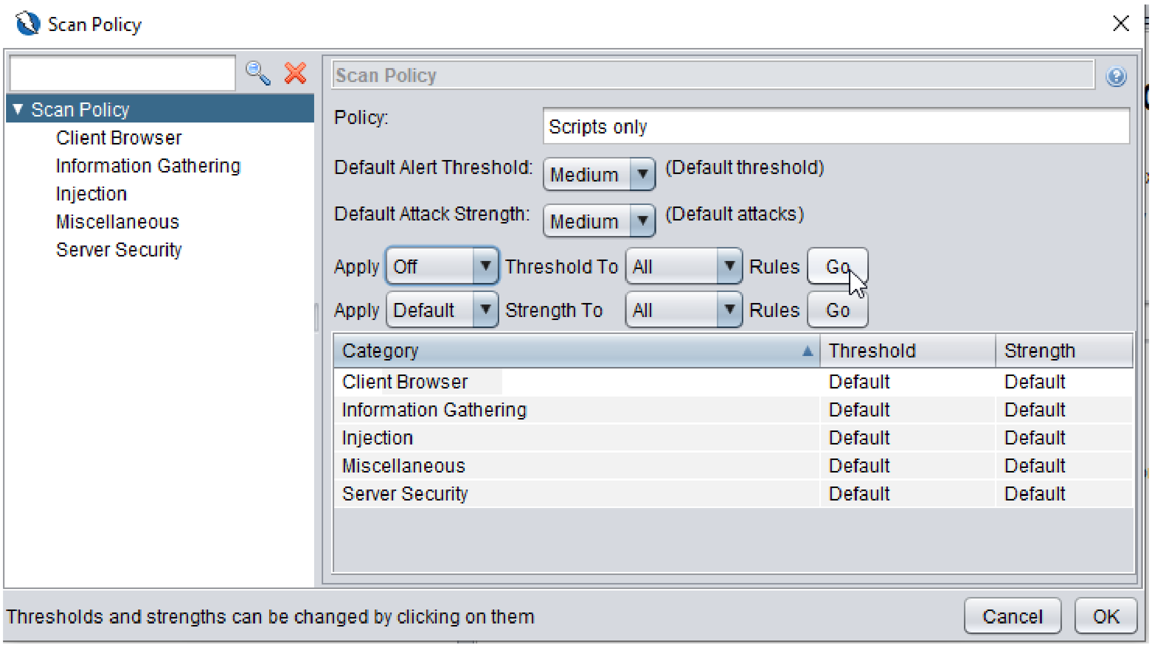
Policy

1. To scan an application using Active Scan scripts go to Scripts > Active Scan and enable all scripts that you wish to use.
2. Go to Analyse > Scan Policy Manager... You will see a pop up box. Click Add



Policy Name
Default Policy

3. Another pop up box will appear. Name your policy "Scripts only" and choose "Apply 'Off' Threshold to 'All'" and press Go.



Policy: Scripts only

Default Alert Threshold: Medium (Default threshold)

Default Attack Strength: Medium (Default attacks)

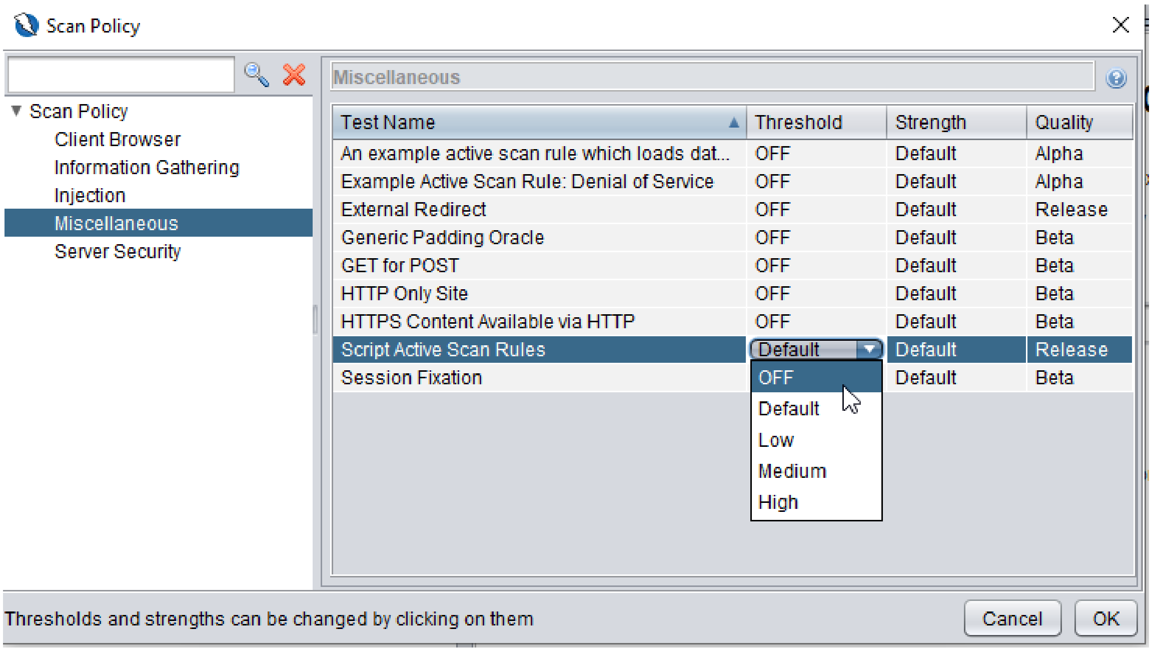
Apply Off Threshold To All Rules

Apply Default Strength To All Rules

Category	Threshold	Strength
Client Browser	Default	Default
Information Gathering	Default	Default
Injection	Default	Default
Miscellaneous	Default	Default
Server Security	Default	Default

Thresholds and strengths can be changed by clicking on them

4. Go to Miscellaneous and choose your preferred threshold - for example Medium. Then click OK.



Test Name	Threshold	Strength	Quality
An example active scan rule which loads dat...	OFF	Default	Alpha
Example Active Scan Rule: Denial of Service	OFF	Default	Alpha
External Redirect	OFF	Default	Release
Generic Padding Oracle	OFF	Default	Beta
GET for POST	OFF	Default	Beta
HTTP Only Site	OFF	Default	Beta
HTTPS Content Available via HTTP	OFF	Default	Beta
Script Active Scan Rules	Default	Default	Release
Session Fixation		Default	Beta

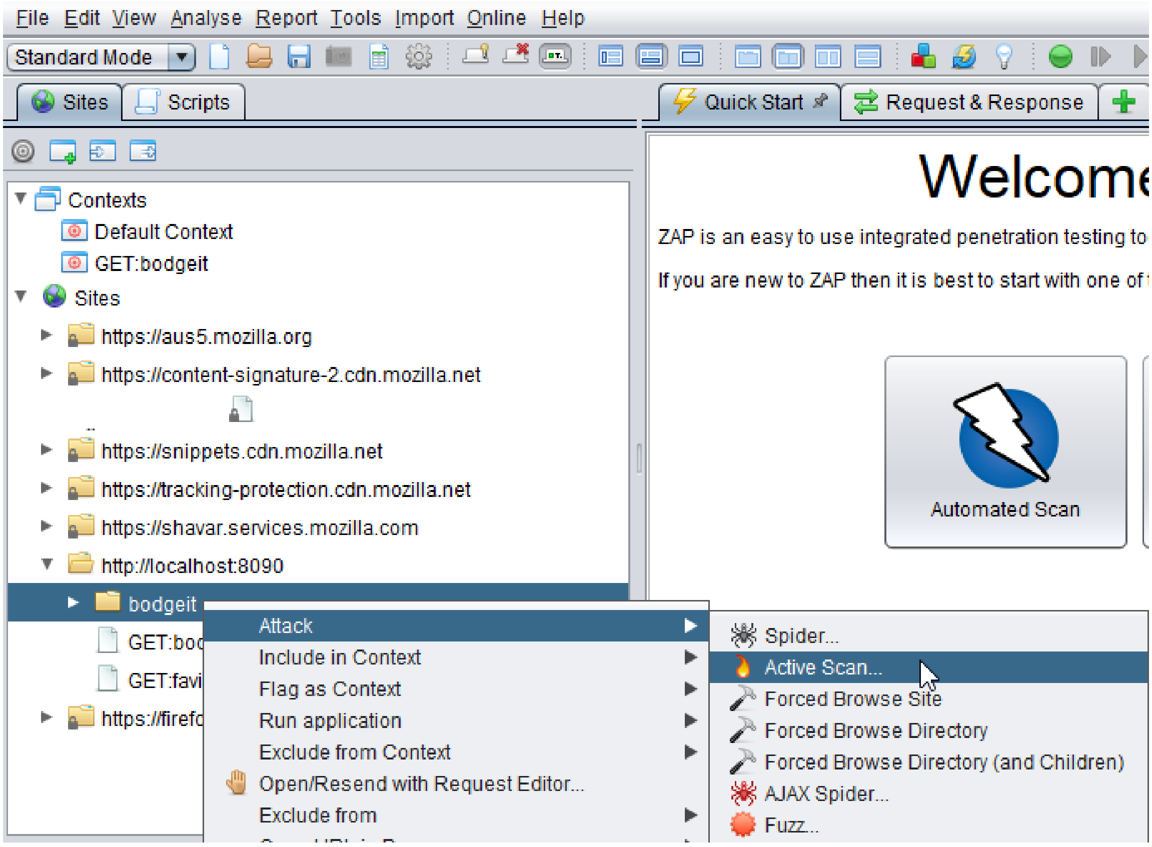
Thresholds and strengths can be changed by clicking on them

Active Scanning

Clone the script from the GitHub and place them in C:\Users\<your user>\OWASP ZAP\scripts\active and then import by going to ZAP > click the green plus next to 'Sites' tab > click 'Scripts' > click the 'import' folder icon > go to active > choose the desired scripts to load.)

It's preferable that you first run a spider before using active scanning for better coverage.

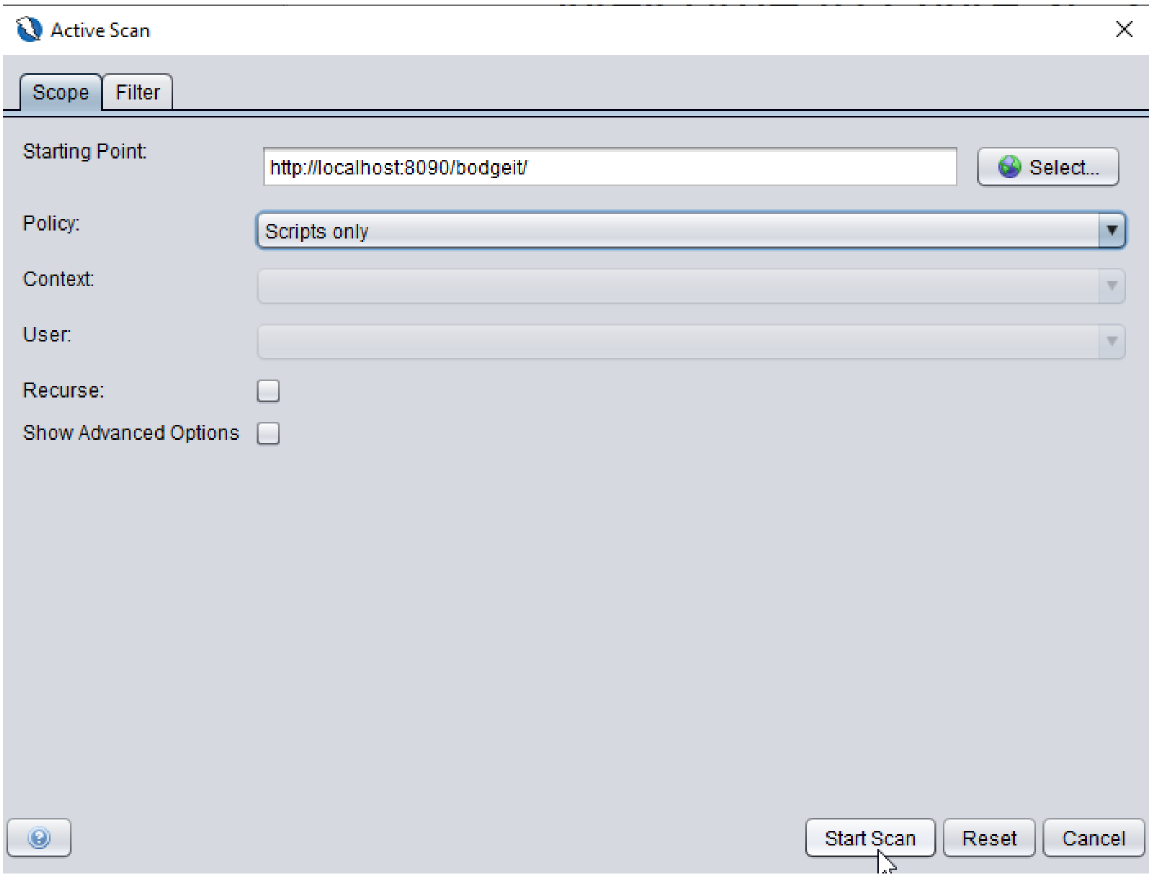
1. Next to Sites tab you will see a Green Plus sign. Press it and choose Scripts. You will see a new tab with example scripts you can use.
2. Go to Active Scan and enable the scripts you wish to scan with.
3. Go back to Sites tab and choose the domain you wish to scan. Left click, choose Attack > Active Scan...



ZAP is an easy to use integrated penetration testing to

If you are new to ZAP then it is best to start with one of

4. A pop up box will appear. Choose script policy "Scripts only" that you configured earlier. If you want to scan the node you have selected in the sites tree, then uncheck "Recurse" option. If you wish the active scan to be executed on all subnodes (subdirectories), leave the option checked. Press Start Scan and let it run for several minutes.



Starting Point: http://localhost:8090/bodgeit/

Policy: Scripts only

Context:

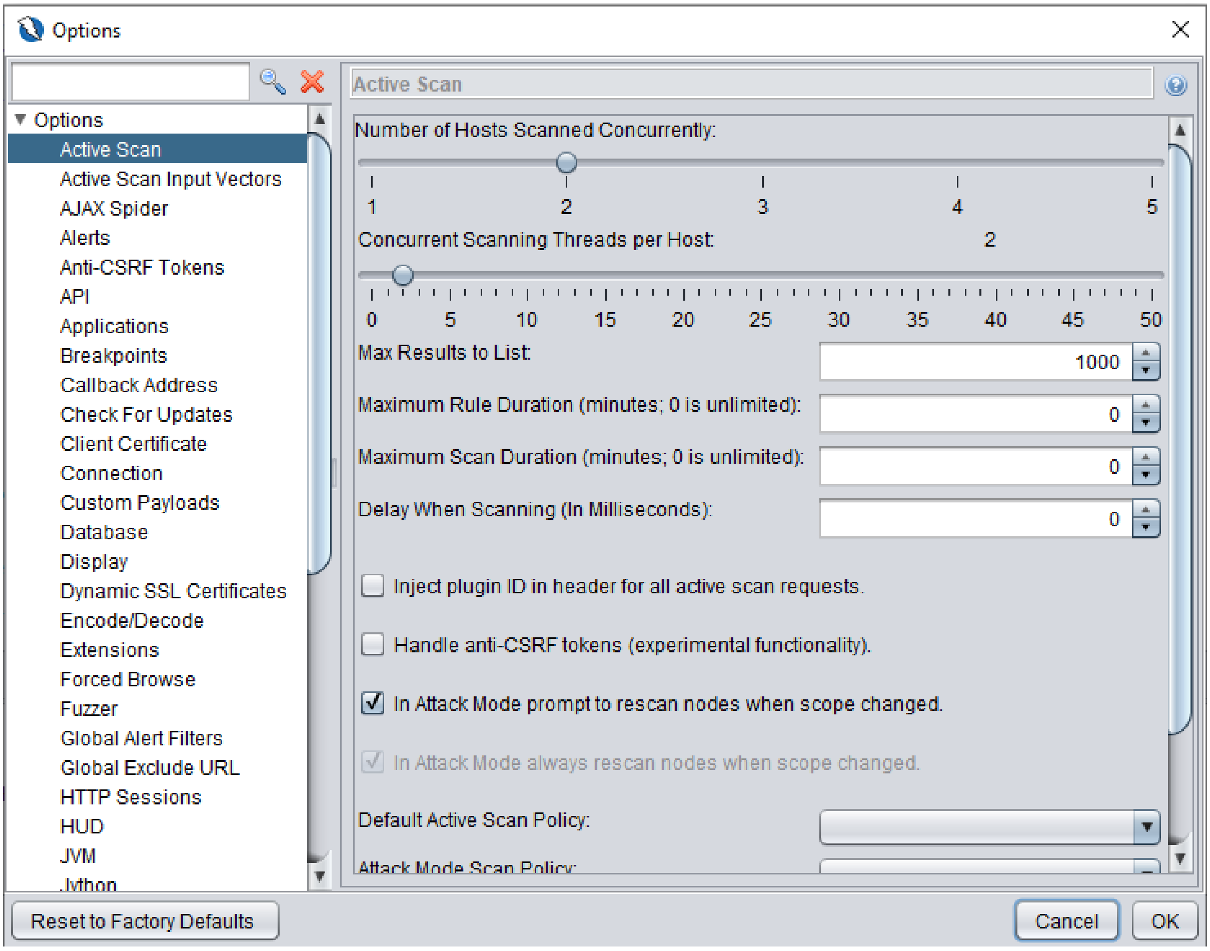
User:

Recurse: □

Show Advanced Options □

(optional) How to slow down the scan

Go to Tools > Options > Active Scan. Here you may change 'Delay When Scanning (in Milliseconds) to 500 - which would be one request per half second. In similar way, if you want to limit how long the scan will last, you can set Maximum Scan Duration.



Number of Hosts Scanned Concurrently:

Concurrent Scanning Threads per Host: 2

Max Results to List: 1000

Maximum Rule Duration (minutes; 0 is unlimited): 0

Maximum Scan Duration (minutes; 0 is unlimited): 0

Delay When Scanning (In Milliseconds): 0

□ Inject plugin ID in header for all active scan requests.

□ Handle anti-CSRF tokens (experimental functionality).

☑ In Attack Mode prompt to rescan nodes when scope changed.

☑ In Attack Mode always rescan nodes when scope changed.

Default Active Scan Policy:

Attack Mode Scan Policy: