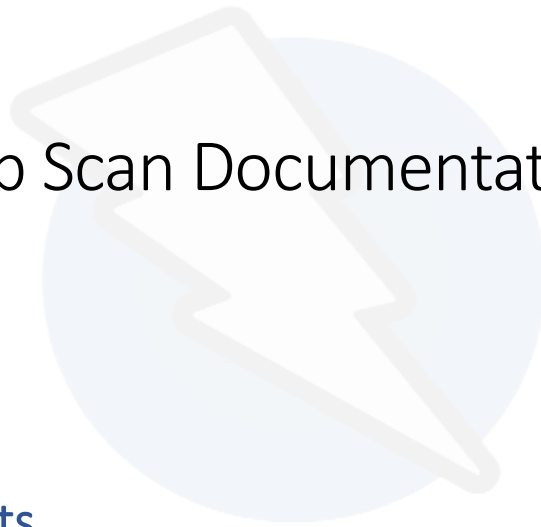


# Zap Scan Documentation



## Table of Contents

<b><i>Zap Installation .....</i></b>	<b><i>2</i></b>
<b><i>Manual Exploration Scan .....</i></b>	<b><i>3</i></b>
Overview .....	3
<b><i>Scan Policy Manager .....</i></b>	<b><i>4</i></b>
Overview .....	4
Editing Policies.....	4
<b><i>Setting Up a Context (Profile) .....</i></b>	<b><i>6</i></b>
Active Scan Using a Profile .....	9

## Zap Installation

Official OWASP Zap download page: [OWASP ZAP – Download \(zaproxy.org\)](https:// zaproxy.org/)

### Kali Linux:

```
sudo apt update  
sudo apt install zaproxy
```

### CentOS

```
yum install owasp-zap
```

### Ubuntu

```
sudo apt update  
sudo apt install owasp-zap
```


# Manual Exploration Scan

## Overview

The Manual Exploration feature on Zap allows one to explore a web application through a web proxy. Zap will then scan whatever pages that are being looked through by the user. This feature is an efficient way to scan specific web pages.

<

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:

Select...

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.

Figure 1: Manual Explore

Enabling HUD (Heads Up Display) will allow users to access tools, panels, and alerts while exploring the web proxy. An in-depth HUD tutorial option will pop-up once the browser is launched.

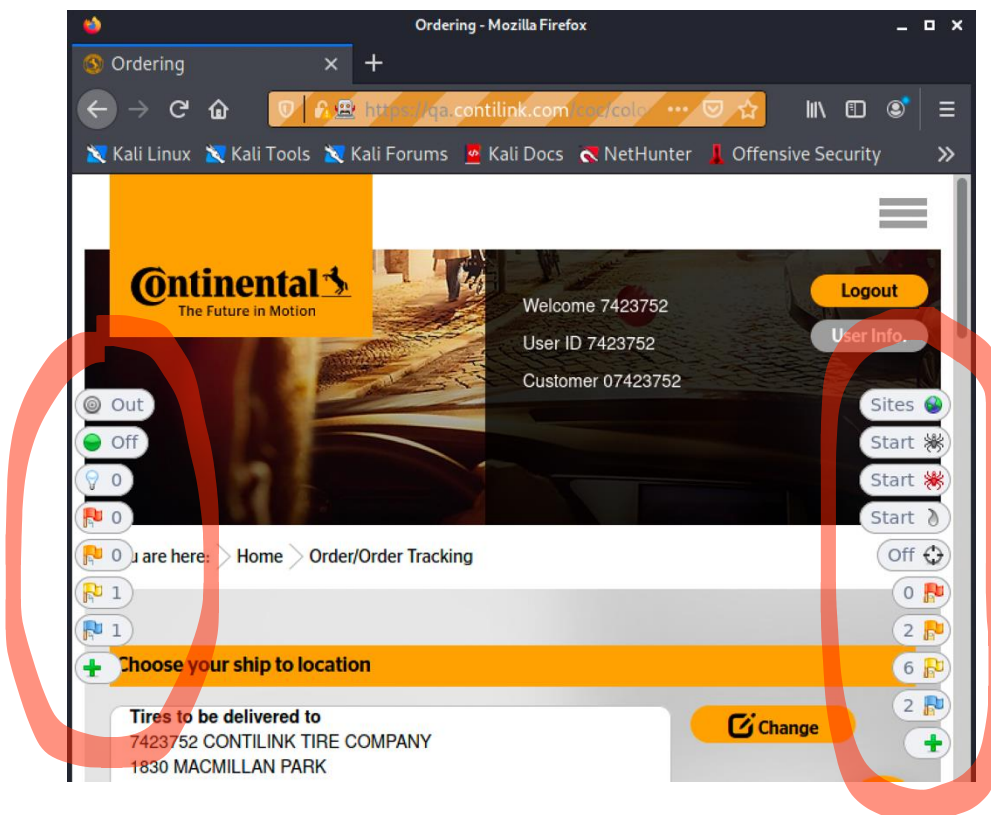


Figure 2: Web proxy after enabling HUD

## Scan Policy Manager

### Overview

This feature allows users to manage scan policies that define the rules when performing an active scan. Users can modify current policies or create new ones.

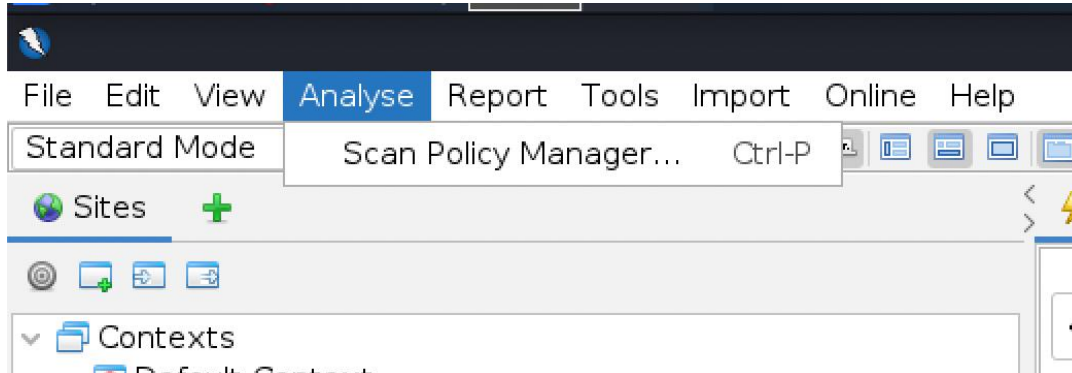


Figure 3: The Scan Policy Manager can be found under the "Analyse" tab in the menu bar.

### Editing Policies

When editing a policy, users can change the threshold and strength of attacks.

**Threshold:** Controls how likely potential vulnerabilities will be detected.

**Strength:** Controls the number of attacks that will be performed.

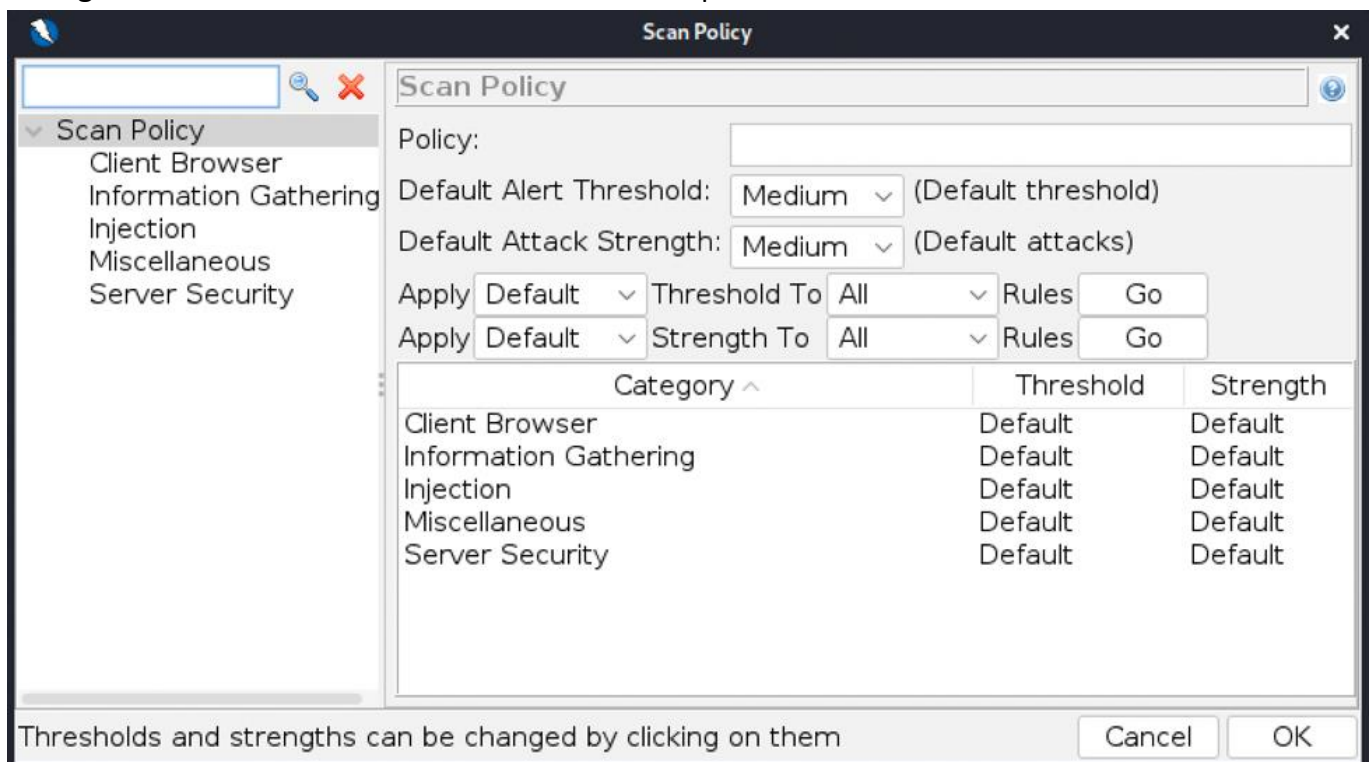


Figure 4: Creating a New Scan Policy Window

The tabs on the left window under “Scan Policy” are different categories of tests that are performed during an active scan. Users can change the threshold and strength of each test to their desired intensity.

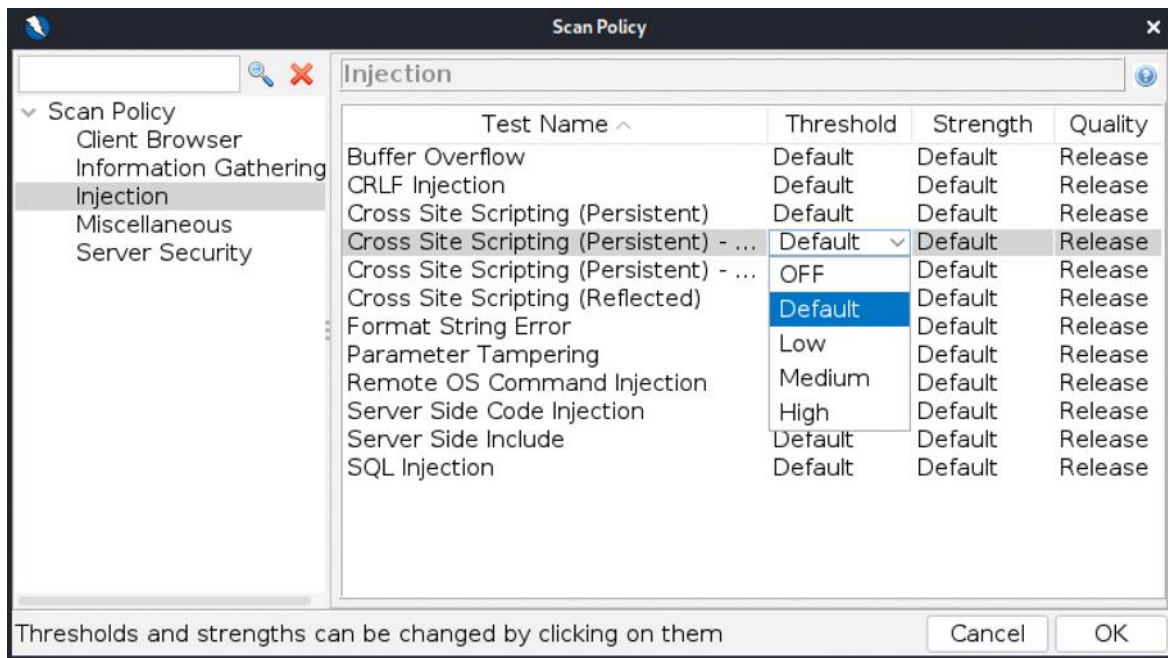


Figure 5: Each type of test can be adjusted

## Setting Up a Context (Profile)

Form Authentication tutorial: <https://www.youtube.com/watch?v=3u7aKXXCCKA>

Step 1: Perform a Manual Explore Scan of the login page of the site.

Step 2: On Zap, find the "POST: login..." tab under your targeted website in the 'Sites' window.

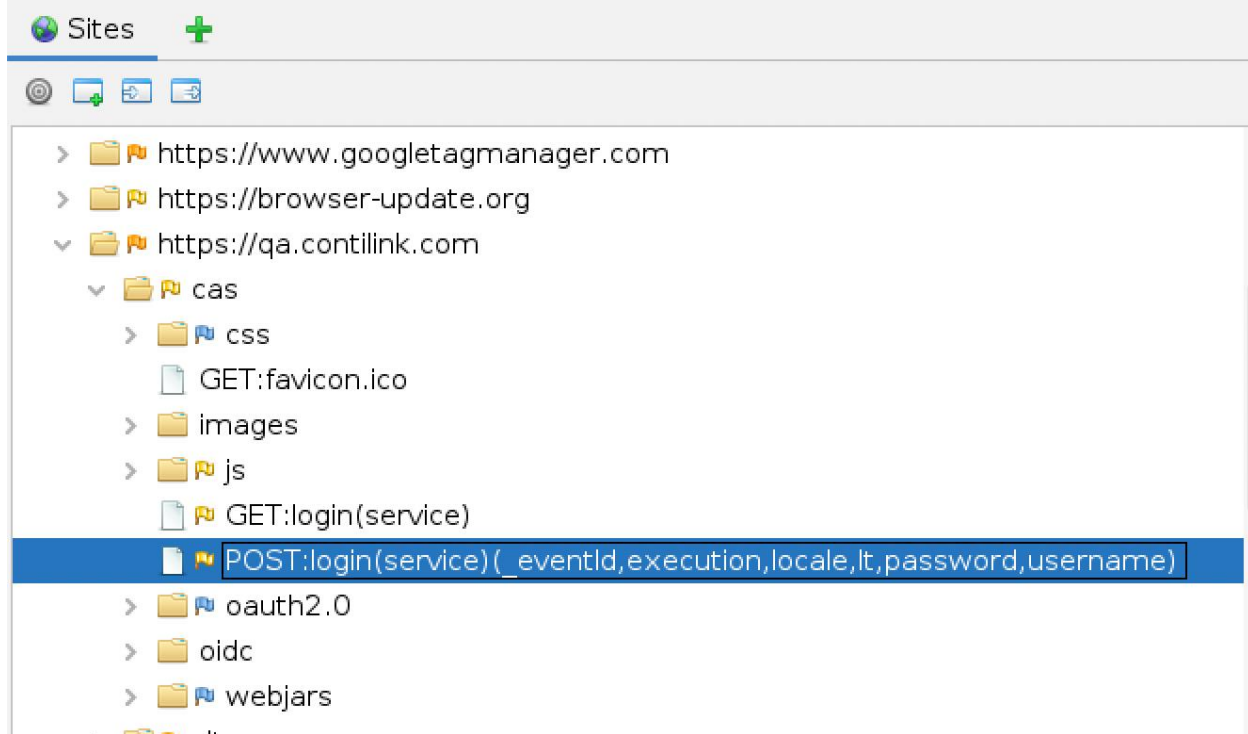


Figure 6: Locating "POST:login..." for <https://qa.contilink.com>

Step 3: Right click on "POST:login..." -> Include in Context -> New Context

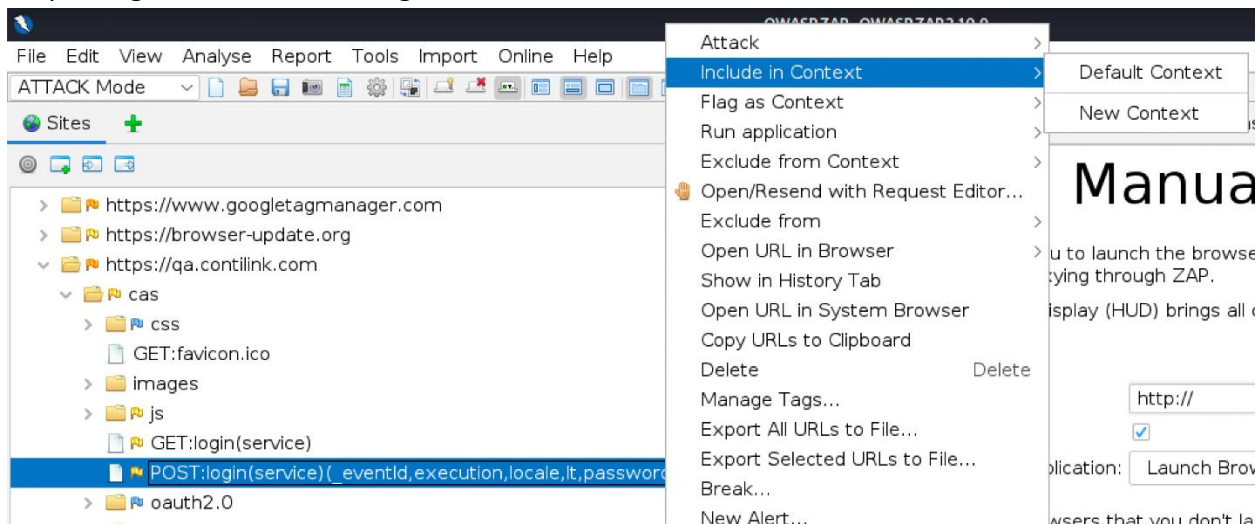


Figure 7: Creating a New Context



Step 9: Under the Users tab, add a new user and enter credentials for the site's login.

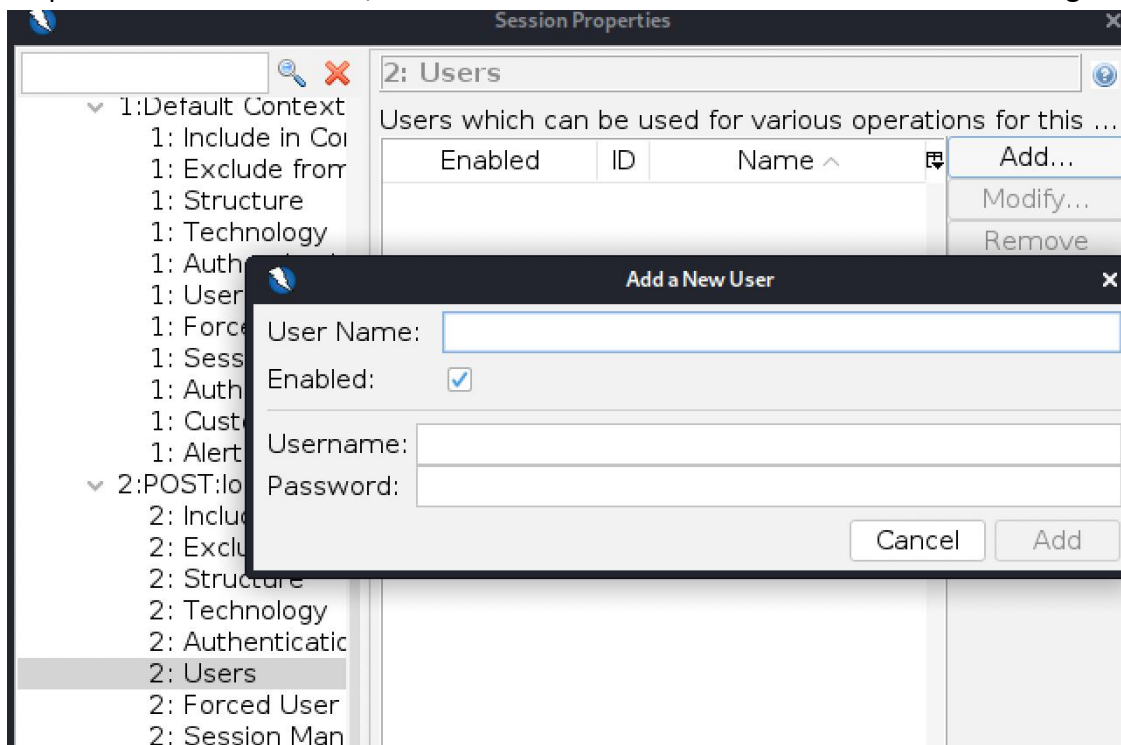


Figure 9:Entering credentials for a new user

Step 10: Exit the Session Properties window by clicking "OK" on the bottom right corner.

**\*A context has now been created.** Proceed with the rest of the steps to perform an active scan with the newly created profile \*



## Active Scan Using a Profile

Step 11: Click on the “Forced User Mode” once to enable. This button can be found around the top right area of the Zap application.

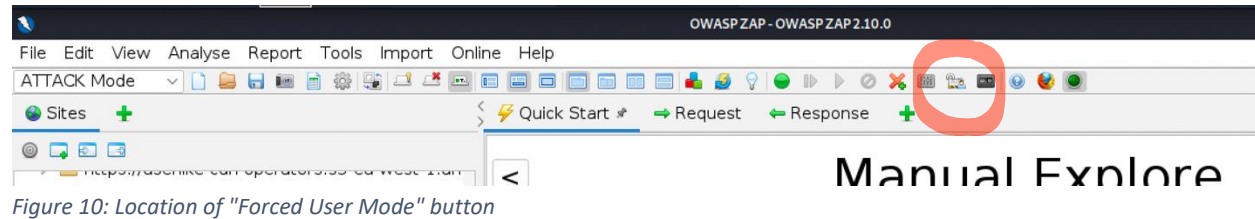


Figure 10: Location of “Forced User Mode” button

Step 12: Right click on the desired site to perform a scan and click on “Flag as Context”, then click on the context you have just created (make sure it includes: “form-based auth login request”).

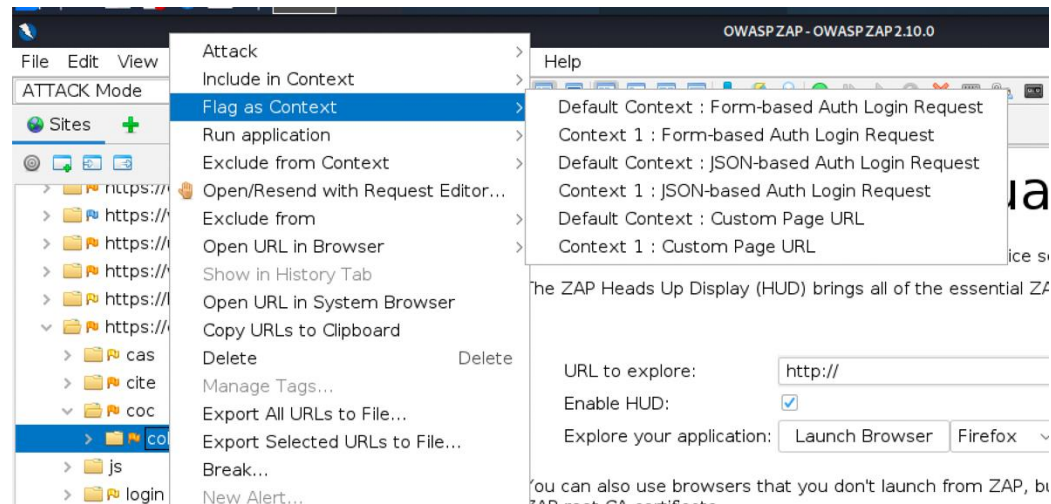


Figure 11: Flag as Context

Step 13: Right click again on the same site and go the “Attack”, then “Active Scan...”.

Step 14: Select the desired Policy, Context, and User for the active scan.

Step 15: Click on “Start Scan”.

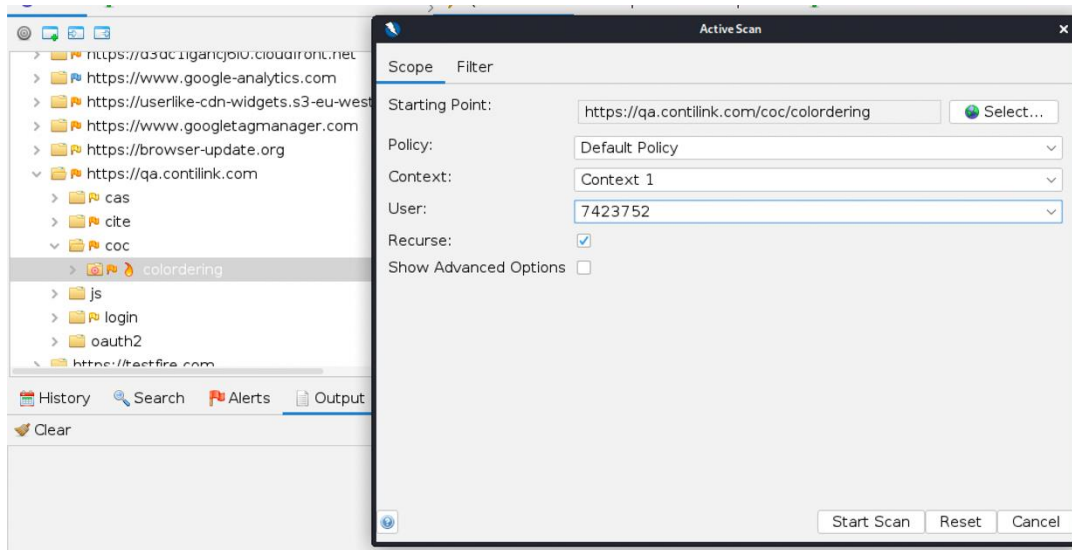


Figure 12: Select the correct settings before starting an active scan