

# Automated Security Testing

## Overview

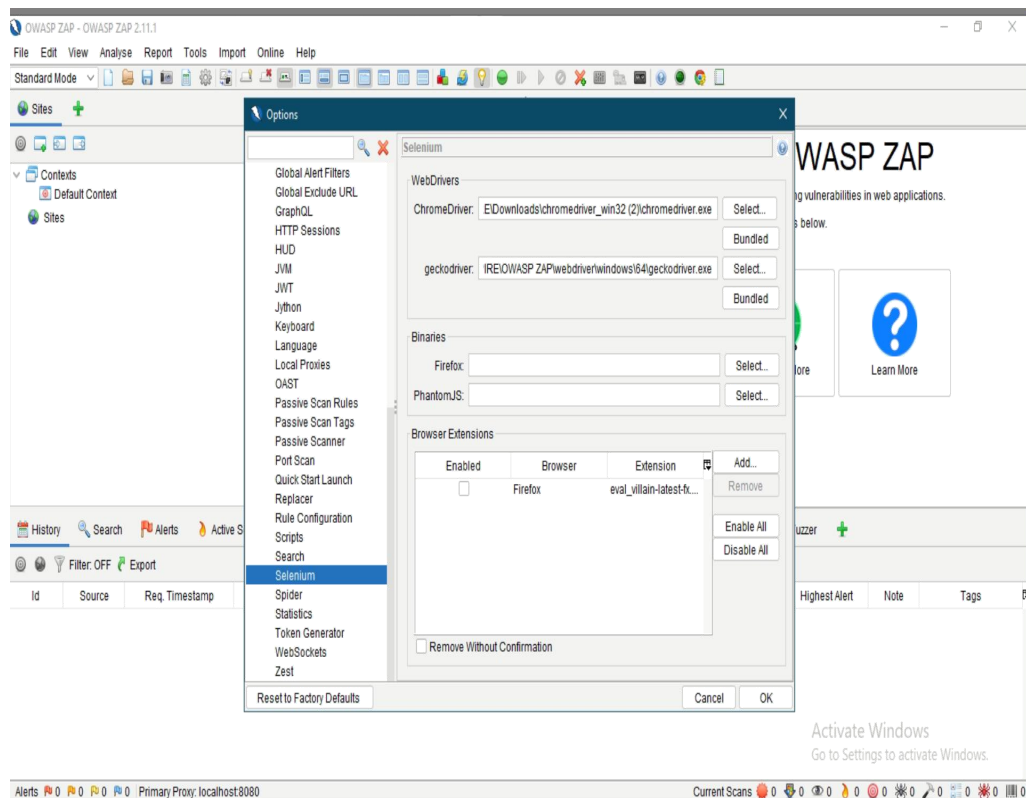
This document is intended to serve as a guide for using OWASP's Zed Attack Proxy (ZAP) tool to perform automated security testing using testproject automation tool and Zap Proxy, even if you don't have a background in security testing.

## Chapter 1: Zap Installation and Setup on Windows

1. Zap was written in Java programming language and running on the Java platform so to use it you need to Download Java 8+ in order to run, check it from this link  
<https://www.oracle.com/java/technologies/downloads/>
2. After that , Download zap installer from this link  
<https://www.zaproxy.org/> , Once the installation is complete, launch ZAP and read the license terms. Click **Agree** if you accept the terms, and ZAP will finish installing, then ZAP will automatically start.
3. Check your chrome browser version and install chrome web driver from this link  
<https://chromedriver.chromium.org/downloads>

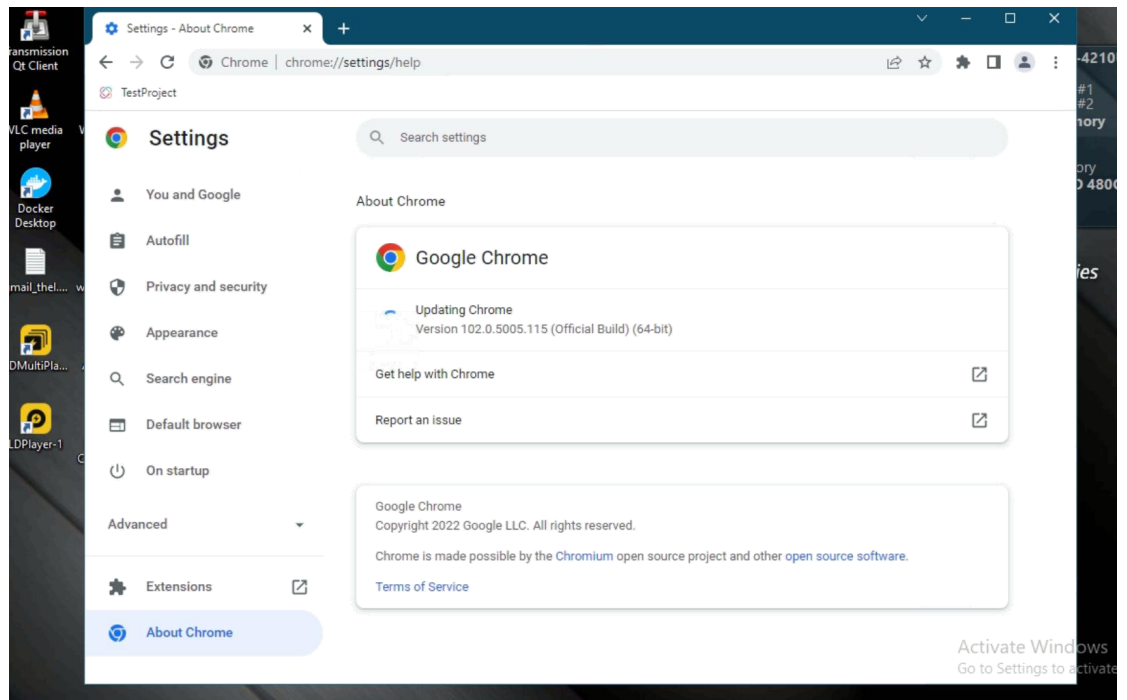
#### 4. Setup zap selenium.

- a) Click **Tools** from the navigation bar.
- b) Select **Options**
- c) Select **Selenium** from the option list.
- d) Select the location of the chrome web driver.
- e) Click **OK** to save changes.

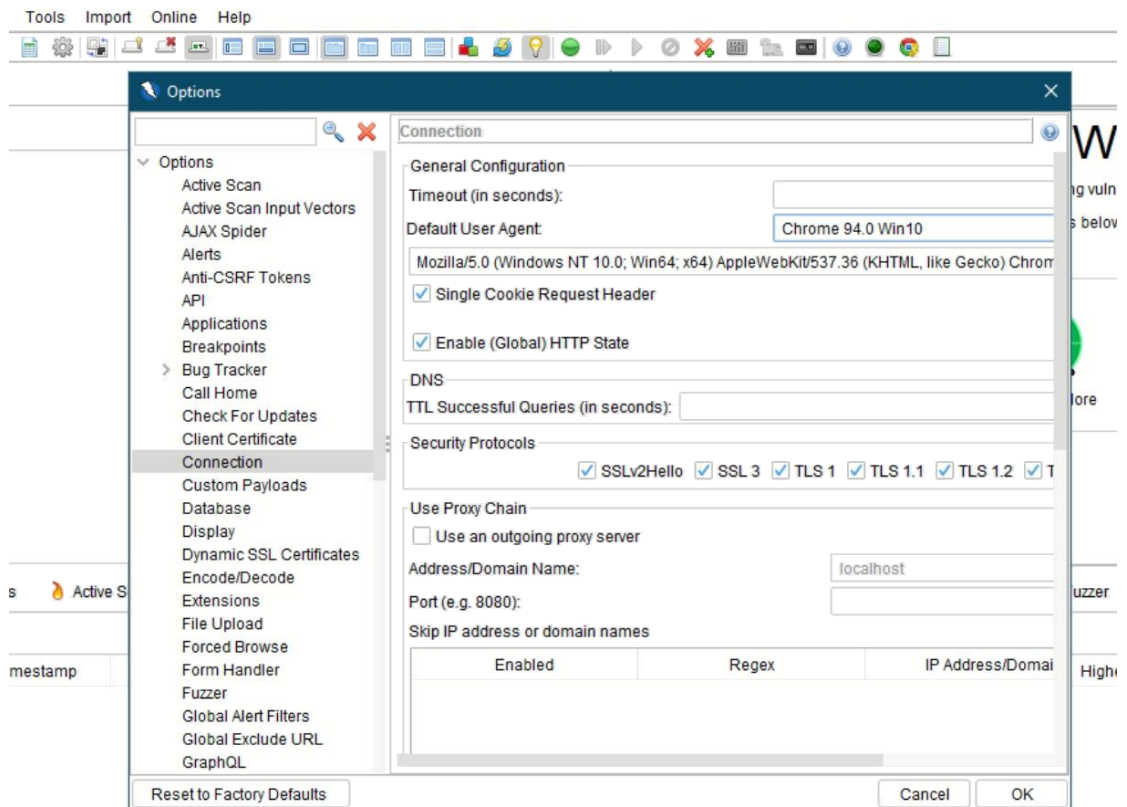


Selenium

5. Setup zap connection. Select the Chrome browser which corresponds or not greater than to your browser version. As my browser version is Chrome 102.0.5005.115 so I will select 94.0 win 10. Please see images below.



My browser version

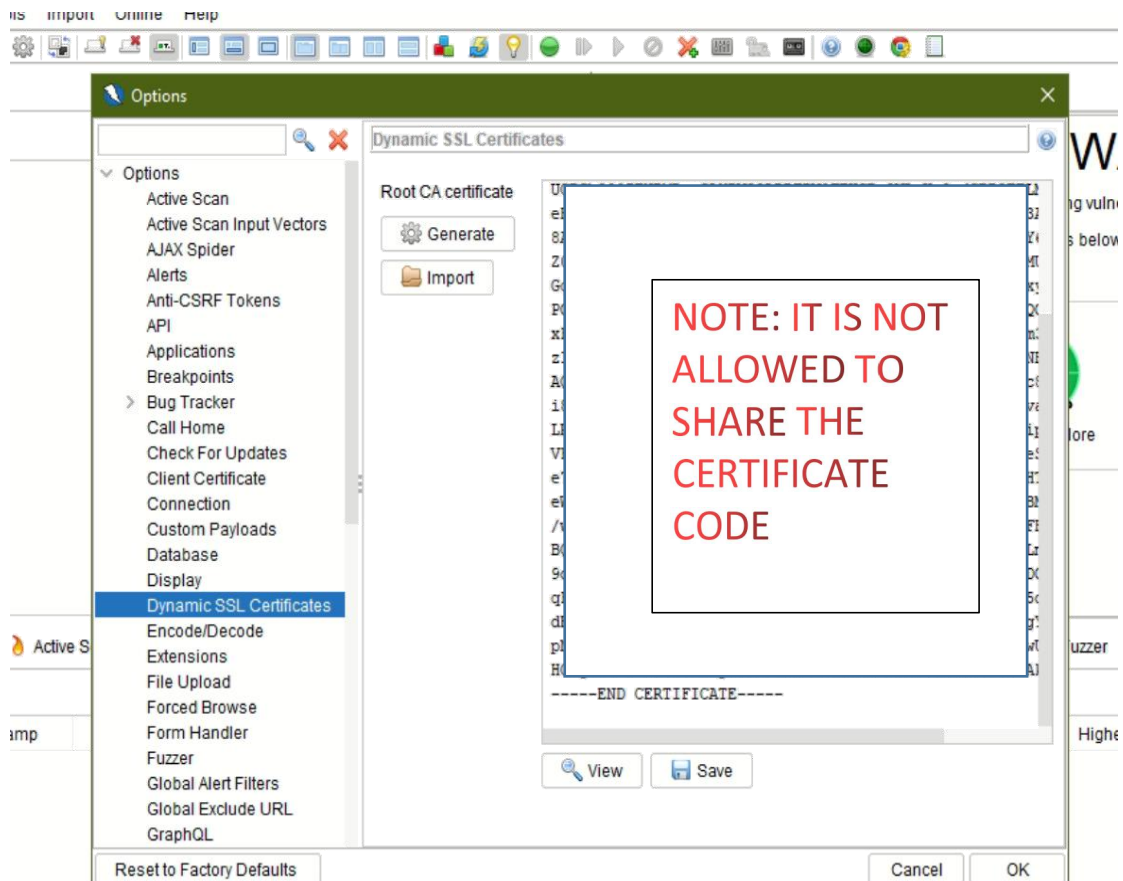


Connection

## 6. Setup Zap Dynamic SSL Certificate .

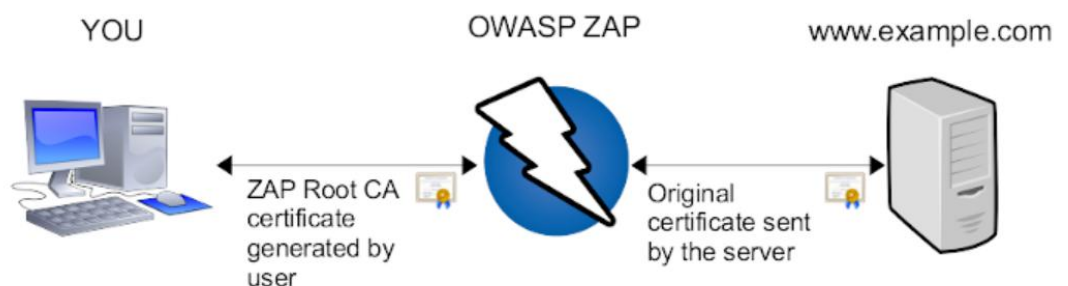
- a) Generate root CA Certificate and Include it on your browser. Check out this link for the step by step guide:

<https://www.zaproxy.org/docs/desktop/ui/dialogs/options/dynsslcert/>



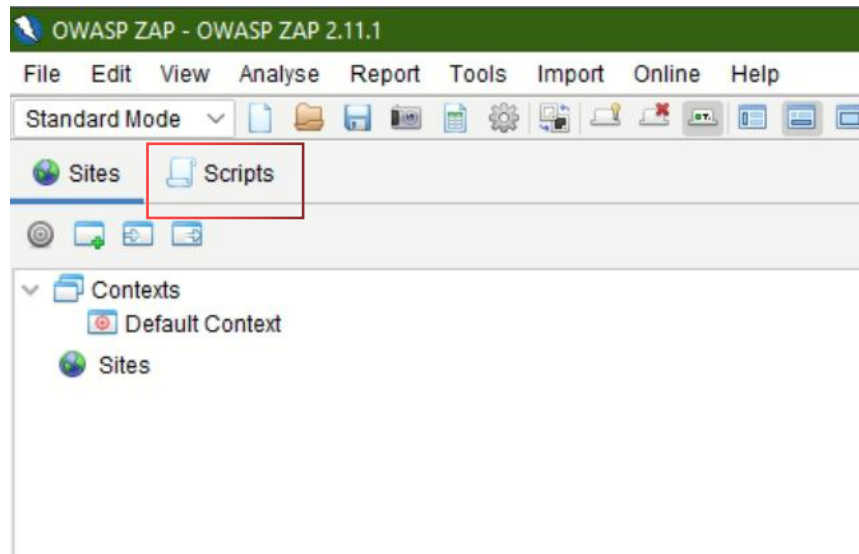
Dynamic SSL Certificate

How ZAP Root CA certificate works.



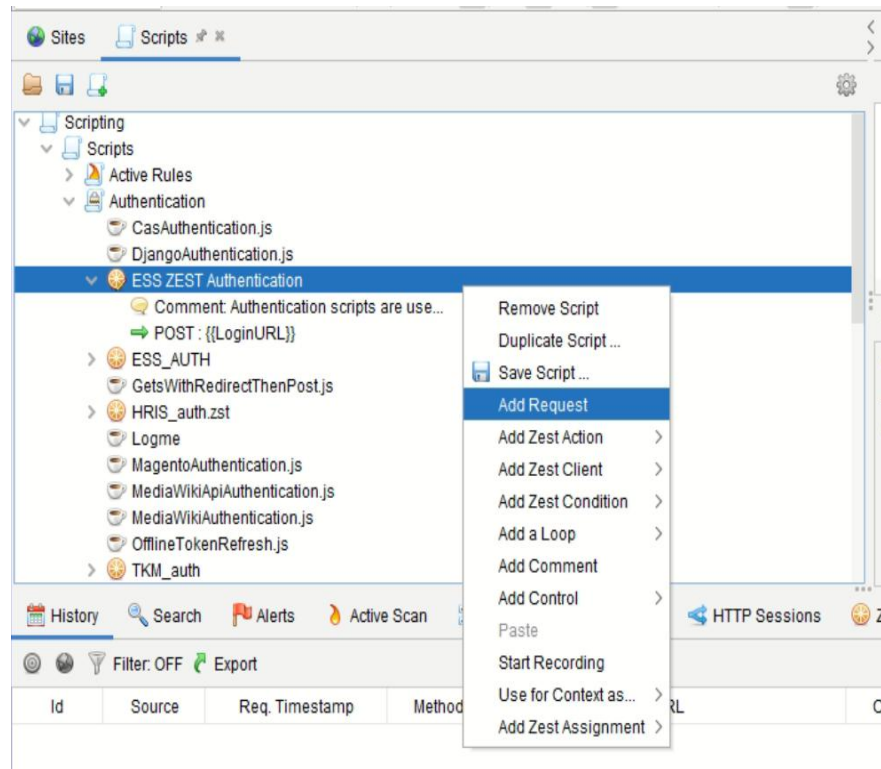
## 7. Setup Script-based Authentication

- a) Click the **Scripts**. It will display the list of ready made scripts but you have to duplicate the script in order to modify and use it on your own.

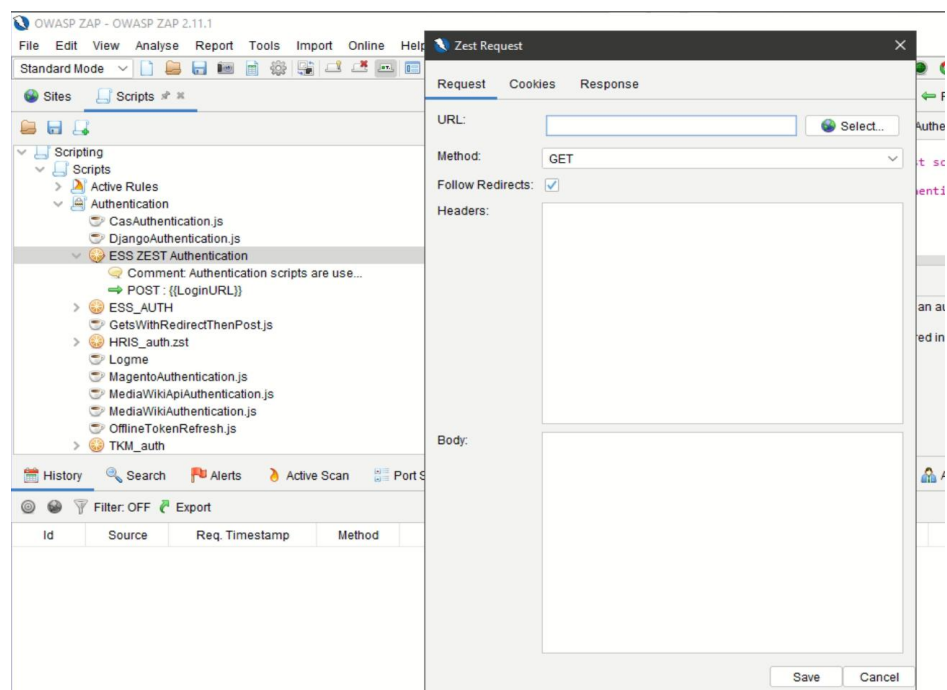


- b) On this Tutorial, We will use **Zest Script** to **authenticate all URL**, that is also included from the testproject automation script.
1. Simply add new authentication script via right clicking the authentication text.
  2. Add Script Name.
  3. Script type should be "**Authentication**"
  4. Script Engine is "**Zest: Mozilla zst**"
  5. Click **Save** and another **Save** button.

6. Now, right click the script you made and select **add request**.



7. Select or enter the URL you want to authenticate then click **save**.



8. Once you have added all the URL then it is time to setup the testproject automation script.

## **Chapter 2: Setup testproject automation script proxied to zap penetration testing tool.**

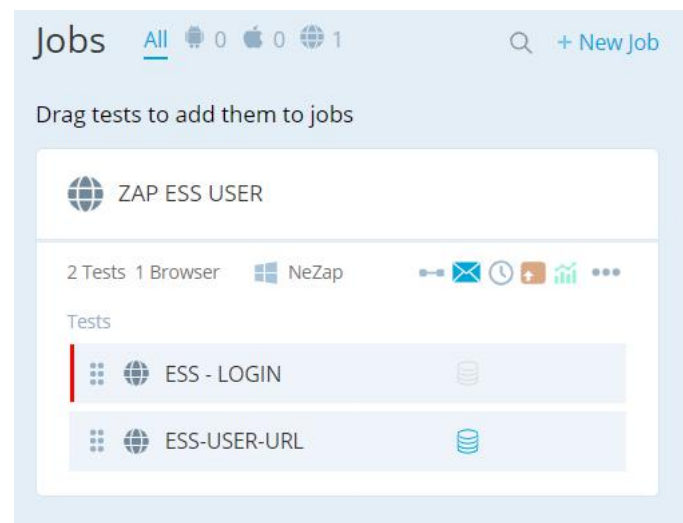
1. Just create test job and include the script into desired capabilities.

```
{
  "browserName": "chrome",
  "version": 98,
  "proxy": {
    "autodetect": false,
    "httpProxy": "localhost:8080",
    "sslProxy": "localhost:8080",
    "proxyType": "manual"
  },
  "goog:chromeOptions": {
    "args": [
      "--ignore-certificate-errors",
      "--start-maximized",
      "--disable-notifications",
      "--allow-running-insecure-content",
      "--disable-web-security",
      "--disable-gpu",
      "--ignore-ssl-errors=yes",
      "--ignore-untrusted-certificate"
    ]
  }
}
```

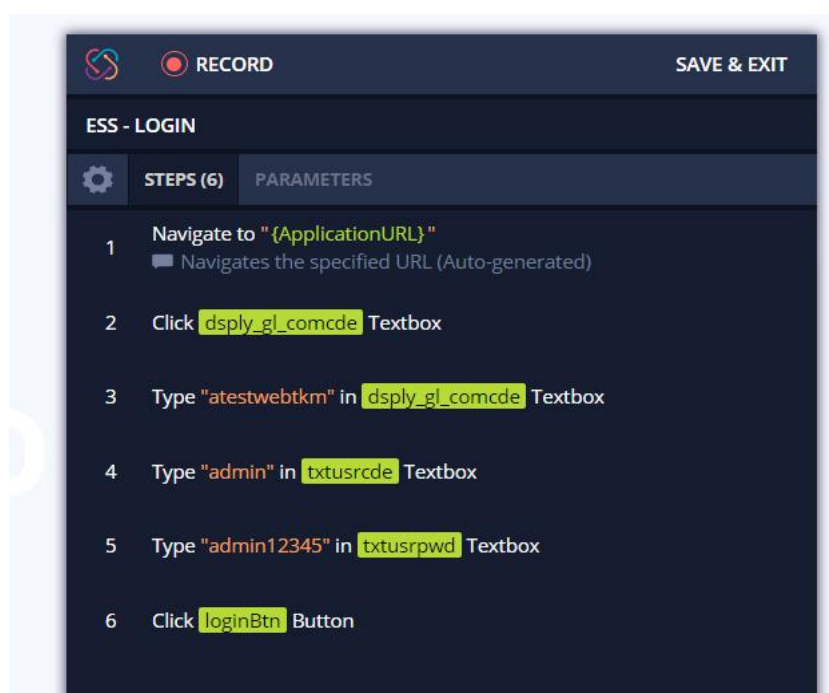
*Note: Make sure that zap is listening to port 8080.*

2. Now , start creating script in test project that will navigate all URL of the web application.

- a) Testdata: All URL of the web application.
- b) Testscript : should login the system and navigate all url.



## Login Sample Script





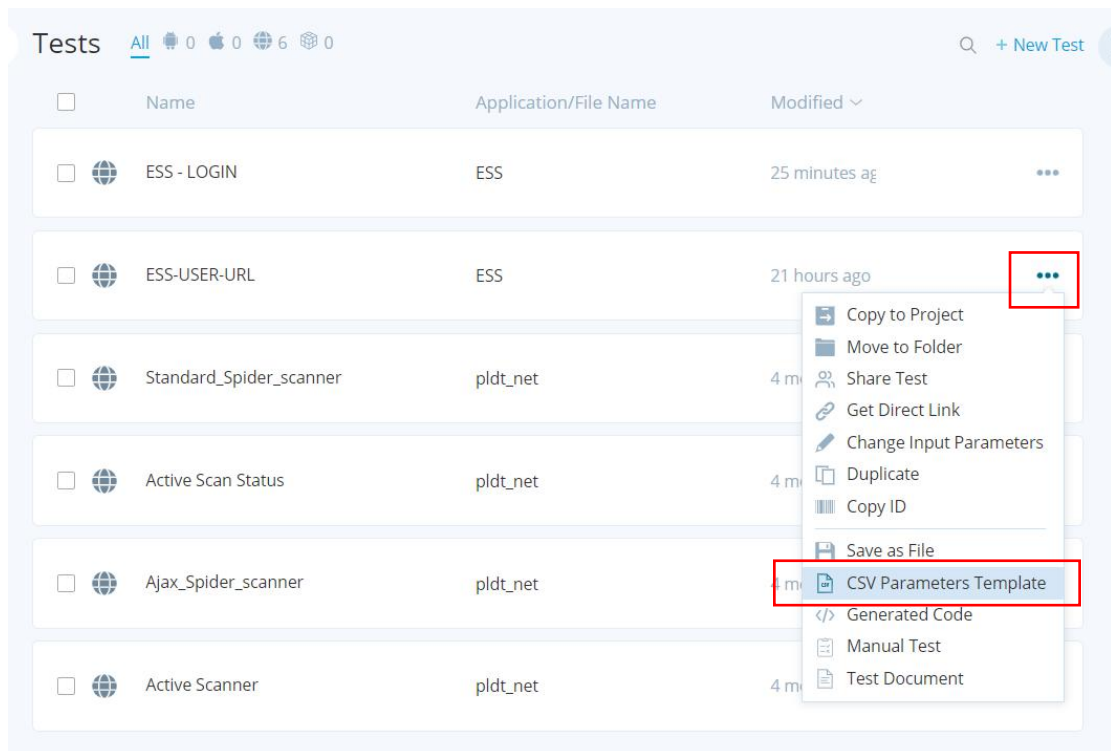
## ESS Navigate to all URL Sample Script



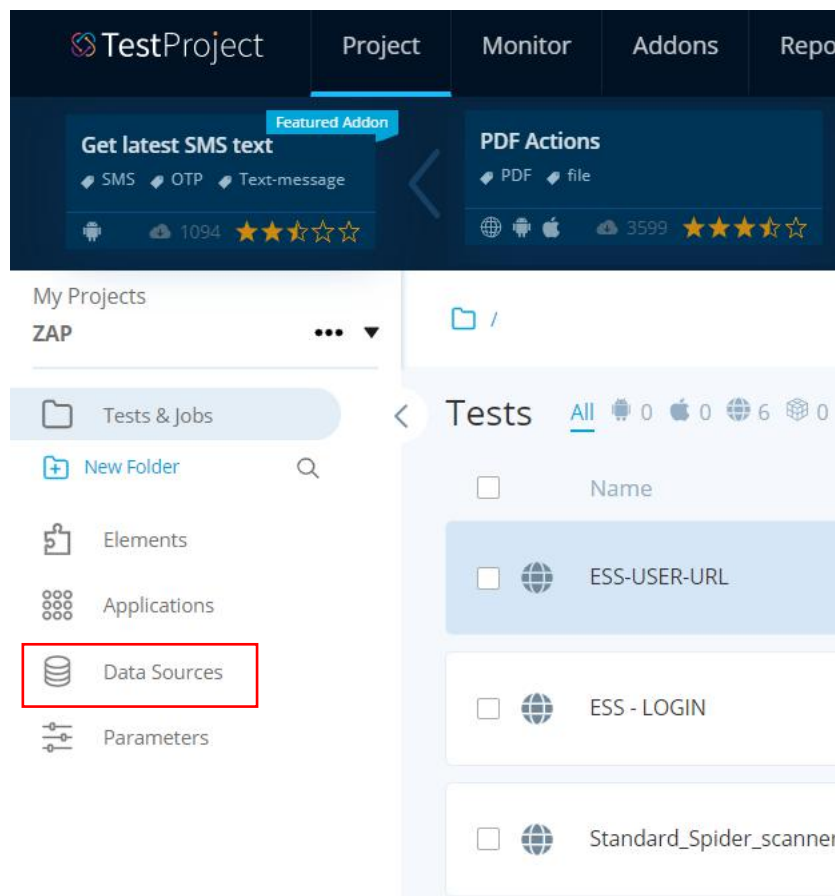
The Data should be parameterized so it needs CSV attachment as its own data source.

## How to create data source and to attach test data to your script?

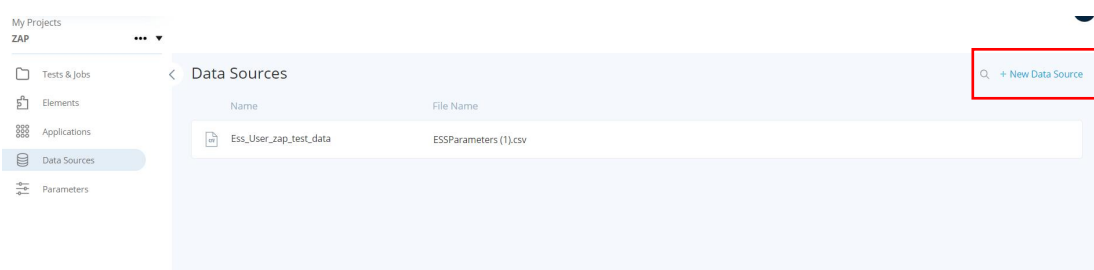
1. Generate template “**CSV Parameters Template**” from the test script that needs URL test data.



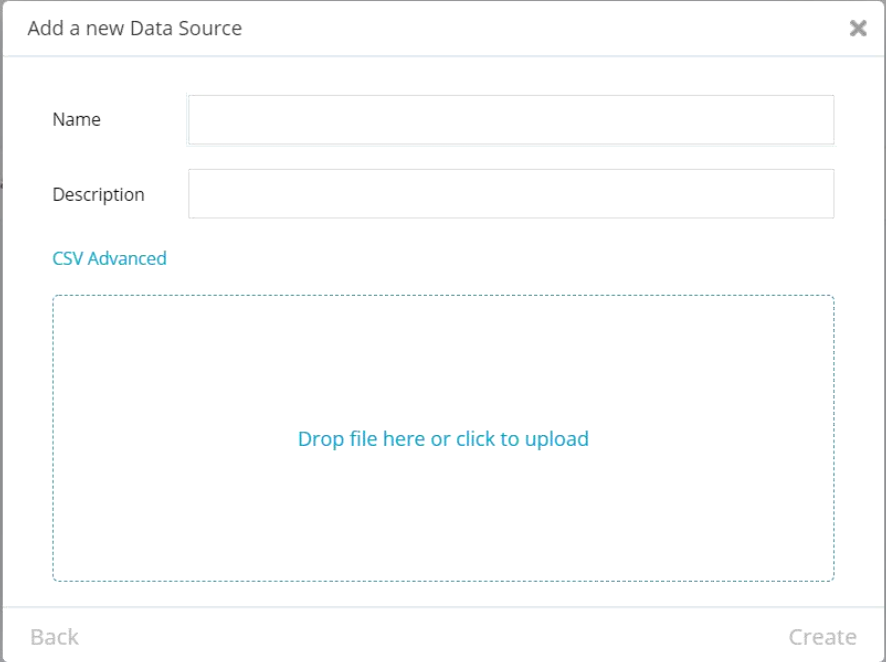
2. Click the **“Data Sources”** on the testproject sidebar menu as shown image below.



3. Add New Data Source

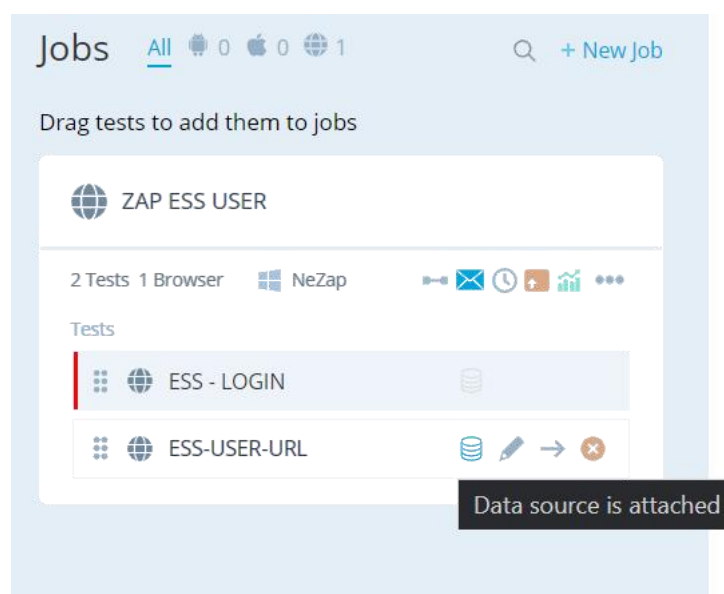


4. Fill the information fields and attach the template.  
Once done then click **Create**.

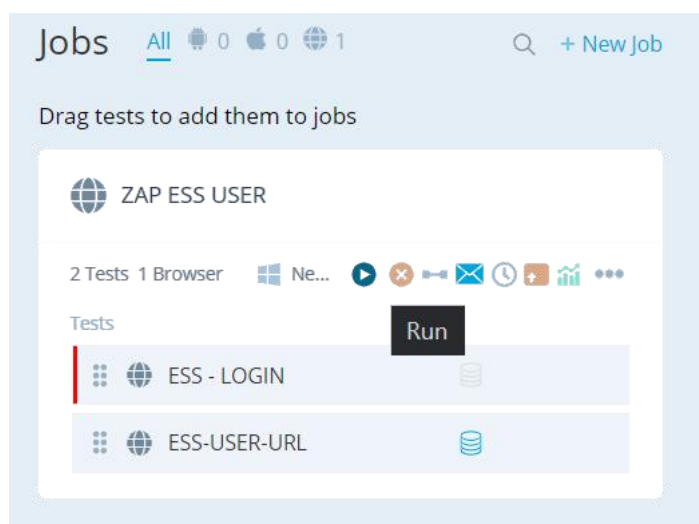


The screenshot shows a modal dialog titled "Add a new Data Source" with a close button (X) in the top right corner. Inside the dialog, there are two input fields: "Name" and "Description". Below these fields is a section labeled "CSV Advanced" in blue text. Underneath is a large dashed rectangular box containing the text "Drop file here or click to upload" in blue. At the bottom of the dialog, there are two buttons: "Back" on the left and "Create" on the right.

5. After that, Go back to the test job and attach the test data.

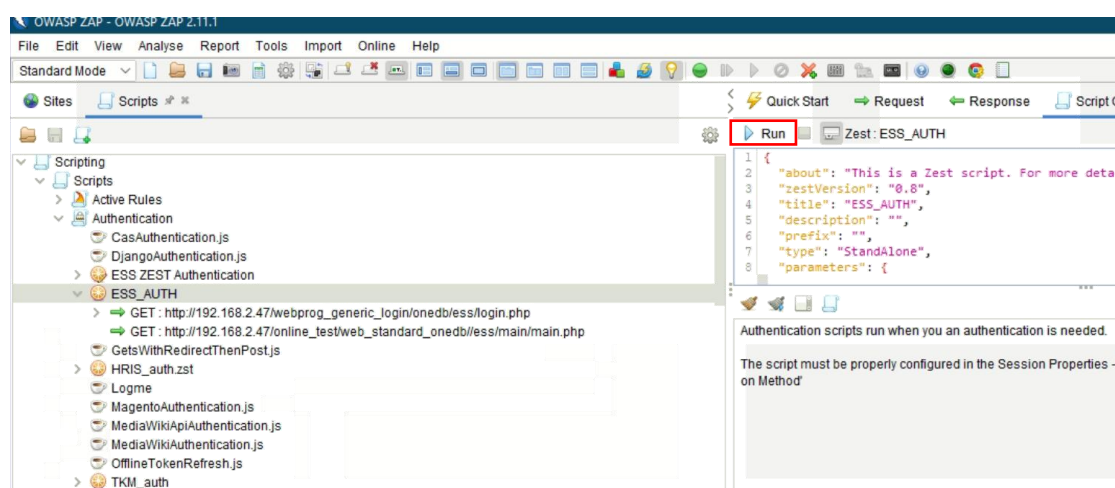


6. It is now the time to Run the script and let test project sends traffic to zap as we have included a capabilities to let zap get the information coming from the system. This process is called **Passive scanning**.



7. For **Spider Scan** and **Active Scan** , You need to run the **Zest Script** . This is to let zap recognized all the URL coming from the passive scan.

a) Click the blue run button as shown below.




8. Now , enter the main url to “**URL to Attack**” of the system. Select **Chrome** as your browser and Click button “**Attack**”

Quick Start Request Response Script Console

## Automated Scan



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

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

URL to attack:   Select...

Use traditional spider: ☐

Use ajax spider: ☒ with Chrome

 Attack  Stop

Progress: Not started

Repeat Step Number 2 from chapter 2 to conduct another security test.

We are done , Happy Testing!