Options:

1.Activscan:

Active scan is an attack on those targets to find the potential vulnerabilities using the known attacks.

Drawbacks:

It cannot perform logical vulnerabilities such as Broken Access Control.

2.Active Scan Input vectors:

These are the elements that the active scan will attack.

Scanning all the elements will take a long time but not scanning some elements may cause some vulnerabilities to miss.

3.Ajax Spiders:

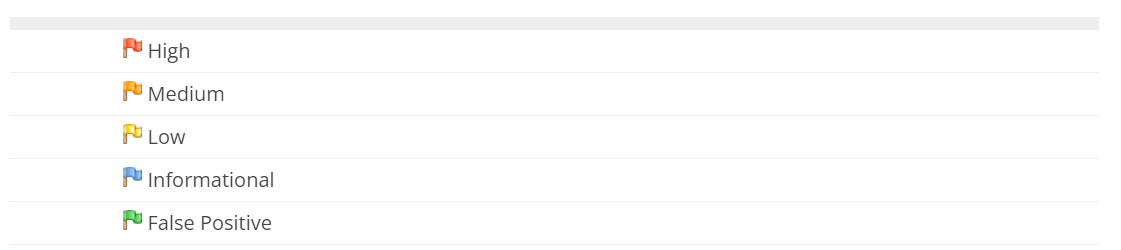
The AJAX Spider allows you to crawl web applications written in AJAX in far more depth than the native Spider. Use the AJAX Spider if you have web applications written in AJAX.

You should also use the native Spider as well for complete coverage of a web application (e.g., to cover HTML comments).

4.Alerts:

i. An alert is a potential vulnerability and is associated with a specific request.

A request can have more than one alert.



ii. Alerts can be raised by various ZAP components, including but not limited to: active scanning, passive scanning, scripts, by addons (extensions), or manually using the Add Alert dialog (which also allows you to update or change alert details/information).

iii. Alerts are flagged in the History tab with a flag which indicates the highest risk alert.

iv. All alerts are listed in the Alerts tab and a count of the total number of alerts by risk is shown in the footer.

**5.Anti-CSRF tokens:**

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they’re currently authenticated.

With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker’s choosing.

If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth.

If the victim is an administrative account, CSRF can compromise the entire web application.

**Options in Anti-CSRF token screen:**

1.Options:

The form POST parameter names that should be treated as anti CSRF tokens.

2.Partial Matches:

Defines if the form POST parameter names should be treated as anti CSRF tokens if they include one of the tokens (instead of requiring an exact match).

**Applications:**

This screen allows you to configure the applications that can be invoked.

**Automation:**

If selected, then the Automation tab will automatically load the last plan opened when the GUI starts. This can be useful if you need to regularly use the same plan.

**Break Points:**

A breakpoint allows you to intercept a request from your browser and to change it before is is submitted to the web application you are testing.