Arachni Scanner plugin

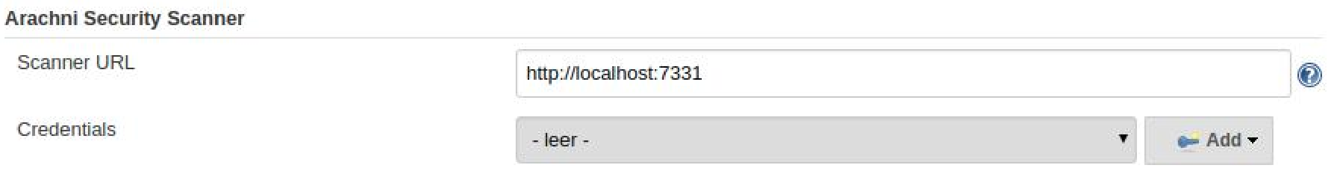
With this plugin you got a very simple integration of the Arachni Security Scanner in your Jenkins jobs. The REST API of the Arachni Security Scanner is used for communication, so a running Arachni REST Server is a prerequisite.

Features:

- Starts a new scan on an Arachni Server
- Monitors the scan status every 5 seconds
- Downloads the HTML scan report from Arachni Server
- Scope of the scan is configurable
- Supports Basic Authentication
- Pipeline compatibility

Configuration and usage

At first configure the URL of your Arachni REST Server under the Jenkins system configuration page.



Arachni Security Scanner

Scanner URL: http://localhost:7331

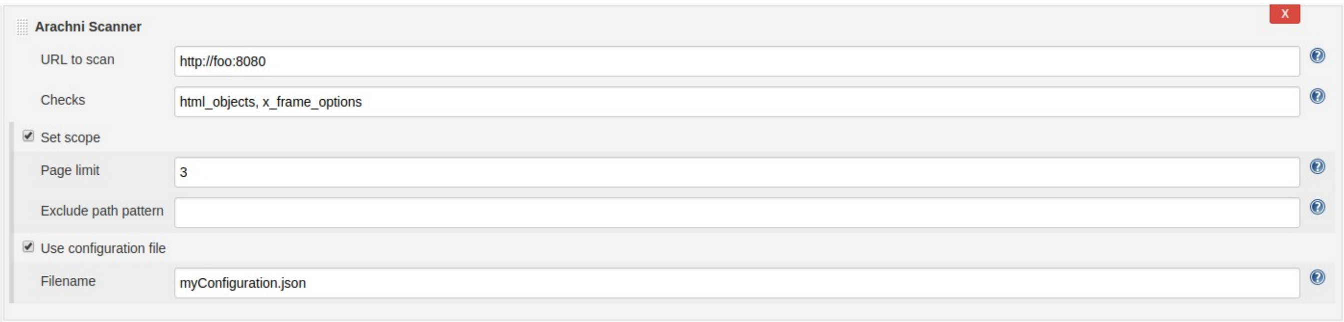
Credentials: - leer -

If your Arachni Server is secured with Basic Authentication then select the credentials from credentials plugin.

In your job configuration select the **Arachni Scanner** build step and enter the URL of the site you want to scan. Leave the Checks field blank (or enter a *) to run all checks or specify a comma separated list with the checks to use. Sometimes a scan can takes very long, so you have the option to specify a scope.

To get the full control over the scan configuration, check the 'Use configuration file' and enter the name of your own configuration file. In the file you can use the full parameter set of Arachni. The settings from the file will be merged with the field settings. If the same parameter is specified in fields and configuration file, the setting from the file wins.

See the Wiki page of the Arachni Security Scanner for more information.



Arachni Scanner

URL to scan: http://foo:8080

Checks: html_objects, x_frame_options

☑ Set scope

Page limit: 3

Exclude path pattern:

☑ Use configuration file

Filename: myConfiguration.json

When the job is running the plugin writes the scan status every 5 seconds to the console log until the scan ends. If you abort the job then the scan on the Arachni Server will be also aborted. At last the HTML scan report will be downloaded from the server and stored in the workspace under the filename **arachni-report-html.zip**.

Pipeline

Below you find a simple pipeline script to configure the Arachni Scanner Plugin.

```
pipeline {
   agent any
   stages {
      stage('Scanning') {
         steps {
            arachniScanner checks: '*', scope: [pageLimit: 3], url: 'http://foo:8080', userConfig: [filename: 'myConfiguration.json'], format: 'json'
         }
      }
   }
}
```

Release history:

- **1.0.0**
    - Credentials plugin is used to store username and password. Values from older configurations will be migrated.
- **0.9.7**
    - Supports more report formats (html, json, xml, yaml)
- **0.9.6**
    - Bugfix: Fix a problem for Jenkins versions newer than 2.107.1 (JEP-200)
- **0.9.5**
    - Support configuration files
- **0.9.4**
    - Support to specify checks
    - Support pipeline