DAST Integration

Avi Technical Reference (v20.1)

DAST Integration

view online

Overview

A Dynamic Application Security Testing (DAST) scanner is a tool to identify potential security issues in applications.

Avi Vantage provides a script called `avi-iwaf-vpatch.py` that imports a DAST scanner results. The imported results are used to construct iWAF Policy that protects from the security threats found by the scanner. The technique is often called virtual patching.

Avi Vantage supports the following DAST scanners:

- OWASP ZAP Attack Proxy
- Qualys Web App Scanning

The supported scanner format is an XML file containing scanner result report.

Workflow

The following are the steps to integrate DAST:

1. Run a scan against a web application not protected by iWAF.
2. If you find any issues, the `avi-iwaf-vpatch.py` uses the output of the scan to generate iWAF Policy rules.
3. Enable iWAF.
4. Scan again. The subsequent scans will not report issues for problems handled by iWAF Policy.

The `avi-iwaf-vpatch.py` generates Avi Vantage iWAF Policy Positive Security rules. It creates a iWAF Policy Positive Security group containing all the rules covering DAST scan issues. The `avi-iwaf-vpatch.py` automatically creates Positive Security locations for each vulnerable URL reported by the scanner, and Positive Security rules for each supported issue.

Note that `avi-iwaf-vpatch.py` does not generate rules to protect from all the potential issues found. The script will generate rules related to parameter security, for instance, URL parameters, HTML form fields and XML or JSON attributes.

The script is delivered as part of Avi SDK, available on Avi Controller in the DAST directory.

Usage

You can use the following format for python:

```
avi-iwaf-vpatch.py PARAMETERS FILENAME
```

where,

PARAMETERS are as follows:

- -c ? hostname or IP address of the Avi Controller to connect to
- -u ? username to log in to Avi Controller
- -p ? password
- -t ? tenant
- -g ? (optional) iWAF Policy PSM group name
- -v ? verbose output
- -f ? force apply changes

FILENAME is a DAST scan output in XML format.

When you run the script without -f option, the system will only print what it would do. Only after --force is set, the system will attempt to connect to the Avi Controller and write iWAF Policy.

If group name is not specified using -g then the system will create a group named zap or qualysweb, depending on the scanner being used. Scanner type is auto detected based on the XML file format.

Example

```
python ./avi-iwaf-vpatch.py -c 127.0.0.1 -g zap_group ./zap_results.xml --verbose
```

Security Issues handled

DAST scanner can report multiple issues that are not handled by the `avi-iwaf-vpatch.py` script. Many of them may be beyond the scope of iWAF. However, some of them can be mitigated by appropriate settings in Avi Vantage Load Balancer. For instance,

- Issues related to clickjacking can be mitigated by adding a X-Frame-Options HTTP header.
- In Avi admin UI, navigate to Virtualservice/Policies/HTTP Response action and select Add Header option.
- Issues related to cookies can be like "A cookie has been set without the HttpOnly flag" or "Cookie Does Not Contain The 'secure' Attribute". These could be set by selecting appropriate options in the Application Profile/Security.