Lesson 06 Demo 04

Performing DAST for a Docker Container Using OWASP ZAP

Objective: To demonstrate the deployment and utilization of a dynamic application security testing (DAST) tool using Docker

Tools required: Docker and Command Line Interface (CLI)

Prerequisites: None

Steps to be followed:

1. Set up and start the ZAP Docker container
2. Run the security scan and retrieve the report

Step 1: Set up and start the ZAP Docker container

1.1 Run the following command to pull a ZAP Docker image:
docker pull ghcr.io/zaproxy/zaproxy:stable

```
root@ip-172-31-29-27:/home/labuser# docker pull ghcr.io/zaproxy/zaproxy:stable
stable: Pulling from zaproxy/zaproxy
3f559f8680cb: Pull complete
567725cf76e2: Pull complete
23a96d0a1583: Pull complete
a94c9f57bb4b: Pull complete
14c570a580f5: Pull complete
97fea53f3427: Pull complete
4f4fb700ef54: Pull complete
e9bd3953f779: Pull complete
5ee4d086ae6d: Pull complete
fcc950e2dc01: Pull complete
f6d0d1a038b1: Pull complete
f65b32df72c0: Pull complete
86ff150ffeda: Pull complete
bcfa8d0a4ac5: Pull complete
a7fa8af87056: Pull complete
75254b018c1e: Pull complete
7551c4bd3d7b: Pull complete
538fc63074a3: Pull complete
63a4e9393bd8: Pull complete
c5fa38f86bf0: Pull complete
Digest: sha256:b8ced82260e2f752e7db9eca9243ddef27f2d706f9186afb3a4444c583eb3eb6
Status: Downloaded newer image for ghcr.io/zaproxy/zaproxy:stable
ghcr.io/zaproxy/zaproxy:stable
root@ip-172-31-29-27:/home/labuser#
```

1.2 Run the following command to start the ZAP container
docker run -dt --name cont1 ghcr.io/zaproxy/zaproxy:stable /bin/bash

```
root@ip-172-31-29-27:/home/labuser# docker run -dt --name cont1 ghcr.io/zaproxy/zaproxy:stable /bin/bash
e3b5119591fd077a102e4f6a8556e73a92b9047899caac1fdbe5b16789291976
root@ip-172-31-29-27:/home/labuser#
```

1.3 Run the following command to create ZAP workspace for scanning the vulnerabilities:
docker exec cont1 mkdir /zap/wrk

```
root@ip-172-31-29-27:/home/labuser# docker exec cont1 mkdir /zap/wrk
root@ip-172-31-29-27:/home/labuser#
```

Step 2: Run the security scan and retrieve the report

2.1 Run the following command to connect to the container:
docker exec -it cont1 sh

```
root@ip-172-31-29-27:/home/labuser# docker exec -it cont1 sh
```

2.2 Run the following command to initiate scanning of the workspace:
zap-baseline.py -t https://medium.com/ -r report.html -I

```
$ zap-baseline.py -t https://medium.com/ -r report.html -I
Using the Automation Framework


Total of 577 URLs
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
```

2.3 Execute the following command to copy the report to the Docker host:
docker cp cont1:/zap/wrk/report.html /tmp/report.html

```
root@ip-172-31-29-27:/home/labuser# docker cp cont1:/zap/wrk/report.html /tmp/report.html~
Successfully copied 201kB to /tmp/report.html~
root@ip-172-31-29-27:/home/labuser#
```

By following the steps above, you have successfully pulled a Docker image, conducted a vulnerability scan, and generated a report using the OWASP ZAP tool for dynamic application security testing (DAST).