DAST Scan using OWASP ZAP & Hosting Report with Apache on EC2

## Step 1: Set Proper Permissions for Current Directory

This makes your current directory readable and writable by any user — including the 'zap' user inside the Docker container — so ZAP can save the report here.

chmod 777 $(pwd)

## Step 2: Run OWASP ZAP Scan and Generate HTML Report

This runs a quick passive scan on the provided URL and saves the report in your current directory as zap-report.html.

docker run --rm -v $(pwd):/zap/wrk ghcr.io/zaproxy/zaproxy:stable zap.sh \  
 -cmd -quickurl http://43.205.196.159:3015/ -quickout /zap/wrk/zap-report.html

## Step 3: Install Apache Web Server (HTTPD)

Apache allows us to host the HTML report so it can be accessed in a browser.

sudo yum install httpd -y

## Step 4: Start Apache Service

This starts the Apache server, making /var/www/html/ available over HTTP.

sudo service httpd start

## Step 5: Move the ZAP Report to Apache's Web Root

Apache serves content from /var/www/html/. Moving the report here allows you to view it via browser.

sudo mv /home/ec2-user/Dimple-CapsuleProject/zap-report.html /var/www/html/

## Step 6: Ensure Port 80 is Open in Security Group

This allows the report to be accessible publicly via a web browser.

Go to AWS EC2 Console → Security Groups → Inbound Rules → Add HTTP (Port 80) from 0.0.0.0/0

## Step 7: Access the Report from Browser

Open this link in your browser to view the report.

http://<your-ec2-public-ip>/zap-report.html