1. X-ray from JFROG
2. Docker security for bench

1) SAST Hands on

=================

[Source code] https://github.com/juice-shop/juice-shop

Step1: git clone https://github.com/juice-shop/juice-shop

[SAST tool link] https://github.com/ZupIT/horusec

Step2: apt-get update ; apt install jq

Step3: curl -fsSL https://raw.githubusercontent.com/ZupIT/horusec/master/deployments/scripts/install.sh | bash -s latest

horusec version

Step3: horusec start -D -e="true" -p ./

2) DAST hands on

================

Run application as container

Step1: docker run --rm -idt -p 3000:3000 bkimminich/juice-shop

Step2: docker run -t ghcr.io/zaproxy/zaproxy:stable zap-baseline.py -t <Application URL>

docker run -t ghcr.io/zaproxy/zaproxy:stable zap-baseline.py -t http://ip172-18-0-100-ckucfiufml8g009dm00g-3000.direct.labs.play-with-docker.com/#/

WARN-NEW: Dangerous JS Functions [10110] x 2

http://ip172-18-0-100-ckucfiufml8g009dm00g-3000.direct.labs.play-with-docker.com/main.js (200 OK)

http://ip172-18-0-100-ckucfiufml8g009dm00g-3000.direct.labs.play-with-docker.com/vendor.js (200 OK)

FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 9 WARN-INPROG: 0 INFO: 0 IGNORE: 0 PASS: 56

3) SCA Hands on

===============

[Source code] https://github.com/juice-shop/juice-shop

Step1: git clone https://github.com/juice-shop/juice-shop

Step2: cd juice-shop/frontend/ ; vi package.json

in package.json we have defined our dependancy.

Step3: add dependacy "lodash": "0.5.0",

lodash: Lodash is a JavaScript library which provides utility functions for common programming tasks using the functional programming paradigm

Step4: apt-get update ; apt install npm

Step5: npm install

added 1479 packages from 2458 contributors and audited 1521 packages in 110.665s

260 packages are looking for funding

run `npm fund` for details

found 11 vulnerabilities (10 moderate, 1 high)

run `npm audit fix` to fix them, or `npm audit` for details