Activity: Static Analysis with OWASP SonarQube

Setting up OWASP SonarQube

1. Download and install **Docker Desktop** **(https://www.docker.com/products/docker-desktop)**. You will need to sign-up for the Docker service. I left the default settings in place when installing on my Windows machine.
   - Be forewarned that this is a large and resource-intensive program.
   - You may be required to restart and enable virtualization and Hyper-V if using windows.
   - **<Optional>** For the full experience, also download and install **node.js** **(https://nodejs.org/en/download/)**, which SonarQube uses to help scan JavaScript files..
2. Once Docker is installed, open a Terminal/Command Prompt and run the commands below. This will download and run the **OWASP SonarQube** **(https://hub.docker.com/r/owasp/sonarqube/)** docker container. This may take some time.

```
docker pull owasp/sonarqube
docker run -d -p 9000:9000 -p 9092:9092 owasp/sonarqube
```

3. Visit **http://localhost:9000** **(http://localhost:9000)** once everything is installed and running. You should the SonarQube web interface.
4. Click the 'Login' button and use admin/admin as the username/password.
5. Skip the Tutorial asking for a token.
6. Go to Administration -> Marketplace, then click the "Installed" button under Plugins. Do the following:
   - '**Uninstall**' GitLab and FindBugs
   - '**Update**' SonarJava, SonarPHP, ad SonarPython
   - There should be a blue banner near the top of the screen now. Click 'Restart' to process the changes. It will take a few minutes. Wait for hte server to finish restarting before proceeding.

General instructions on starting/stopping the SonarQube container

- Docker commands are always run from the Terminal / Command Prompt / PowerShell
- To start: `docker run -d -p 9000:9000 -p 9092:9092 owasp/sonarqube`
- To stop:
  - `docker container ls`. Note either the CONTAINER ID (first column) or the NAMES (last column) of your SonarQube container.
  - `docker stop <container id>` or `docker stop <name>`

Running the scan on DVWA

We do this from the command line, and the results are sent to the web application for browsing.

1. Download the **SonarQube Scanner (https://docs.sonarqube.org/display/SCAN/Analyzing+with+SonarQube+Scanner)** for your operating system and unzip it. Make note of the path to the bin directory, e.g., `C:\Users\laymanl\Downloads\sonar-scanner-cli-3.3.0.1492-windows\bin`
2. Find your DVWA web application on your disk. Find the root of the xampp directory containin DVWA and go /xampp-portable/htdocs/dvwa
3. In this directory, create the necessary config file for SonarQube named `sonar-project.properties`. Edit the file in a text editor and paste in the following:

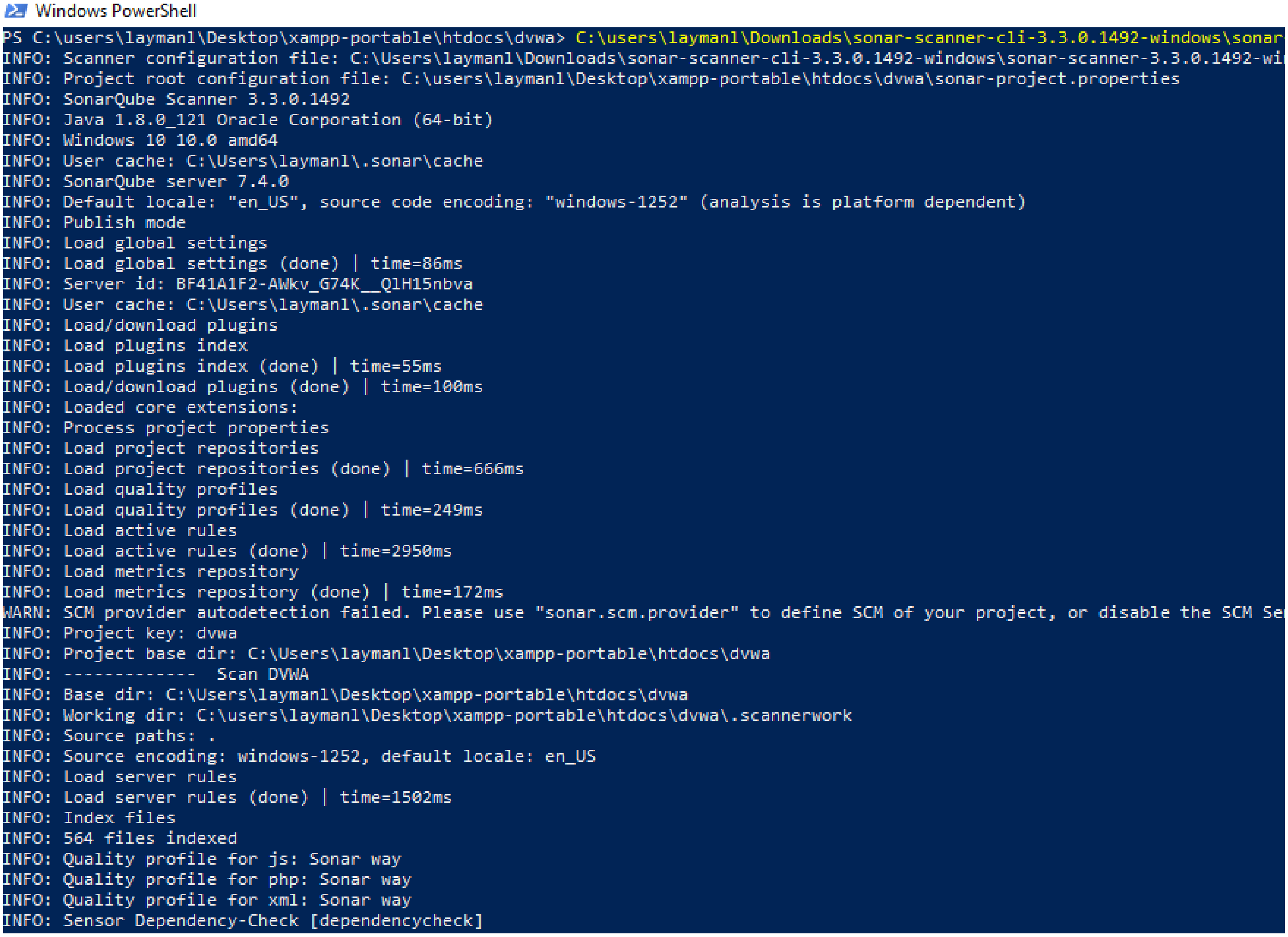
```
# must be unique in a given SonarQube instance
sonar.projectKey=dvwa
# this is the name and version displayed in the SonarQube UI. Was mandatory prior to SonarQube 6.1.
sonar.projectName=DVWA
sonar.projectVersion=1.10

# Path is relative to the sonar-project.properties file. Replace "\" by "/" on Windows.
# This property is optional if sonar.modules is set.
sonar.sources=.

# Encoding of the source code. Default is default system encoding
#sonar.sourceEncoding=UTF-8
```

4. Verify that SonarQube is till running by visiting **http://localhost:9000 (http://localhost:9000)**.
5. Open a Terminal / Command Prompt and browse to your xampp-portable/htdocs/dvwa directory. Launch the SonarScanner by invoking conar-scanner.bat (Windows) or sonar-scanner.sh (Mac/Linux) from the bin directory, e.g., `C:\users\laymanl\Downloads\sonar-scanner-cli-3.3.0.1492-windows\bin\sonar-scanner.bat`. The screenshot below shows an example of executing the program. It will take some time

to complete the scan.



```
PS C:\users\laymanl\Desktop\xampp-portable\htdocs\dvwa> C:\users\laymanl\Downloads\sonar-scanner-cli-3.3.0.1492-windows\sonar
INFO: Scanner configuration file: C:\Users\laymanl\Downloads\sonar-scanner-cli-3.3.0.1492-windows\sonar-scanner-3.3.0.1492-wi
INFO: Project root configuration file: C:\users\laymanl\Desktop\xampp-portable\htdocs\dvwa\sonar-project.properties
INFO: SonarQube Scanner 3.3.0.1492
INFO: Java 1.8.0_121 Oracle Corporation (64-bit)
INFO: Windows 10 10.0 amd64
INFO: User cache: C:\Users\laymanl\.sonar\cache
INFO: SonarQube server 7.4.0
INFO: Default locale: "en_US", source code encoding: "windows-1252" (analysis is platform dependent)
INFO: Publish mode
INFO: Load global settings
INFO: Load global settings (done) | time=86ms
INFO: Server id: BF41A1F2-AWkv_G74K__Q1H15nbva
INFO: User cache: C:\Users\laymanl\.sonar\cache
INFO: Load/download plugins
INFO: Load plugins index
INFO: Load plugins index (done) | time=55ms
INFO: Load/download plugins (done) | time=100ms
INFO: Loaded core extensions:
INFO: Process project properties
INFO: Load project repositories
INFO: Load project repositories (done) | time=666ms
INFO: Load quality profiles
INFO: Load quality profiles (done) | time=249ms
INFO: Load active rules
INFO: Load active rules (done) | time=2950ms
INFO: Load metrics repository
INFO: Load metrics repository (done) | time=172ms
WARN: SCM provider autodetection failed. Please use "sonar.scm.provider" to define SCM of your project, or disable the SCM Se
INFO: Project key: dvwa
INFO: Project base dir: C:\Users\laymanl\Desktop\xampp-portable\htdocs\dvwa
INFO: -------------  Scan DVWA
INFO: Base dir: C:\Users\laymanl\Desktop\xampp-portable\htdocs\dvwa
INFO: Working dir: C:\users\laymanl\Desktop\xampp-portable\htdocs\dvwa\.scannerwork
INFO: Source paths: .
INFO: Source encoding: windows-1252, default locale: en_US
INFO: Load server rules
INFO: Load server rules (done) | time=1502ms
INFO: Index files
INFO: 564 files indexed
INFO: Quality profile for js: Sonar way
INFO: Quality profile for php: Sonar way
INFO: Quality profile for xml: Sonar way
INFO: Sensor Dependency-Check [dependencycheck]
```

6. You should receive a "EXECUTION SUCCESS" message when the program terminates.
7. Once done, refresh **http://localhost:9000** (http://localhost:9000) and you should see scan results for the DVWA project. You may need to wait a minute for SonarQube to process the results of the scan.
8. Click on the 'DVWA' project link, then selecting 'Vulnerabilities'
9. You will be taken to the offending code when you select a vulnerability (or any issue type) in SonarQube. You can then click the ellipsis (...) to get more information.

Questions for DVWA

1. Select 'Vulnerabilities' in the Issue list
   - How many 'Vulnerabilities' did SonarQube find? How many were Critical?
   - Discuss all of the vulnerabilities with your colleagues. What is your assessment of their importance?
2. Select 'Security Hotspot' in the Issue list
   - Sample some of the Security Hotspots. Do they overlap with the Vulnerabilties?
   - Do any of the hotspots jump out at you?

3. Select the 'Security Reports' page, then 'OWASP Top 10 (https://www.owasp.org/index.php/Top_10-2017_Top_10)' from the dropdown menu
   - Note the ratings. Despite a lot of open issues, SonarQube is optimistic in it's ratings.
   - Click on one of the security issues, then click where it says 'Open' and change it to 'Detect'. Go back to the Security report. How has it changed?
   - So, what can you infer about *how* the security ratings are decided? What is the danger in presenting the reports this way?

Running on bad_stuff

1. Download bad_stuff_updated.zip (https://uncw.instructure.com/courses/16302/files/535328/download?wrap=1) and unzip it. This contains all the *unmitigated* Python vulnerabilities we showed during the Defensive Programming modules.
2. Using a Terminal / Command Prompt, navigate to the directory and run the `sonar-scanner.bat` as you did for DVWA. It will take far less time.
3. Select 'Projects' in SonarQube. You will now see a project titled 'vulnerable Python code'. Click on it.
4. What issues are there?

Running on bWAPP

1. bWAPP is packaged with the DVWA.
   - Start the apache and mysql servers in the xampp-portable/ directory.
   - Browse to http://localhost:10000 (http://localhost:10000).
   - Click the little link 'First install here' next to bwAPP.
   - Now go to the Login screen. Username and password are bee/bug
2. Using your OS's file browser, navigate to /xampp-portable/htdocs/bWAPP.
3. In this directory, create the necessary config file for SonarQube named `sonar-project.properties`. Edit the file in a text editor and paste in the following:

```
# must be unique in a given SonarQube instance
sonar.projectKey=bwapp
# this is the name and version displayed in the SonarQube UI. Was mandatory prior to SonarQube 6.1.
sonar.projectName=bWAPP
sonar.projectVersion=1.0

# Path is relative to the sonar-project.properties file. Replace "\" by "/" on Windows.
# This property is optional if sonar.modules is set.
sonar.sources=.

# Encoding of the source code. Default is default system encoding
#sonar.sourceEncoding=UTF-8
```

4. Run the `sonar-scanner.bat` as you did for DVWA. It will take a little while. Then look at the issues for bWAPP in SonarQube.
5. Open the bWAPP project in SonarQube. Click on the 'Vulnerabilities'. What are they? What can you infer about how SonarQube is detecting these vulnerabilities?
6. Select the 'Security Reports' and scroll through them. Which vulnerabilities that we have seen in class did it detect?