Threat Probe

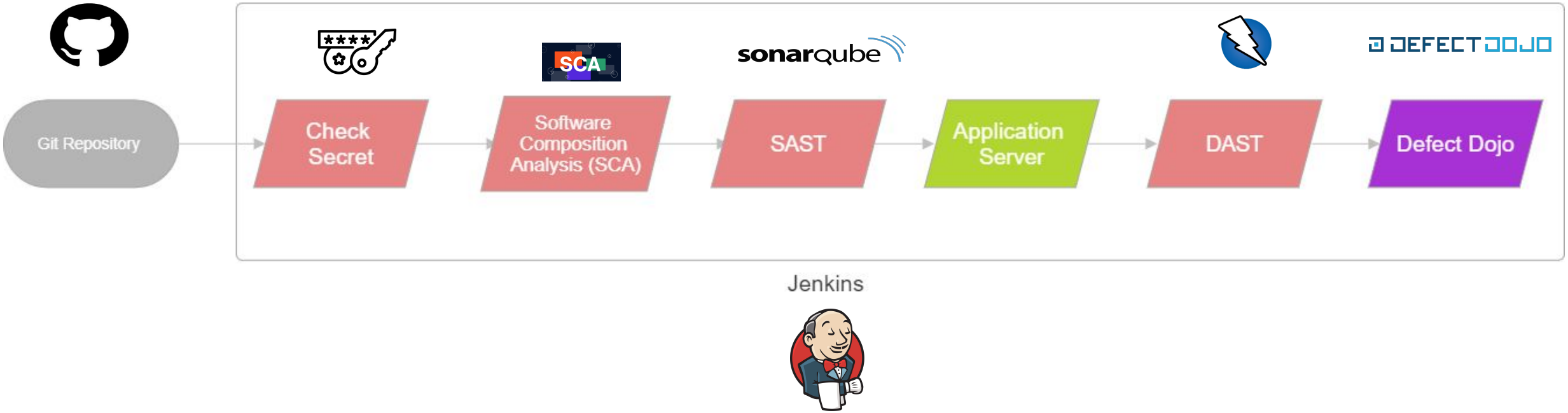
TO IDENTIFY VULNERABILITIES, ASSESS THE EFFECTIVENESS OF SECURITY CONTROLS, AND GENERATE REPORT ON HOW AN ATTACKER MIGHT EXPLOIT WEAKNESSES

Contents :

What is Threat Probe

Threat Probe is a DevSecOps pipeline that provide's complete security of the web application. This process automates the testing for security vulnerabilities under categories like Secret Scanning, Software Composition Analysis (SCA), SAST, DAST and issue reporting on – Defect Dojo.

Workflow


Git Repository
Check Secret
SCA
Software Composition Analysis (SCA)
sonarqube
SAST
Application Server
DAST
DEFECTDOJO
Defect Dojo
Jenkins

Workflow in brief

- 5 Instances created are : Jenkins, SAST, DAST, Application Server, Defect Dojo.
- Jenkins helps developers work faster and more efficiently by automating repetitive tasks involved in building, testing, and deploying software.
- In Jenkins we have added plugins like Git, Maven , Sonarqube, dependency checker, docker, Zap Proxy (Owasp Zap) and tools like trufflehog etc
- SAST helps developers identify and fix security vulnerabilities in their code before the software is even run, making it a crucial part of secure software development practices.

Workflow in brief

- DAST helps identify security issues by testing an application in its running state, focusing on vulnerabilities that appear during execution.
- Application Server helps hosting a website. In our project we have used Apache server to host the website
- Defect Dojo is designed to simplify the process of handling vulnerabilities discovered during security testing and integrate security findings into a comprehensive security program.

Overview of work flow

Stage Name	Tools used	Findings
Check Secret	TruffleHog	used to detect and manage sensitive information, such as passwords, API keys, tokens, or other secrets, that may accidentally be exposed in source code, configuration files, or logs.
Software Composition Analysis (SCA)	Dependency Checker	essential for managing the risks associated with using open-source and third-party components in software development.

Overview of work flow

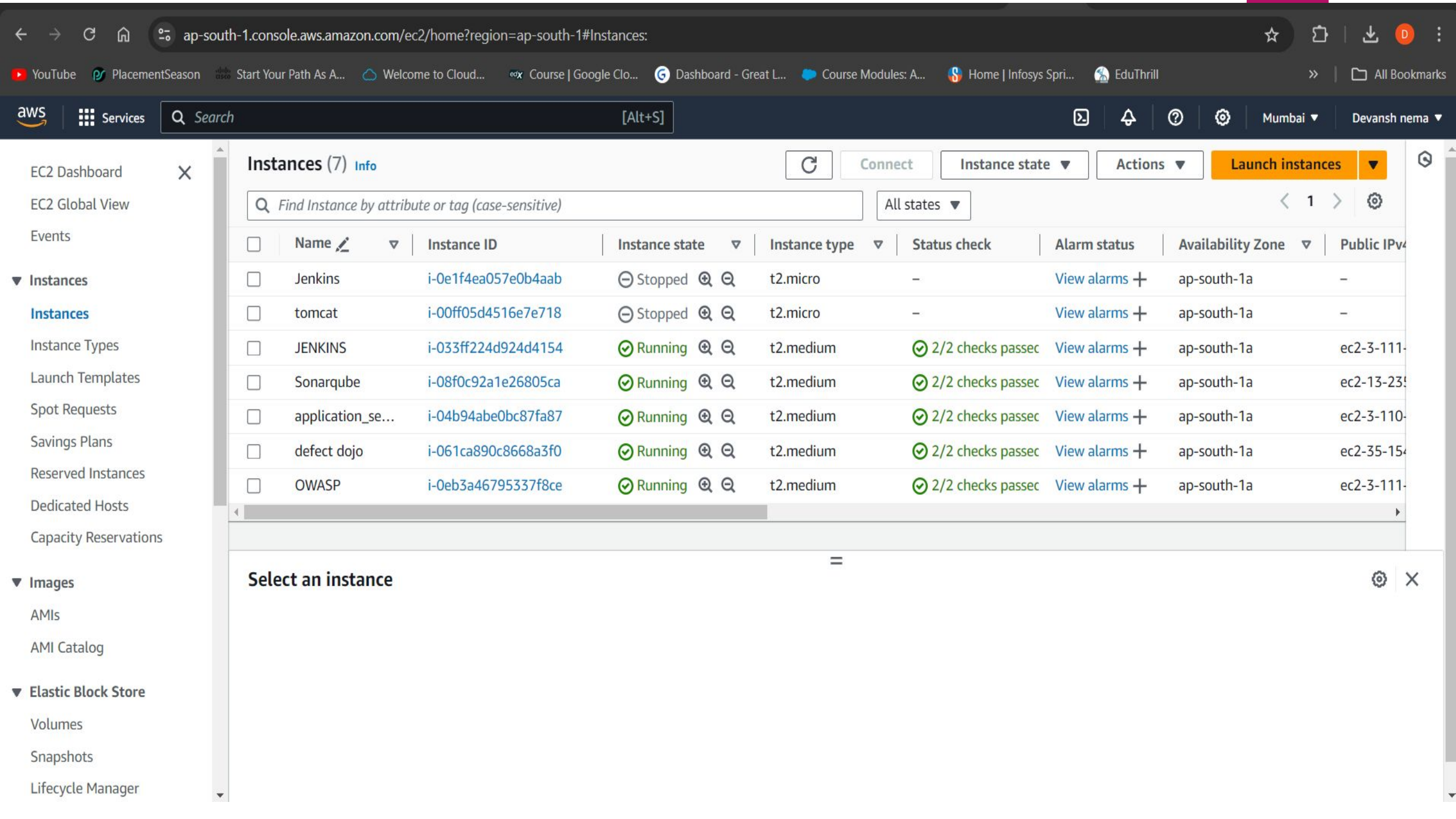
Stage Name	Tools Used	Findings
SAST (Static Application Security Testing)	SonarQube	helps ensure that the software is secure, compliant with industry standards, and free of common security flaws before it is even executed. Common vulnerabilities detected by SAST are Sql Injection, Cross-Site Scripting (XSS), Buffer Overflow, Command Injection etc.
DAST (Dynamic Application Security Testing)	OWASP ZAP	helps identify vulnerabilities that may not be visible in the source code, providing an essential layer of security testing for web applications, APIs, and other software systems of an application while it is running. Common vulnerabilities detected by DAST are Cross-Site Scripting (XSS), Sql detection etc.

Use Cases of our project :

- Continuous Security Testing
- Compliance and Regulatory Requirements
- Prevent Secret Leakage
- Automated Security Regression Testing

Sc

Screenshots & Outputs


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:
YouTube
PlacementSeason
Start Your Path As A...
Welcome to Cloud...
Course | Google Clo...
Dashboard - Great L...
Course Modules: A...
Home | Infosys Spri...
EduThrill
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai
Devansh nema
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (7) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4
Jenkins i-0e1f4ea057e0b4aab Stopped t2.micro – View alarms ap-south-1a –
tomcat i-00ff05d4516e7e718 Stopped t2.micro – View alarms ap-south-1a –
JENKINS i-033ff224d924d4154 Running t2.medium 2/2 checks passec View alarms ap-south-1a ec2-3-111-
Sonarqube i-08f0c92a1e26805ca Running t2.medium 2/2 checks passec View alarms ap-south-1a ec2-13-235
application_se... i-04b94abe0bc87fa87 Running t2.medium 2/2 checks passec View alarms ap-south-1a ec2-3-110-
defect dojo i-061ca890c8668a3f0 Running t2.medium 2/2 checks passec View alarms ap-south-1a ec2-35-154
OWASP i-0eb3a46795337f8ce Running t2.medium 2/2 checks passec View alarms ap-south-1a ec2-3-111-
Select an instance

Files

main

Go to file

CREATE_RELEASE.md
DevSecOps_case_study.jpg
Dockerfile
Dockerfile_desktop
FAQ.md
Intergration_of_Security_tools.pdf
Jenkinsfile
LICENSE.txt
Old_Configurationfile
PULL_REQUEST_TEMPLATE.md
README.MD
README.md
README_I18N.md
RELEASE_NOTES.md
TestClass.class
buildspec.yml
config.json
docker-compose-local.yml


```
27          stage ('Software composition analysis') {
28              steps {
29              dependencyCheck additionalArguments: '''
30              -o "./"
31              -s "./"
32              -f "ALL"
33              --prettyPrint''', odcInstallation: 'OWASP-DC'
34              dependencyCheckPublisher pattern: 'dependency-check-report.xml'
35
36              }
37
38          }
39
40        stage ('SAST - SonarQube') {
41           steps {
42             withSonarQubeEnv('sonarqube') {
43
44               sh 'mvn clean sonar:sonar -Dsonar.java.binaries=src'
45               //sh 'sudo python3 sonarqube.py'
46               //sh './sonarqube_report.sh'
47             }
48           }
49         }
50              // stage ('Generate build') {
51              //      steps {
52              //              //sh 'sudo update-alternatives --install /usr/bin/java java /usr/lib/jvm/java-11-openjdk-amd64/bin/java 2000'
53              //              //sh 'sudo update-alternatives --install /usr/bin/java java /usr/lib/jvm/java-17-openjdk-amd64/bin/java 1000'
54              //              sh 'mvn clean install -DskipTests'
55              //
56
57                              //  }
```

Status
Changes
Console Output
Edit Build Information
Delete build '#152'
Timings
Git Build Data
Dependency-Check
Open Blue Ocean
Pipeline Overview
Pipeline Console
Restart from Stage
Replay
Pipeline Steps
Workspaces
Previous Build

Dependency-Check Results

SEVERITY DISTRIBUTION

20 | 80 | 124 | 8

Search

File Name	Vulnerability	Severity	Weakness
ajv:6.6.2	OSSINDEX CVE-2020-15366	Medium	CWE-1321
ajv:6.6.2	NPM GHSA-v88g-cgmw-v5xw	Medium	CWE-1321
ansi-regex:3.0.0	OSSINDEX CVE-2021-3807	High	CWE-1333
ansi-regex:3.0.0	NPM GHSA-93q8-gq69-wqmw	High	CWE-697
axios:0.17.1	OSSINDEX CVE-2019-10742	High	CWE-400
axios:0.17.1	OSSINDEX CVE-2021-3749	High	CWE-1333
axios:0.17.1	NPM GHSA-42xw-2xvc-qx8m	High	CWE-755
axios:0.17.1	NPM GHSA-cph5-m8f7-6c5x	High	CWE-400
axios:0.17.1	OSSINDEX CVE-2023-45857	Medium	CWE-352
axios:0.17.1	NPM GHSA-wf5p-g6vw-rhxx	Medium	CWE-352

25°C Mostly clear
Search
ENG IN
12:58 AM 8/16/2024

Devsecop- | Dependen | Git [Jenkin | jenkins / d | Instances | EC2 Instan | EC2 Instan | webgoat_c | threatprob | Unzipping

Not secure 3.111.218.26:8080/blue/organizations/jenkins/devsecops-pipeline/detail/devsecops-pipeline/152/pipeline/21

Devsecop-pipeline < 152 >

Pipeline Changes Tests Artifacts Logout

Branch: –
Commit: –

2m 13s
4 hours ago

No changes
Started by user Goup2 Devsecops

Initialize - <1s

Restart Initialize

✓	Check out from version control	<1s
✓	Maven — Use a tool from a predefined Tool Installation	<1s
✓	Fetches the environment variables for a given tool in a list of 'FOO=bar' strings suitable for the withEnv step.	<1s
✓	Maven — Use a tool from a predefined Tool Installation	<1s
✓	Fetches the environment variables for a given tool in a list of 'FOO=bar' strings suitable for the withEnv step.	<1s
✓	echo "PATH = ${PATH}" echo "M2_HOME = ${M2_HOME}" — Shell Script	<1s

```
1  + echo PATH = /var/lib/jenkins/tools/hudson.tasks.Maven_MavenInstallation/Maven/bin:/var/lib/jenkins/tools/hudson.tasks.Maven_MavenInstallation/Maven/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
2  PATH = /var/lib/jenkins/tools/hudson.tasks.Maven_MavenInstallation/Maven/bin:/var/lib/jenkins/tools/hudson.tasks.Maven_MavenInstallation/Maven/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
3  + echo M2_HOME = /var/lib/jenkins/tools/hudson.tasks.Maven_MavenInstallation/Maven
4  M2_HOME = /var/lib/jenkins/tools/hudson.tasks.Maven_MavenInstallation/Maven
```

25°C Mostly clear

Search

ENG IN 12:58 AM 8/16/2024

Branch: –
Commit: –

2m 13s
4 hours ago

No changes
Started by user Goup2 Devsecops

Software composition analysis - 19s

Restart Software composition analysis

- Maven — Use a tool from a predefined Tool Installation <1s
- Fetches the environment variables for a given tool in a list of 'FOO=bar' strings suitable for the withEnv step. <1s
- Invoke Dependency-Check 19s

```
[INFO] Checking for updates
[INFO] Skipping the NVD API Update as it was completed within the last 240 minutes
[INFO] Skipping Known Exploited Vulnerabilities update check since last check was within 24 hours.
[INFO] Check for updates complete (907 ms)
[INFO]

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of
the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the
tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of
this tool, the analysis performed, or the resulting report.


   About ODC: https://jeremylong.github.io/DependencyCheck/general/internals.html
   False Positives: https://jeremylong.github.io/DependencyCheck/general/suppression.html
```

Devsecop-pi | Devsecop-pi | Instances | EC | EC2 Instance | EC2 Instance | webgoat_dev | threatprobe/ | Unzipping Fil | WebGoat Par

Not secure 13.235.132.178:9000/dashboard?id=org.owasp.webgoat%3Awebgoat-parent&codeScope=overall

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More

WebGoat Parent Pom / main

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

New Code 1 failed | Overall Code

Security

25 Open issues — E

20 H | 0 M | 5 L

Reliability

64 Open issues — E

13 H | 35 M | 16 L

Maintainability

665 Open issues — A

40 H | 274 M | 351 L

Accepted issues

0

Valid issues that were not fixed

Coverage

0.0%

On 3.4k lines to cover.

Duplications

1.6%

On 18k lines.

Security Hotspots

75 — E

Activity

25°C Mostly clear

Search

ENG IN

1:01 AM 8/16/2024

Devsecop-pi | Devsecop-pi | Instances | EC | EC2 Instance | EC2 Instance | webgoat_dev | threatprobe/ | Unzipping Fi | Rules - Sonar

Not secure 13.235.132.178:9000/coding_rules?selected=css%3AS4655

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration More

Filters

Language

Search for languages...

Java	667
C#	462
TypeScript	406
JavaScript	400
Python	291

5 shown Show More

Clean Code Attribute

Consistency	767
Intentionality	1.8k
Adaptability	271
Responsibility	163

Search for rules... Bulk Change Select rules Navigate to rule **3,398** rules

"!important" should not be used on "keyframes"
Intentionality
Reliability
CSS • Bug

"$this" should not be used in a static context
Intentionality
Reliability
PHP • Bug

"&&" and "||" should be used
Intentionality
Maintainability
PHP • Code Smell • suspicious

".equals()" should not be used to test the values of "Atomic" classes
Intentionality
Reliability
Java • Bug • multi-threading

"<!DOCTYPE>" declarations should appear before "<html>" tags
Consistency
Reliability
HTML • Bug • user-experience

"<>" should not be used to test inequality
Consistency
Maintainability
Python • Code Smell • obsolete

Embedded database should be used for evaluation purposes only

The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine

25°C Mostly clear

Search

ENG IN 1:02 AM 8/16/2024

Build #152

Rebuild | Overview | Configure | ...

Success 4 hr 28 min ago in 2 min 13 sec

- Checkout SCM
- Tool Install
- Initialize
- Check secrets
- Software composition analysis
- SAST - SonarQube
- Deploy to server

View as plain text

Maven
Use a tool from a predefined Tool Installation — 30 ms

Fetches the environment variables for a given tool in a list of 'FOO=bar' strings suitable for the withEnv step. — 35 ms

ssh -o StrictHostKeyChecking=no ubuntu@3.110.210.81 "nohup java -jar /WebGoat/webgoat-2023.8.jar &"
Shell Script — 34 sec

```
0  + ssh -o StrictHostKeyChecking=no ubuntu@3.110.210.81 nohup java -jar /WebGoat/webgoat-2023.8.jar &
1  2024-08-15T15:03:00.401Z  INFO 56964 --- [           main] org.owasp.webgoat.server.StartWebGoat    : Starting StartWebGoat v2023.8 using Java
   17.0.12 with PID 56964 (/WebGoat/webgoat-2023.8.jar started by ubuntu in /home/ubuntu)
2  2024-08-15T15:03:00.406Z  INFO 56964 --- [           main] org.owasp.webgoat.server.StartWebGoat    : No active profile set, falling back to 1
   default profile: "default"
3  2024-08-15T15:03:01.397Z  INFO 56964 --- [           main] org.owasp.webgoat.server.StartWebGoat    : Started StartWebGoat in 1.783 seconds
   (process running for 2.738)
4        __         __      _       _____                 _
5        \ \       / /     | |     / ____|               | |
6         \ \  /\  / /  ___  | |__  | |  __    ___     __ _  | |_
7          \ \/  \/ /  /   \ | '  \ | | |  | /   \   /  ' | |   |
```


25°C Mostly clear
Search
ENG IN
1:00 AM 8/16/2024

Branch: –
Commit: –

2m 13s
4 hours ago

No changes
Started by user Goup2 Devsecops

Deploy to server - 35s

Restart Deploy to server

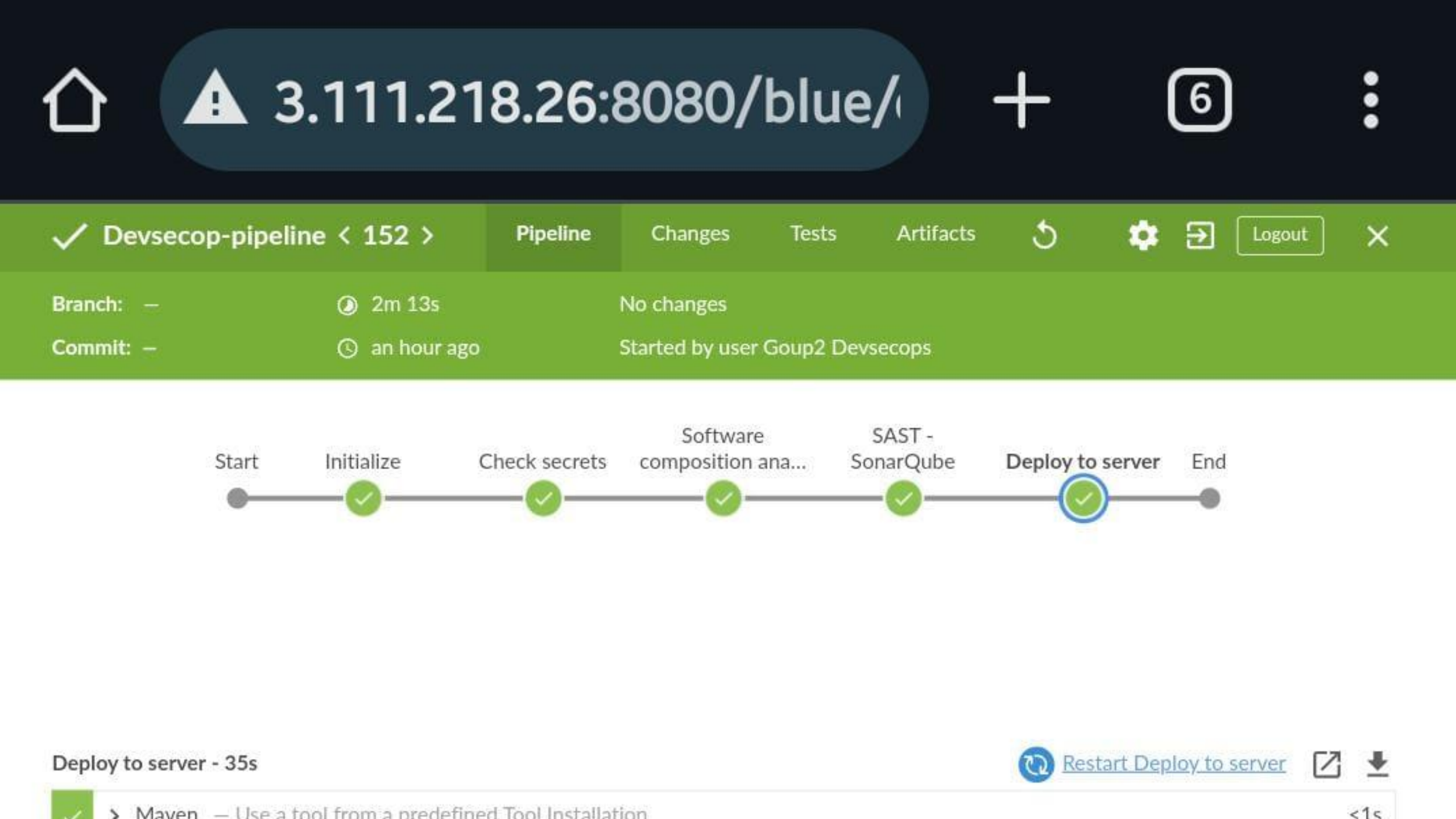
Maven — Use a tool from a predefined Tool Installation <1s

Fetches the environment variables for a given tool in a list of 'FOO=bar' strings suitable for the withEnv step. <1s

ssh -o StrictHostKeyChecking=no ubuntu@3.110.210.81 "nohup java -jar /WebGoat/webgoat-2023.8.jar &" — Shell Script 34s

```
+ ssh -o StrictHostKeyChecking=no ubuntu@3.110.210.81 nohup java -jar /WebGoat/webgoat-2023.8.jar &
2024-08-15T15:03:00.401Z  INFO 56964 --- [          main] org.owasp.webgoat.server.StartWebGoat    : Starting StartWebGoat v2023.8 using Java 17.0.12 with PID 56964 (/WebGoat/webgoat-2023.8.jar
started by ubuntu in /home/ubuntu)
2024-08-15T15:03:00.406Z  INFO 56964 --- [          main] org.owasp.webgoat.server.StartWebGoat    : No active profile set, falling back to 1 default profile: "default"
2024-08-15T15:03:01.397Z  INFO 56964 --- [          main] org.owasp.webgoat.server.StartWebGoat    : Started StartWebGoat in 1.783 seconds (process running for 2.738)
    __         __      _       ____                  _
    \ \       / /     | |     / ___|                | |
     \ \  /\  / /  ___ | |__  | |  _   ___    __ _  | |_
      \ \/  \/ /  / _ \| '_ \ | | |_| / _ \  / _` | | __|
       \  /\  /  |  __/| |_) || |__| | (_) || (_| | | |_
        \/  \/    \___||_.__/  \____|  \___/  \__,_|  \__|

2024-08-15T15:03:01.489Z  INFO 56964 --- [          main] org.owasp.webgoat.server.StartWebGoat    : No active profile set, falling back to 1 default profile: "default"
2024-08-15T15:03:03.088Z  INFO 56964 --- [          main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
```


3.111.218.26:8080/blue/
6
Devsecop-pipeline < 152 >
Pipeline
Changes
Tests
Artifacts
Logout
Branch: –
2m 13s
No changes
Commit: –
an hour ago
Started by user Goup2 Devsecops
Start
Initialize
Check secrets
Software composition ana...
SAST - SonarQube
Deploy to server
End
Deploy to server - 35s
Restart Deploy to server
Maven — Use a tool from a predefined Tool Installation
<1s