

Configuration Manual

MSc Research Project MSc in Cybersecurity

Preeti Bhardwaj Student ID: x21139351

School of Computing National College of Ireland

Supervisor: Arghir Nicolae Moldovan

National College of Ireland

MSc Project Submission Sheet



School of Computing

Student Name:	Preeti Bhardwaj		
Student ID:	X21139351		
Programme:	MSc Cybersecurity	Year:	2022-2023
Module:	MSc Research Project		
Lecturer:	Arghir Nicolae Moldovan		
Submission Due Date:	15-12-2022		
Project Title:	Detecting container vulnerabilities levera	aging th	e CICD pipeline

Word Count:

Page Count:

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Preeti Bhardwaj

Date: 15-12-2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	
Attach a Moodle submission receipt of the online project	
submission, to each project (including multiple copies).	
You must ensure that you retain a HARD COPY of the project, both	
for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Introduction:

In the research project we explored how docker vulnerabilities can be detected in an automated pipeline to strengthen the security of vulnerable docker images.. The research methodology and design followed consisted of an implementation that was setup to achieve the research outputs. We set up a CICD pipeline in Gitlab and incorporated a vulnerability scanning tool to scan docker images. The configuration manual is a step-by-step guide to install, setup and implement the research.

Configurations:

Gitlab Enterprise edition	15.7.0
Trivy tool	Version : v0.35.0
Clair tool	Version : v8.0
Docker Image #1	cern/cc7-base
Docker Image #2	centos/httpd-24-centos7

Implementation:

For implementation, the initial goal is to set up a CI CD pipeline:

Step 1. Setup a new account on Gitlab by Registering a new account.

	₩	
c	GitLab.com	
Username or email		_
Password		
Remember me	Forgot your password	?
	Sign in	
By signing in you accept the Privacy Policy and Cookie Po	e Terms of Use and acknowledge the olicy.	
Don't have a	n account yet? Register now	
	Sign in with	
G Google	GitHub 🔰 Twitter	
🖬 Bitbu	icket Salesforce	
	Remember me	

Step 2. Once registered, users need to set up the details and after that there will be an option to Create or import a project. We will create a new project for the research. Enter the project and group.

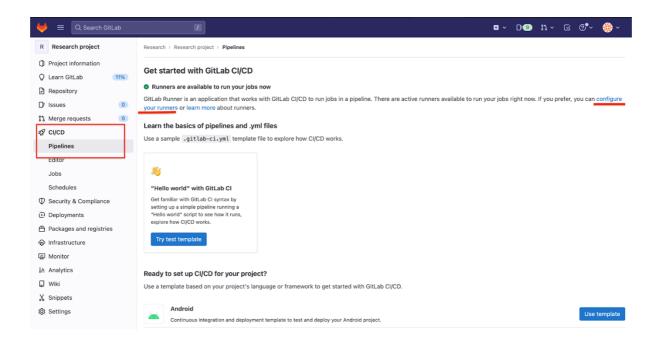
Create or import your first project

Create	Import
Group name	
Research	
Project name	
Research project	
Your project w	vill be created at:
https://gitlab.com/rese	earch180/research-project
You can always ch	nange your URL later
✓ Include a Getting Started R	README
Recommended if you're ne	w to GitLab

• Click on Create Project

Step 3. After saving the project, the user will be directed to the dashboard. We will configure the Gitlab Runner [1]

- Click on CICD.
- Under CICD, Click on Pipeline
- Click on Configure your runner



Step 4. Enable the shared runner. Runner can be used locally as well following the official documentation by gitlab [2]. However, for our research project it is convenient to use the shared runner without any hassle.

R Research project	How do runners pick up jobs?	
Project information	Runners are either:	
C Learn GitLab C Learn GitLab C Repository C Issues 0		g a runner, you make sure shared runners only handle the jobs they
Merge requests O CI/CD	are equipped to run. Learn more. Specific runners	Shared runners
 Security & Compliance Deployments 	These runners are specific to this project.	These runners are available to all groups and projects.
Packages and registries Infrastructure Monitor Analytics Wiki Snippets	Use GitLab Runner in AWS Use an AWS CloudFormation Template (CFT) to install and configure GitLab Runner in AWS. 1. Copy this registration token. GR13489414q6gayxWBJHKEEzaBac C 2. Choose the preferred Runner and populate the AWS CFT. Learn more.	Each CI/CD job runs on a separate, isolated virtual machine. Enable shared runners for this project Available shared runners: 50 #17142247 (ZQ74L_ri)
 Settings General Integrations 	Deploy GitLab Runner in AWS	blue-2.saas-linux-medium-amd64.runners- manager.gitlab.com/default saas-linux-medium-amd64 #11574045 (8cwZ3F43)
Webhooks Repository Merge requests	Set up a specific runner for a project 1. Install GitLab Runner and ensure it's running. 2. Register the runner with this URL: https://gitLab.com/	4-blue.shared-gitlab-org.runners-manager.gitlab.com gitlab-org #17142265 (xeNoC751) proces dage liaw lang and 64 suppose
« Collapse sidebar	And this registration token:	green-4.saas-linux-large-amd64.runners-

Step 5. We will now create the files that will define CICD jobs. We will first create the <u>.gitlab-ci.yml</u> at the root repository.

- Click on Repository on dashboard
- Click on Files

• Click on + symbol (beside the project name)

븢 🛛 🚍 🔍 Search Git	tLab			□ ~ D•• \$\$ ~ @ \$\$ ~ @
R Research project		Research > Research project > Repos	sitory	
 Project information Learn GitLab Repository 	11%	Initial commit Preeti Bhardwaj authored	1 32 minutes ago	c273f995 🛱
Files		main ~ research-project /	+ ~	History Find file Web IDE Clone Clone
Commits Branches		Name	This directory New file	Last update
Tags		M# README.md	Upload file	32 minutes ago
Contributors Graph		E README.md	New directory	
Compare			This repository	
Issues	0	Research project	New branch New tag	
Ղ Merge requests ₽ CI/CD	0	Getting started	New lag	
Security & Compliance		To make it easy for you to get	t started with GitLab, here's a list of r	ecommended next steps.
Deployments		Already a pro? Just edit this F	README.md and make it your own. W	ant to make it easy? Use the template at the bottom!
Packages and registrie	s	Add your files		

Step6. We will create the pipeline file with stages as:

- build
- test
- clair
- trivy

#Code of the pipeline and tools(entire file code) has been shared in the artefacts and code zip file.

- Use the .gitlab-ci.yml pipeline code. (Shared in artefacts and code zip)
- Save file extensions as: .gitlab-ci.yml
- Click on Commit changes

Project information	E alla d	4 1-	
Q Learn GitLab 22%	» Edit f	ne	
Repository			End call
Files	Write	Preview changes	_
Commits	₽ mai	inigitlab-ci.yml v Apply a template v	= No wrap
Branches	1	stages:	
Tags	2	- build - test	
Contributors	4	- clair	
Graph	5	- trivy	
Compare	7	containerbuild:	
D Issues	0 9 10	stage: build	
3 Merge requests	0 11	services:	
2 CI/CD	12		
	14		
D Security & Compliance	15		
Deployments	17	- docker buildcache-from \$CI_REGISTRY_IMAGE:latesttag \$CI_REGISTRY_IMAGE:\$CI_COMMIT_SHAtag \$CI_REGISTRY_IMAGE:latest .	
Packages and registries	18		
Anfrastructure	20		

븢 😑 🔍 Search GitLab	↗
R Research project	[^"]+)",*/\1/') 85 - echo \$TRIVY_VERSION
Project information	86 - wgetno-verbose https://github.com/aquasecurity/trivy/releases/download/v\${TRIVY_VERSION}/trivy_\${TRIVY_VERSION}_Linux-64bit.tar.gz -0 - tar -zxvf -
Q Learn GitLab	87 allow_failure: true 88 script:
Repository	89 # Build image 90 - docker build -t \$IMAGE .
Files	91 # Image report 92/trivy imageexit-code 0format templatetemplate "@contrib/gitlab-codeguality.tpl" -o gl-codeclimate-image.json \$IMAGE
Commits	93 # Filesystem report /trivy filesystem —security-checks config.vuln —exit-code 0 —format template "@contrib/gitlab-codeguality.tpl" -o
Branches	gl-codeclimate-fs.json .
Tags	95 # Combine report 96 - apk update && apk add jq
Contributors	97 - jq -s 'add' gl-codeclimate-image.json gl-codeclimate-fs.json > gl-codeclimate.json 98 cache:
Graph	99 paths: 100trivcache/
Compare	101 # Enables https://docs.gitlab.com/ee/user/application_security/container_scanning/ (Container Scanning report is available on Gitlab EE Ultimate or Gitlab.com Gold)
D Issues	102 artifacts: paths:
 Merge requests 	104 gl-codeclimate.json
2 CI/CD	105 reports: 106 codequality: gl-codeclimate.json
① Security & Compliance	107
Deployments	Commit message Add new file
Packages and registries	
lnfrastructure	Target Branch main
🛄 Monitor	
년 Analytics	Commit changes Cancel
📮 Wiki	
« Collapse sidebar	

Step.7 We will now create the docker file, which will contain the docker image.

- Click on Repository on dashboard
- Click on Files
- Click on + symbol (beside the project name)
- Use Docker Image file code.
- Name the file as: Dockerfile
- Click on Commit changes.

#Code of the Docker images : Image #1 : cern/cc7-base, Image #2 :centos/httpd-24-centos7 has been shared in the artefacts and code zip file.

R Research project	Research > Research project > Repository
Project information	
Q Learn GitLab	New file
Repository	
Files	Image: P main / Dockerfile Apply a template Image: Top water
Commits	1 FROM cern/cc7-base
Branches	3 MAINTAINER djuarezg@cern.ch
Tags	5 COPY helloworld.sh /
Contributors	6 RUN chmod 700 /helloworld.sh
Graph	8 ENTRYPOINT /helloworld.sh
Compare	
D' Issues	
🕄 Merge requests	
Ø CI/CD	
① Security & Compliance	
ව Deployments	
Packages and registries	
폪 Monitor	
止 Analytics	
📮 Wiki	
« Collapse sidebar	Commit message Add new file

Step8. We will also create a small Hello word code file that will sit on the top of the Docker image.

- Click on Repository on dashboard
- Click on Files
- Click on + symbol (beside the project name)
- Use helloworld.sh file
- Click on Commit changes

#Code of the helloworld.sh file has been shared in the artefacts and code zip file.

😝 🔳 🔍 Search GitLab	Z Z	• •	₽9	11 ~	G (?∮~	🏶 ~
R Research project	Research > Research project > Repository						
Project information							
Q Learn GitLab 22%	New file						
Repository							
Files	Image: Provide a start of the start of t					⇒= No w	rap
Commits	1 #1/bin/bash 2 echo HelloWorld script within Docker image						
Branches	3 exit 0 4						_
Tags							
Contributors							
Graph							
Compare							
D' Issues 0							
11 Merge requests 0							
🕼 CI/CD							
① Security & Compliance							
Deployments							
Packages and registries							
🛄 Monitor							
撞 Analytics							
📮 Wiki	Commit message Add new file						
« Collapse sidebar	Commit message Add new file						

Important note: One thing to note here is if the user has not provided Credit card details to validate the user account. The pipeline will give an **error**:

븢 📃 🔍 Search GitLab					
R Research project	A Pipeline failing? To keep GitLab spam and abuse free we ask that you verify your identity.				
Project information	Until then, shared runners will be unavailable. Validate your account or use your own runners-				
Q Learn GitLab (22%)	Research > Research project > Pipelines > #722198037				
Repository					
D' Issues 0	📀 failed Pipeline #722198037 triggered just now by 🔅 Preeti Bhardwaj Delete				
3 Merge requests	① User validation required ×				
Ø CI/CD	To use free CI/CD minutes on shared runners, you'll need to validate your account with a credit card. If you prefer not to provide one, you can run pipelines by bringing your own runners and disabling shared runners for your project. This is required to discourage and reduce abuse on GitLab infrastructure. GitLab will not				
Pipelines	charge your card, it will only be used for validation. Learn more.				
Editor	Validate account				
Jobs					
Schedules	Add new file				
D Security & Compliance					
Deployments	() 0 jobs for main				
Packages and registries	P latest error				
Infrastructure					
Monitor	∞ 2a158fca (⁶)				
i Analytics	Ph. No. exclusion ensures found				
₽ Wiki	\$\% No related merge requests found.				
X Snippets	Pipeline Needs Jobs 0 Tests 0				
Settings					

Once the card details are saved, the account will be validated and CICD pipeline will be ready to run jobs.

Running the CICD Pipeline: Once the implementation is done, we will now run our pipeline to scan the docker images.

Step1.

- Click on CICD on the dashboard
- Click on Run pipeline

All the status of the running pipeline will show on the screen, hover above the stages and click to check the running jobs. The status of the running job will show on Pipeline page as well as the status of the running job can be checked from the stages and clicking on each running job under the stage.

• Note: While scanning with Clair tool pipeline gets terminated whenever the errors are encountered and detected in the docker image.

Project information	All 10 Finished	Branches Tags		Clear runner caches Cl lint Run pipeline
Q Learn GitLab 22% ☐ Repository	Filter pipelines		Q Show Lipeline 2 and	
D Issues				
11 Merge requests 0	Status	Pipeline	Triggerer Stages	
명 CI/CD Pipelines	() passed ③ 00:02:03 ⊟ 6 minutes ago	Update_gitlab-ci.yml file <u>#7222550102</u>	build: passed	
Editor Jobs Schedules	() passed © 00:02:46	Update Dockerfile <u>#721296529</u> ♀ main -0-9e1aaf93 ११	ا⊙ \$	
 ♥ Security & Compliance ● Deployments 	20 hours ago(*) failed	Update .gitlab-ci.yml file	* **	
Packages and registries	© 00:00:34 ⊟ 1 day ago	<u>#720242862</u> 🐉 main 🗠 010f7022 ô		
linfrastructure Monitor 地 Analytics	(♥ failed) ③ 00:00:31 ⊟ 1 day ago	Update Dockerfile <u>#720241646</u>	(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)<l< td=""><td></td></l<>	
Wiki Collapse sidebar	() passed ③ 00:02:21 茴 2 days ago	Update .gitlab-ci.yml file <u>#719510635</u> \$ ⁹ main -O- 138b8878 🛞	١.	

References:

[1] *Gitlab Runner* (no date) *GitLab*. Available at: https://docs.gitlab.com/runner/ (Accessed: December 15, 2022).

[2] *Install gitlab runner* (no date) *GitLab*. Available at: https://docs.gitlab.com/runner/install/ (Accessed: December 15, 2022).