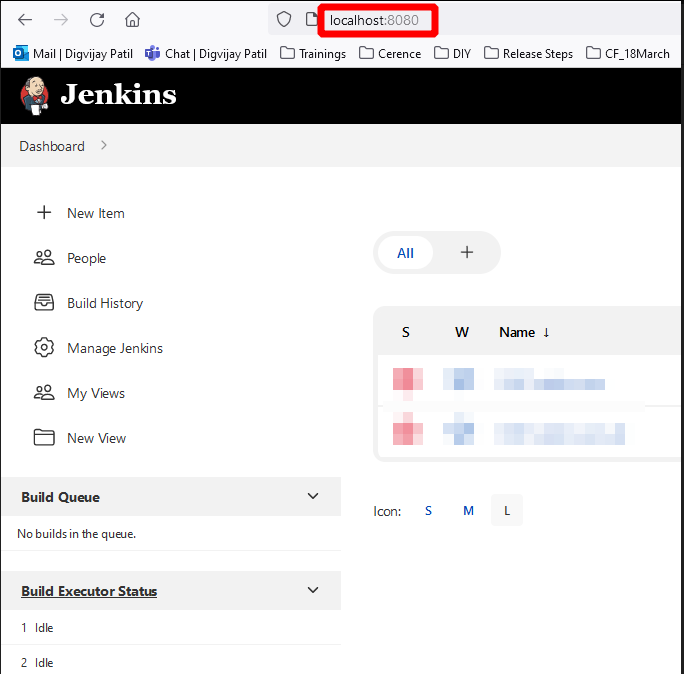
Jenkins Setup

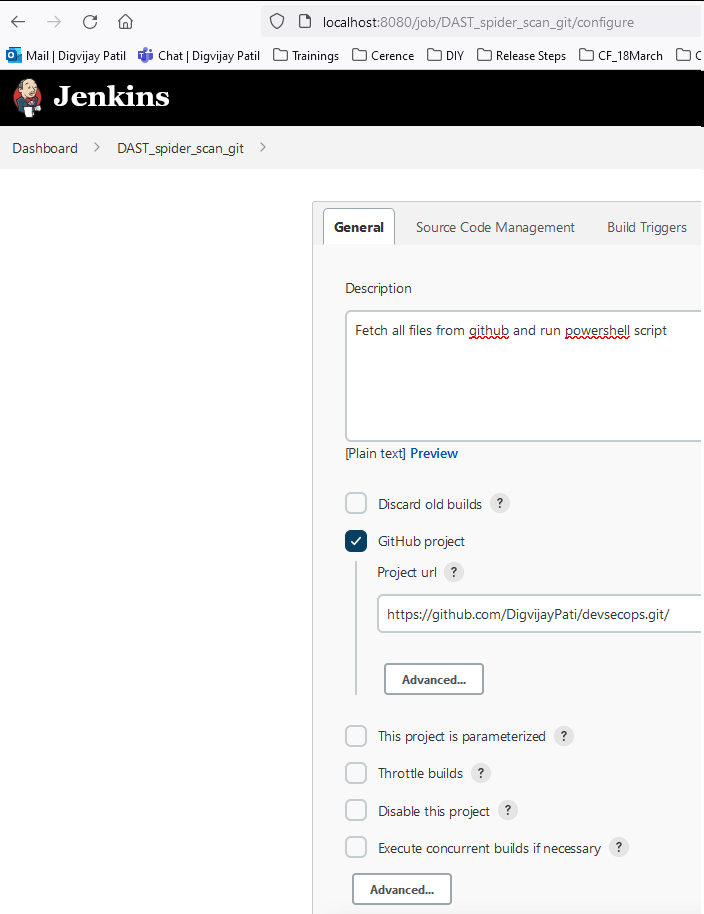
# Install Jenkins

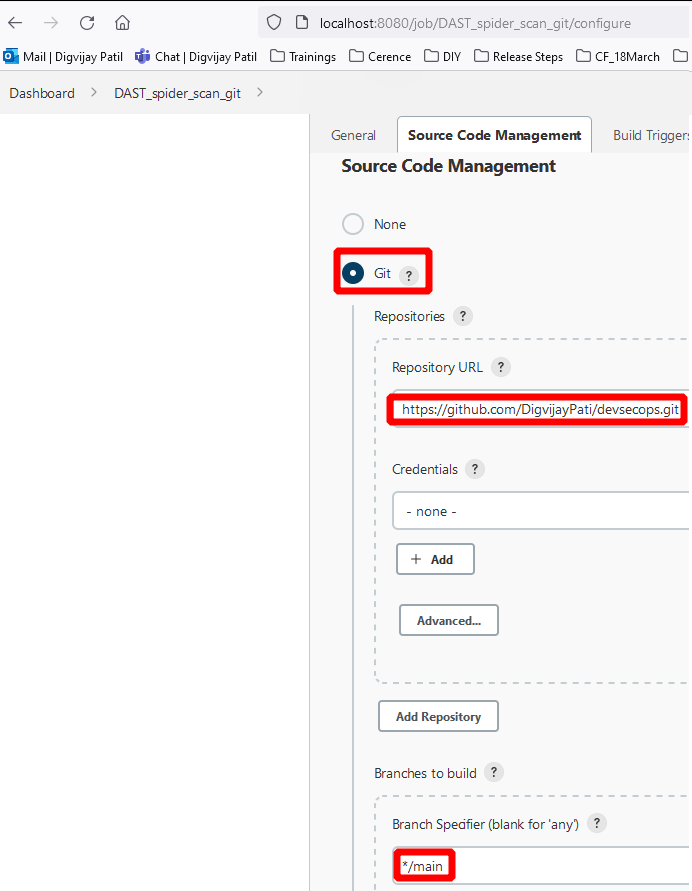


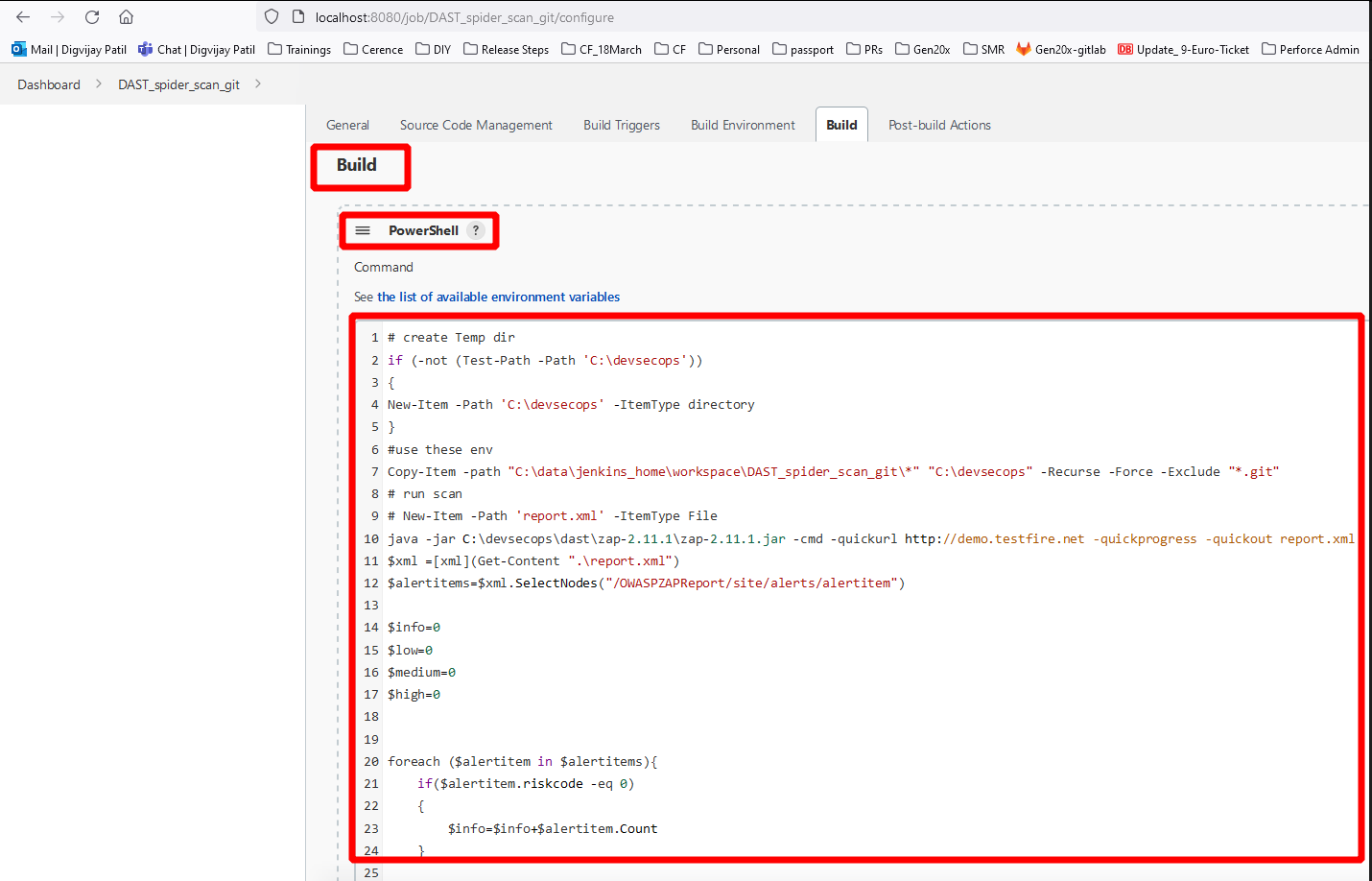
# Install plugins

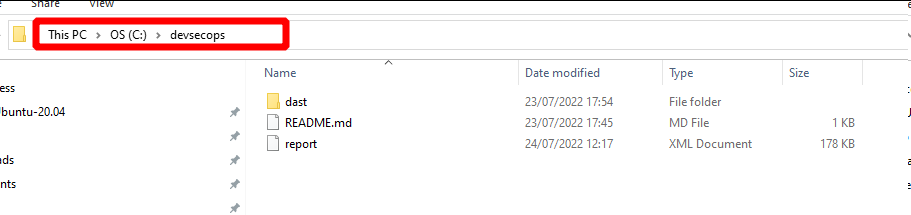
1. Git
2. Powershell

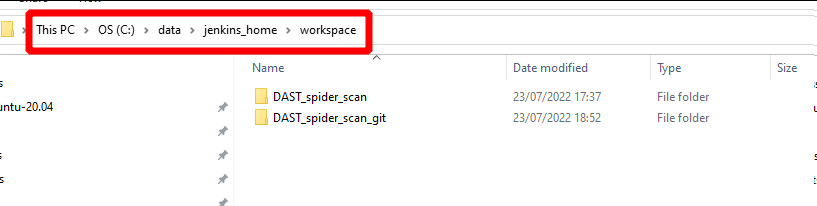
# Create a Job











Powershell script

***# create Temp dir***

***if (-not (Test-Path -Path 'C:\devsecops'))***

***{***

***New-Item -Path 'C:\devsecops' -ItemType directory***

***}***

***#use these env***

***Copy-Item -path "C:\data\jenkins\_home\workspace\DAST\_spider\_scan\_git\\*" "C:\devsecops" -Recurse -Force -Exclude "\*.git"***

***# run scan***

***# New-Item -Path 'report.xml' -ItemType File***

***java -jar C:\devsecops\dast\zap-2.11.1\zap-2.11.1.jar -cmd -quickurl http://demo.testfire.net -quickprogress -quickout report.xml***

***$xml =[xml](Get-Content ".\report.xml")***

***$alertitems=$xml.SelectNodes("/OWASPZAPReport/site/alerts/alertitem")***

***$info=0***

***$low=0***

***$medium=0***

***$high=0***

***foreach ($alertitem in $alertitems){***

***if($alertitem.riskcode -eq 0)***

***{***

***$info=$info+$alertitem.Count***

***}***

***if($alertitem.riskcode -eq 1)***

***{***

***$low=$low+$alertitem.Count***

***}***

***if($alertitem.riskcode -eq 2)***

***{***

***$medium=$medium+$alertitem.Count***

***}***

***if($alertitem.riskcode -eq 3)***

***{***

***$high=$high+$alertitem.Count***

***}***

***}***

***Write-Host "High Vulnerabilities:"$high***

***Write-Host "Medium Vulnerabilities:"$medium***

***Write-Host "Low Vulnerabilities:"$low***

***Write-Host "Info Vulnerabilities:"$info***

***if($high -gt 0 -Or $medium -gt 0 )***

***{***

***Write-Host "There are vulnerbailities in your application, Please fix them.."***

***exit 1***

***}***

***else***

***{***

***Write-Host "Your application received signoff for DAST.."***

***}***