Lab 5 - DevSecOps

Name: Mohamad Nour Shahin, Yehia Sobeh, Ali Hamdan

Group number: B22-CBS-01

In today's rapidly evolving software development landscape, integrating security into every phase of the development lifecycle is important. DevSecOps, a combination of development, security, and operations, emphasizes the importance of embedding security practices into the DevOps workflow to ensure secure, high-quality software delivery. This lab introduces fundamental concepts and hands-on exercises to help you understand how security can seamlessly integrate into continuous integration/continuous delivery (CI/CD) pipelines. By the end of this lab, you will gain practical experience in identifying vulnerabilities, implementing security checks, and automating security tasks to build resilient systems.

PyGoat is the vulnerable Python application we are using in this practice.

Instructions

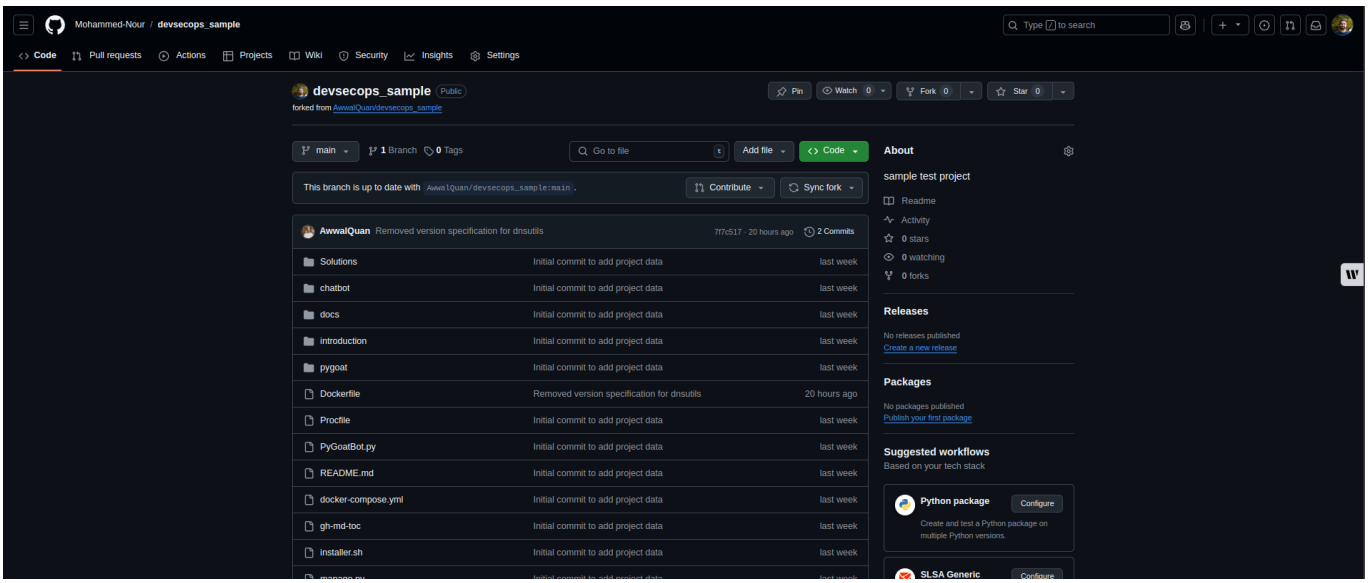
- You may work in teams of up to 4 students.
- Ensure your repository is public and share its URL in the report.
- Also include links to pipeline runs that are relevant to each task you complete.

Task 1: Fork the repository

Create a fork of the https://github.com/AwwalQuan/devsecops_sample GitHub repository.

Solution:

Link to Github repo



Task 2: Create the base pipeline

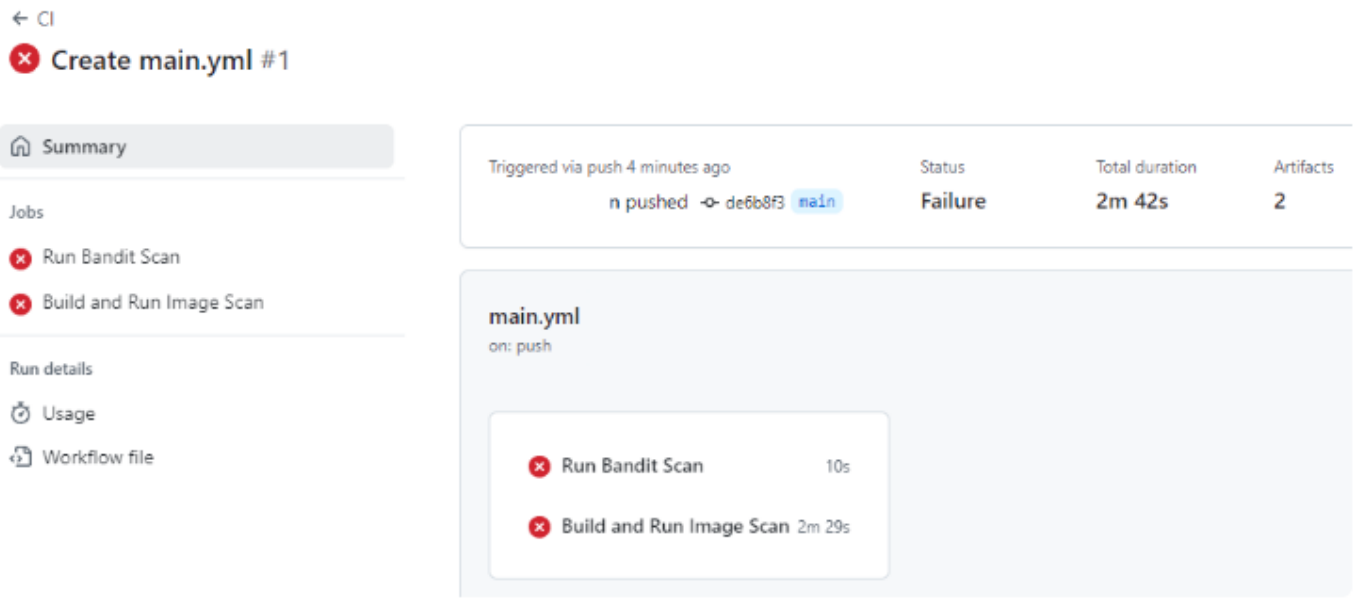
Create the pipeline (workflow) using GitHub actions. Work with the following pipeline configuration:

- It is preconfigured with the SAST scan using Bandit, and Docker image scanning using Docker Scout.
- Each job runs on the default GitHub `ubuntu-latest` runner.
- Note that the workflow authenticates to Dockerhub using secrets. You need to add your DockerHub credentials to the repository using GitHub secrets. The variables you need to configure are `DOCKERHUB_USERNAME` and `DOCKERHUB_PASSWORD`.

```
name: CI

# triggers pipeline when push is made to any branch (typical CI pipeline
rule)
on: [push]

jobs:
 sast_scan:
   name: Run Bandit Scan
   runs-on: ubuntu-latest

   steps:
   - name: Checkout code
     uses: actions/checkout@v2

   - name: Set up Python
     uses: actions/setup-python@v2
     with:
       python-version: 3.8

   - name: Install Bandit
     run: pip install bandit

   - name: Run Bandit Scan
     #safe report in json format
     run: bandit -ll -ii -r . -f json -o bandit-report.json

   - name: Upload Artifact
     uses: actions/upload-artifact@v3
     #execute this step no matter of previous status
     if: always()
     with:
        #how artifacts will be named when exported
        name: bandit-findings.json
        path: bandit-report.json

 image_scan:
 #each new job runs in a new isolated environment
   name: Build and Run Image Scan
   runs-on: ubuntu-latest
```

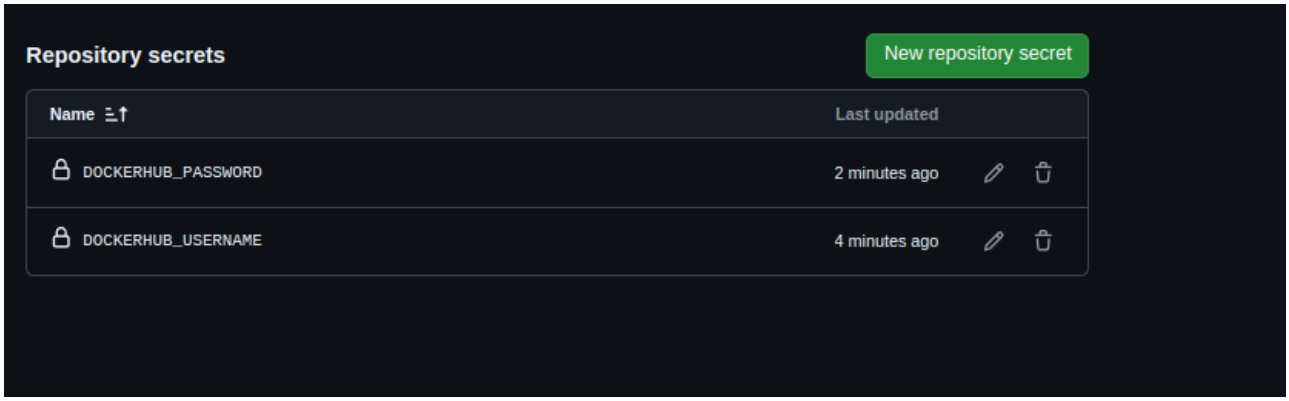
```
    steps:
    - name: Checkout code
      uses: actions/checkout@v2

    - name: Set up Docker
      uses: docker-practice/actions-setup-docker@v1
      with:
       docker_version: '20.10.7'

    - name: Build Docker Image
      run: docker build -f Dockerfile -t mytestapp:latest .

    - name: Docker Scout Scan
      uses: docker/scout-action@v1.15.1
      with:
        dockerhub-user: ${{ secrets.DOCKERHUB_USERNAME }}
        dockerhub-password: ${{ secrets.DOCKERHUB_PASSWORD }}
        command: quickview,cves
        only-severities: critical,high
        sarif-file: scout-report.sarif
        #exit code by default is true which means 0, add true to produce non
success exit code when vulns are found
        exit-code: true

    - name: Upload Artifact
      uses: actions/upload-artifact@v3
      if: always()
      with:
        name: docker-scout-findings
        path: scout-report.sarif
```

- Show that the workflow executed after you pushed the changes.
- The "Failed" ❌ status of the workflow is expected. In this case, it indicates that some vulnerabilities were discovered in the application.

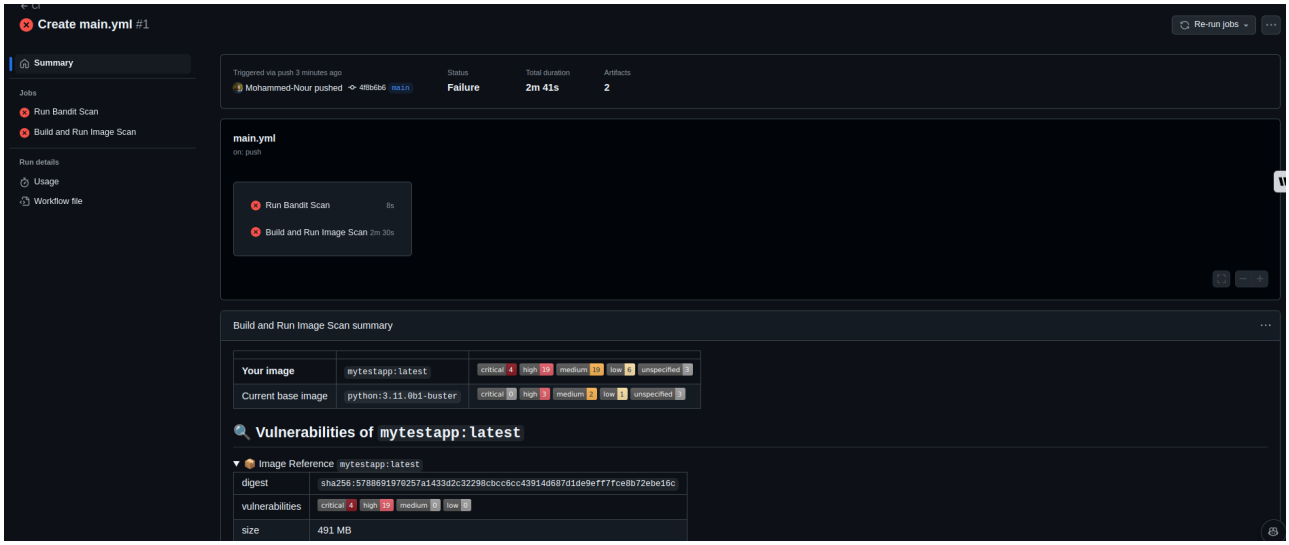


Solution:

- Adding the secrets:



- After create an action and its running:



Task 3: DAST

Create a new job named dast_scan, and perform the following actions under it.

- Deploy PyGoat.
- You can deploy it on an `ubuntu-latest` runner.
- You might encounter some challenges when building and deploying the application. You can instead deploy the application by pulling and running from the official PyGoat repository with the following commands in your pipeline.

```
docker pull pygoat/pygoat:latest
```

```
docker run --rm -d -p 8000:8000 pygoat/pygoat:latest
```

Bonus points if you can build and deploy PyGoat from your own repository.

- Configure your workflow to perform dynamic application security test under the dast_scan job.

For example, you may consider any of the following tools in your pipeline: ZAP, Nikto, Arachni, etc.

- Show and summarize the report generated by your DAST tool.

Solution:

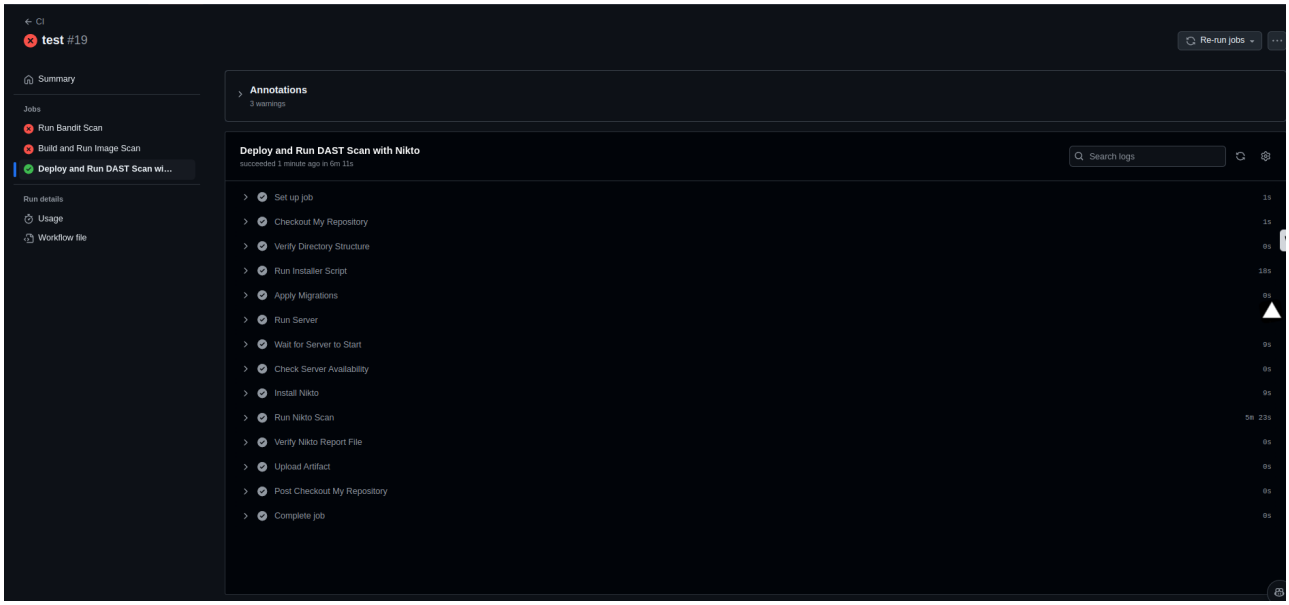
I added the followinf code to `main.ymal`:

```
name: CI

# triggers pipeline when push is made to any branch (typical CI pipeline
rule)
on: [push]

jobs:
  sast_scan:
    name: Run Bandit Scan
    runs-on: ubuntu-latest

    steps:
      - name: Checkout code
        uses: actions/checkout@v2

      - name: Set up Python
        uses: actions/setup-python@v2
        with:
          python-version: 3.8

      - name: Install Bandit
        run: pip install bandit

      - name: Run Bandit Scan
        #safe report in json format
        run: bandit -ll -ii -r . -f json -o bandit-report.json

      - name: Upload Artifact
        uses: actions/upload-artifact@v3
        #execute this step no matter of previous status
        if: always()
        with:
          #how artifacts will be named when exported
          name: bandit-findings.json
          path: bandit-report.json

  image_scan:
    #each new job runs in a new isolated environment
    name: Build and Run Image Scan
    runs-on: ubuntu-latest

    steps:
      - name: Checkout code
        uses: actions/checkout@v2

      - name: Set up Docker
```

```
        uses: docker-practice/actions-setup-docker@v1
        with:
          docker_version: "20.10.7"

      - name: Build Docker Image
        run: docker build -f Dockerfile -t mytestapp:latest .

      - name: Docker Scout Scan
        uses: docker/scout-action@v1.15.1
        with:
          dockerhub-user: ${{ secrets.DOCKERHUB_USERNAME }}
          dockerhub-password: ${{ secrets.DOCKERHUB_PASSWORD }}
          command: quickview,cves
          only-severities: critical,high
          sarif-file: scout-report.sarif
          #exit code by default is true which means 0, add true to produce
non success exit code when vulns are found
          exit-code: true

      - name: Upload Artifact
        uses: actions/upload-artifact@v3
        if: always()
        with:
          name: docker-scout-findings
          path: scout-report.sarif

  dast_scan:
    name: Deploy and Run DAST Scan with Nikto
    runs-on: ubuntu-latest

    steps:
      - name: Checkout My Repository
        uses: actions/checkout@v2

      - name: Verify Directory Structure
        run: ls -la

      - name: Run Installer Script
        run: bash installer.sh

      - name: Apply Migrations
        run: python3 manage.py migrate

      - name: Run Server
        run: nohup python3 manage.py runserver 0.0.0.0:8000 &

      - name: Wait for Server to Start
        run: sleep 10

      - name: Check Server Availability
        run: curl -I http://127.0.0.1:8000

      - name: Install Nikto
        run: sudo apt-get update && sudo apt-get install -y nikto
```

```
    - name: Run Nikto Scan
      run: |
        nikto -h http://127.0.0.1:8000 -o nikto-report.html -Format html

    - name: Verify Nikto Report File
      run: ls -la

    - name: Upload Artifact
      uses: actions/upload-artifact@v3
      with:
        name: nikto-report
        path: nikto-report.html
```

- The code is fully explained.
- The results of running the pipeline:



```
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        8000
+ Start Time:         2024-11-20 19:51:51 (GMT0)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.10.12
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Root page / redirects to: /login/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-17113: /SilverStream: SilverStream allows directory listing
+ Server banner has changed from 'WSGIServer/0.2 CPython/3.10.12' to 'WSGIServer/0.2 Python/3.10.12' which may suggest a WAF, load balancer or proxy is in place
+ OSVDB-27071: /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS).  http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3931: /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS).
http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-
2000-02.html.
+ OSVDB-4598: /members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-2946: /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ Cookie csrftoken created without the httponly flag
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3299: /forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20'';%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See
http://www.securiteam.com/securitynews/5IP0B203PI.html
+ OSVDB-3299: /forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20'';%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See
http://www.securiteam.com/securitynews/5IP0B203PI.html
+ OSVDB-3299: /htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20'';%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See
http://www.securiteam.com/securitynews/5IP0B203PI.html
+ OSVDB-3299: /vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20'';%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See
http://www.securiteam.com/securitynews/5IP0B203PI.html
+ OSVDB-3299: /vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20'';%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See
http://www.securiteam.com/securitynews/5IP0B203PI.html
+ OSVDB-724: /ans.pl?p=../../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely.  http://ans.qq.nu/ default admin string 'admin:aaLR8vE.jjhss:root@127.0.0.1', password file location
'ans_data/ans.passwd'
+ OSVDB-724: /ans/ans.pl?p=../../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely.
+ 6544 items checked: 0 error(s) and 20 item(s) reported on remote host
+ End Time:           2024-11-20 19:57:14 (GMT0) (323 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
23  -rw-r--r--  1 runner docker  26840 Nov 20 19:57 nikto-report.html
```

- The report of the DAST:

  you can find it here action under Artifacts/nikto-report

localhost / 127.0.0.1 port 8000

Target IP	127.0.0.1
Target hostname	localhost
Target Port	8000
HTTP Server	WSGIServer/0.2 CPython/3.10.12
Site Link (Name)	http://localhost:8000
Site Link (IP)	http://127.0.0.1:8000

URI	/
HTTP Method	GET
Description	Uncommon header 'x-frame-options' found, with contents: DENY
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	Uncommon header 'referrer-policy' found, with contents: same-origin
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	Uncommon header 'x-content-type-options' found, with contents: nosniff
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0
URI	/SilverStream
HTTP Method	GET
Description	/SilverStream: SilverStream allows directory listing
Test Links	http://localhost:8000/SilverStream http://127.0.0.1:8000/SilverStream
OSVDB Entries	OSVDB-17113
URI	/phpimageview.php?pic=javascript:alert(8754)
HTTP Method	GET
Description	/phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/phpimageview.php?pic=javascript:alert(8754) http://127.0.0.1:8000/phpimageview.php?pic=javascript:alert(8754)
OSVDB Entries	OSVDB-27071
URI	/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent

URI	/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent
HTTP Method	GET
Description	/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent http://127.0.0.1:8000/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent
OSVDB Entries	OSVDB-3931
URI	/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0
HTTP Method	GET
Description	/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0 http://127.0.0.1:8000/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0
OSVDB Entries	OSVDB-0
URI	/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index
HTTP Method	GET
Description	/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index http://127.0.0.1:8000/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index
OSVDB Entries	OSVDB-0
URI	/members.asp?SF=%22;]alert(223344);function%20x(){v%20=%22
HTTP Method	GET
Description	/members.asp?SF=%22;]alert(223344);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/members.asp?SF=%22;]alert(223344);function%20x(){v%20=%22 http://127.0.0.1:8000/members.asp?SF=%22;]alert(223344);function%20x(){v%20=%22
OSVDB Entries	OSVDB-4598
URI	/forum_members.asp?find=%22;]alert(9823);function%20x(){v%20=%22
HTTP Method	GET
Description	/forum_members.asp?find=%22;]alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/forum_members.asp?find=%22;]alert(9823);function%20x(){v%20=%22 http://127.0.0.1:8000/forum_members.asp?find=%22;]alert(9823);function%20x(){v%20=%22
OSVDB Entries	OSVDB-2946
URI	/login/
HTTP Method	GET
Description	Cookie csrftoken created without the httponly flag
Test Links	http://localhost:8000/login/ http://127.0.0.1:8000/login/
OSVDB Entries	OSVDB-0
URI	/login/
HTTP Method	GET
Description	/login/: This might be interesting...
Test Links	http://localhost:8000/login/ http://127.0.0.1:8000/login/
OSVDB Entries	OSVDB-3092
URI	/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22

URI	/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/ans.pl?p=../../../../usr/bin/id|&blah
HTTP Method	GET
Description	/ans.pl?p=../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely. http://ans.gq.nu/ default admin string 'admin:aaLR8vE.jjhss:root@127.0.0.1', password file location 'ans_data/ans.passwd'
Test Links	http://localhost:8000/ans.pl?p=../../../../usr/bin/id|&blah http://127.0.0.1:8000/ans.pl?p=../../../../usr/bin/id|&blah
OSVDB Entries	OSVDB-724
URI	/ans/ans.pl?p=../../../../usr/bin/id|&blah
HTTP Method	GET
Description	/ans/ans.pl?p=../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely.

URI	/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/ans.pl?p=../../../../usr/bin/id|&blah
HTTP Method	GET
Description	/ans.pl?p=../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely. http://ans.gq.nu/ default admin string 'admin:aaLR8vE.jjhss:root@127.0.0.1', password file location 'ans_data/ans.passwd'
Test Links	http://localhost:8000/ans.pl?p=../../../../usr/bin/id|&blah http://127.0.0.1:8000/ans.pl?p=../../../../usr/bin/id|&blah
OSVDB Entries	OSVDB-724
URI	/ans/ans.pl?p=../../../../usr/bin/id|&blah
HTTP Method	GET
Description	/ans/ans.pl?p=../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely.
Test Links	http://localhost:8000/ans/ans.pl?p=../../../../usr/bin/id|&blah http://127.0.0.1:8000/ans/ans.pl?p=../../../../usr/bin/id|&blah
OSVDB Entries	OSVDB-724

Host Summary

Start Time	2024-11-20 19:51:51
End Time	2024-11-20 19:57:14
Elapsed Time	323 seconds
Statistics	6544 items checked, 0 errors, 20 findings

Scan Summary

Software Details	Nikto 2.1.5
CLI Options	-h http://127.0.0.1:8000 -o nikto-report.html -Format html
Hosts Tested	1
Start Time	Wed Nov 20 19:51:51 2024
End Time	Wed Nov 20 19:57:14 2024
Elapsed Time	323 seconds

- Link to last action.

Task 4: Analyze vulnerabilities

- Analyze at least one critical or medium vulnerability and describe it based on the CWE or CVE databases.

What is the vulnerability score, the impact, the required privilege, etc.

Solution:

Vulnerability: PHP Image View Cross-Site Scripting (XSS)

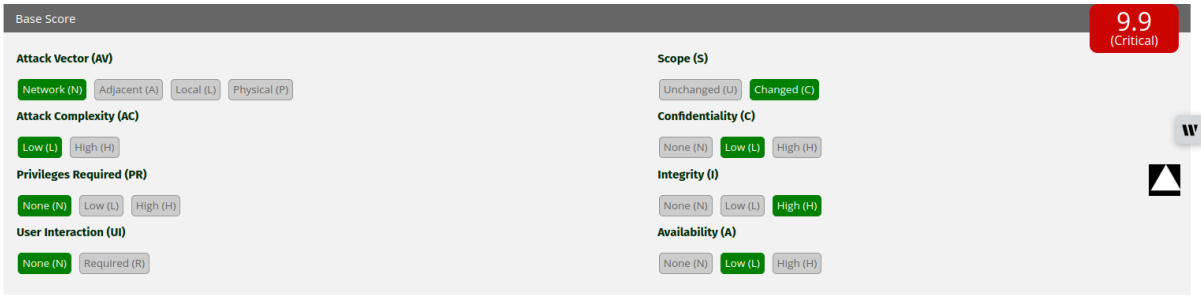
- **URI**: /phpimageview.php?pic=javascript:alert(8754)
- **Description**: PHP Image View 1.0 is vulnerable to Cross-Site Scripting (XSS). This allows an attacker to inject arbitrary JavaScript code into the application.
- **Impact**:
    - An attacker could execute malicious scripts in the context of a user's browser.
    - This can lead to:
        - Theft of session cookies.
        - Execution of unauthorized actions on behalf of the victim (CSRF).
        - Phishing or malware delivery.

Analysis of the Vulnerability:

1. CVSS Score

   Using the Common Vulnerability Scoring System (CVSS), this vulnerability typically has:

    - **Base Score**: 9.9 (Critical)



2. CWE Reference:

    - **CWE-79**: Improper Neutralization of Input During Web Page Generation ('Cross-Site Scripting').
    - The application fails to validate or sanitize user input before rendering it in the browser, allowing attackers to inject scripts.

Remediation Steps:

1. Input Validation:

    - Sanitize all user inputs to ensure only valid data is accepted.

- Use a server-side library like ```htmlspecialchars`` in PHP to escape potentially dangerous characters.

2. Output Encoding:
    - Encode any data before rendering it in the browser to prevent injection.
3. Content Security Policy (CSP):
    - Add a CSP header to restrict the execution of scripts:

```
Content-Security-Policy: default-src 'self';
```

Required Privileges:

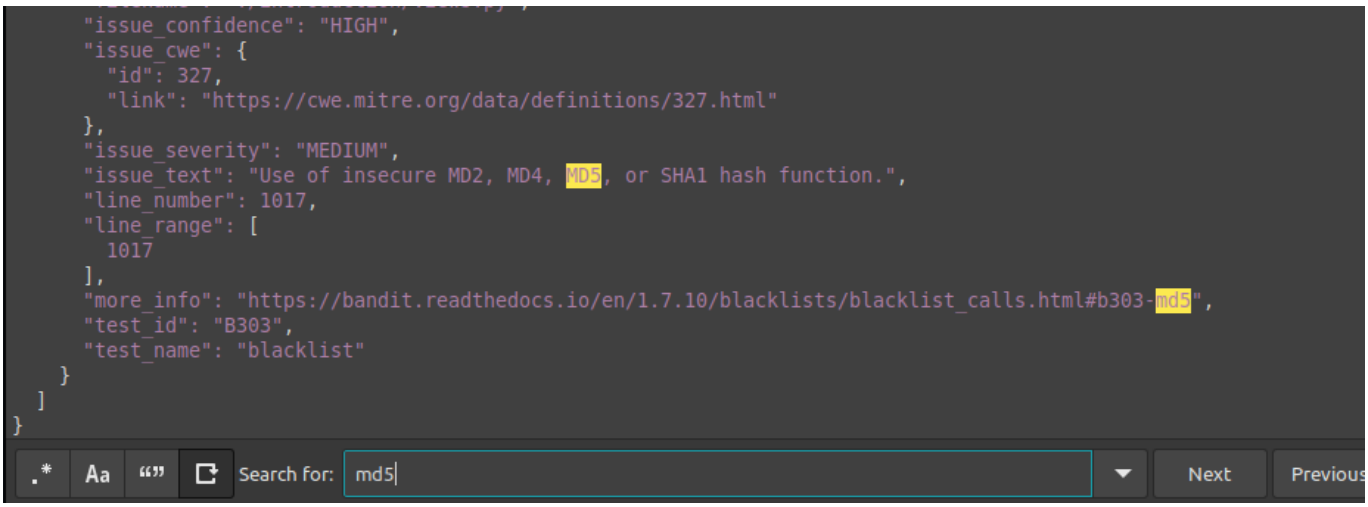
- None: The vulnerability is exploitable without authentication, making it critical in multi-user environments.

Bonus task: Patch vulnerability

- Patch some vulnerabilities in the application code or the Docker image and show the results from your SAST and DAST scan to validate your fix.

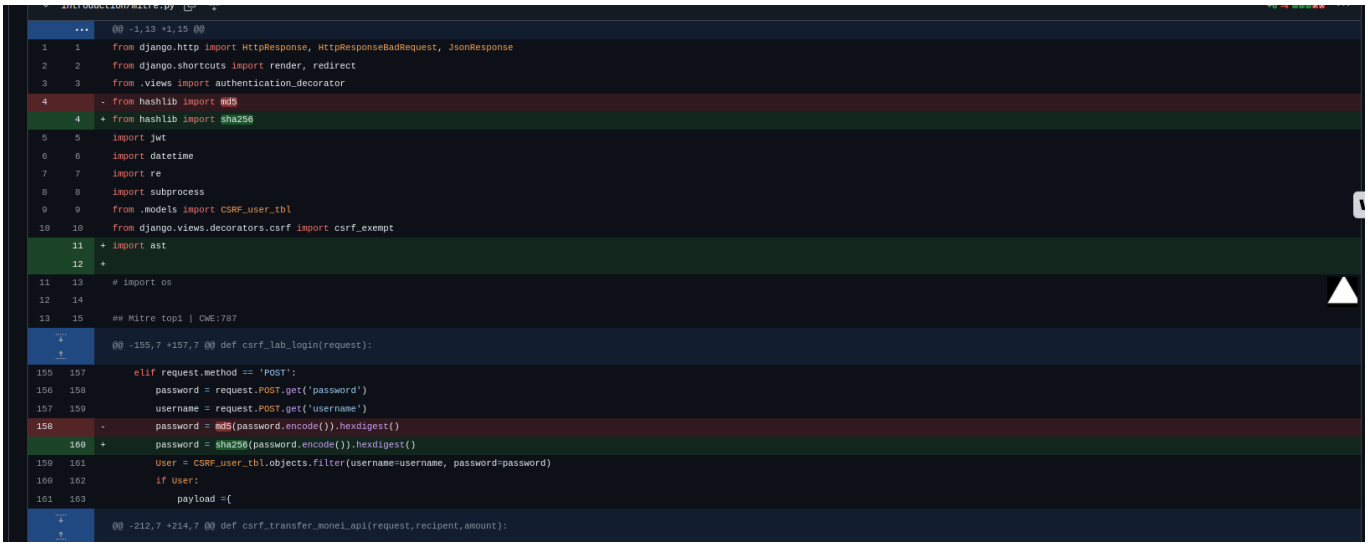
Solution:

before patching:



after patching:

You can check the bandit-report file in the artificat section:


introduction/mitre.py
@@ -1,13 +1,15 @@
from django.http import HttpResponse, HttpResponseBadRequest, JsonResponse
from django.shortcuts import render, redirect
from .views import authentication_decorator
- from hashlib import md5
+ from hashlib import sha256
import jwt
import datetime
import re
import subprocess
from .models import CSRF_user_tbl
from django.views.decorators.csrf import csrf_exempt
+ import ast
+
import os
Mitre top1 | CWE:787
@@ -155,7 +157,7 @@ def csrf_lab_login(request):
elif request.method == 'POST':
password = request.POST.get('password')
username = request.POST.get('username')
- password = md5(password.encode()).hexdigest()
+ password = sha256(password.encode()).hexdigest()
User = CSRF_user_tbl.objects.filter(username=username, password=password)
if User:
payload ={
@@ -212,7 +214,7 @@ def csrf_transfer_monei_api(request,recipent,amount):