**COMP-5710 Workshop 1:**

**Automated Security Weakness Identification**

**User: Will May (wdm0032@auburn.edu)**

**Most frequent security weaknesses detected:**

* Use of assert detected – [B101:assert\_used]
* Standard pseudo-random generators are not suitable for security/cryptographic purposes. - [B311:blacklist]
* Subprocess call - check for execution of untrusted input - [B603:subprocess\_without\_shell\_equals\_true]

**Results:**

**File:** run\_with\_submitit.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/…

**Observations:**

* 81 lines of code
* 0 Total Issues across all levels

**File:** hubconf.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/…

**Observations:**

* 140 lines of code
* 0 Total Issues across all levels

**File:** main.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/…

**Observations:**

* 199 lines of code
* 1 LOW Total Issue (by severity)
* 1 HIGH Total Issue (by confidence)
* Use of assert detected.

**File:** engine.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/…

**Observations:**

* 120 lines of code
* 0 Total Issues across all levels

**File:** test\_all.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/…

**Observations:**

* 166 lines of code
* 0 Total Issues across all levels

**File:** converter.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/d2/…

**Observations:**

* 52 lines of code
* 0 Total Issues across all levels

**File:** train\_net.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/d2/…

**Observations:**

* 177 lines of code
* 0 Total Issues across all levels

**File:** \_\_init\_\_.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/d2/detr/…

**Observations:**

* 3 lines of code
* 0 Total Issues across all levels

**File:** config.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/d2/detr/…

**Observations:**

* 22 lines of code
* 0 Total Issues across all levels

**File:** dataset\_mapper.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/d2/detr/…

**Observations:**

* 94 lines of code
* 1 LOW Total Issue (by severity)
* 1 HIGH Total Issue (by confidence)
* Use of assert detected.

**File:** detr.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/d2/detr/…

**Observations:**

* 222 lines of code
* 3 LOW Total Issues (by severity)
* 3 HIGH Total Issues (by confidence)
* Use of assert detected x 3

**File:** \_\_init\_\_.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/datasets/…

**Observations:**

* 16 lines of code
* 0 Total Issues across all levels

**File:** coco.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/datasets/…

**Observations:**

* 122 lines of code
* 1 LOW Total Issue (by severity)
* 1 HIGH Total Issue (by confidence)
* Use of assert detected

**File:** coco\_eval.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/datasets/…

**Observations:**

* 191 lines of code
* 1 LOW Total Issue (by severity)
* 1 HIGH Total Issue (by confidence)
* Use of assert detected

**File:** coco\_panoptic.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/datasets/…

**Observations:**

* 72 lines of code
* 3 LOW Total Issues (by severity)
* 3 HIGH Total Issues (by confidence)
* Use of assert detected x 3.

**File:** panoptic\_eval.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/datasets/…

**Observations:**

* 35 lines of code
* 0 Total Issues across all levels

**File:** transforms.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/datasets/…

**Observations:**

* 198 lines of code
* 8 LOW Total Issues (by severity)
* 8 HIGH Total Issues (by confidence)
* Standard pseudo-random generators are not suitable for security/cryptographic purposes. x 7
* Use of assert detected x 1

**File:** \_\_init\_\_.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/models/…

**Observations:**

* 3 lines of code
* 0 Total Issues across all levels

**File:** backbone.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/models/…

**Observations:**

* 93 lines of code
* 1 LOW Total Issue (by severity)
* 1 HIGH Total Issue (by confidence)
* Use of assert detected

**File:** detr.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/models/…

**Observations:**

* 279 lines of code
* 7 LOW Total Issues (by severity)
* 7 HIGH Total Issues (by confidence)
* Use of assert detected x 7

**File:** matcher.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/models/…

**Observations:**

* 58 lines of code
* 1 LOW Total Issue (by severity)
* 1 HIGH Total Issue (by confidence)
* Use of assert detected

**File:** position\_encoding.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/models/…

**Observations:**

* 74 lines of code
* 1 LOW Total Issue (by severity)
* 1 HIGH Total Issue (by confidence)
* Use of assert detected

**File:** segmentation.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/models/…

**Observations:**

* 286 lines of code
* 5 LOW Total Issues (by severity)
* 5 HIGH Total Issues (by confidence)
* Use of assert detected x 5

**File:** transformer.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/models/…

**Observations:**

* 241 lines of code
* 0 Total Issues across all levels

**File:** \_\_init\_\_.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/util/…

**Observations:**

* 0 lines of code
* 0 Total Issues across all levels

**File:** box\_ops.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/util/…

**Observations:**

* 58 lines of code
* 2 LOW Total Issues (by severity)
* 2 HIGH Total Issues (by confidence)
* Use of assert detected x 2

**File:** misc.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/util/…

**Observations:**

* 369 lines of code
* 9 Total Issues (by severity)
  + 8 LOW
  + 1 MEDIUM
* 9 Total Issues (by confidence)
* Use of assert detected (severity LOW, confidence HIGH) x 2
* Try, Except, Pass detected (severity LOW, confidence HIGH)
* subprocess call - check for execution of untrusted input. (severity LOW, confidence HIGH) x 2
* Starting a process with a partial executable path (severity LOW, confidence HIGH)
* Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue. (severity MEDIUM, confidence HIGH)
* Consider possible security implications associated with pickle module. (severity LOW, confidence HIGH)
* Consider possible security implications associated with the subprocess module. (severity LOW, confidence HIGH)

**File:** plot\_utils.py

**Path:** continuous-secsoft-master/software-quality-assurance/workshops/detr-main/util/…

**Observations:**

* 84 lines of code
* 0 Total Issues across all levels