# Part 1- Reference Monitor

**Due 3 March 2021 - > Gradescope**

In this part of the assignment, you will write a security layer. The specifications will be in the link below.

Detailed assignment instructions:

https://github.com/SeattleTestbed/docs/blob/master/EducationalAssignments/ABStoragePartOne.md

Remember the attacker's objective is to bypass the file's restrictions or cause the security layer to act in a disallowed manner so you should try to anticipate it.

Important:
1.Use log instead of print
2. Your security layer should produce no output!!!
3. Remember that filenames can only contain lowercase letters and numbers.
4. Your reference monitor should be named as reference_monitor_[netid].r2py, e.g. reference_monitor_abc123.r2py
5. DO NOT put them together in a zip file. Upload them as separate files.
6. Not modify or disable any functionality of any RepyV2 API calls.

# Part 2 - Attack

**Due 13 April 2021 ->NYU classes**

In this part of the assignment, you will pretend to be an attacker. Remember the attacker's objective is to bypass the file's restrictions or cause the security layer to act in a disallowed manner. You should be able to understand how the attacker thinks. Students should submit 5 different attack cases. Each case should test a different potential problem. There should be at least one accuracy test case and one security test case.

An accuracy case tests how accurate the reference monitor is allowing or disallowing certain input. This is about following specifications. A security case tests more for vulnerabilities that lead to compromising accuracy, consistency, or integrity and thus is more about exploiting things that might have been overlooked. Think of things like allowing a nop sled through, or exploiting timing. You can also include an efficiency case testing the efficient use of resources as well.

In the documentation, it states that you will gain points for every reference monitor broken, we won't be doing that. Instead, we would be grading you on whether you have 5 different valid cases. Different here is defined as if it tests a different problem, so a test case that tests whether there is an 'S' in the beginning, and a separate test that tests whether there is an 'E' at

the end would not count as two different test cases. Valid is defined as whether it is a valid test case for the reference monitor, this includes whether it logs an error accurately. For example if the reference monitor disallows an invalid file to be saved, which is correct, and you output that the test failed, then this is invalid as the reference monitor should have passed the test.

Please number your attack cases, and comment in the file what issue it attempts to tackle.

# Part 3

**Due 12 May 2021 -> Gradescope**

Fix your reference monitor based on the feedback given for part 1 so that it passes the given test cases.

**RePy FAQ - No Extra Credit with this assignment**

The document containing answers to frequently asked questions aggregated into one place

Timeline

- **3 March 2021**
- Part 1 Due. Please submit on grade scope and wait for autograder to calculate your score out of 10. Unlimited submissions allowed before the due date
- **13 April 2021**
- Part 2 Due - Submit on NYU classes with all your (5) attacks in a zip file
- Can summit more (minimum is 5, the more the better)
- Attacks used to grade Part 1 Released so you can fix your reference monitors from Part 1
- **12 May 2021**
- Part 3 Due Please submit on Gradescope

**Questions**

- **What is the difference between RePy and Regular Python?**
  This is listed here in https://github.com/SeattleTestbed/docs/blob/master/Programming/PythonVsRepy.md#python-built-ins-not-in-repy
- **Can we do x y z in RePy?**
  So long as it is not part of the excluded functions (listed https://github.com/SeattleTestbed/docs/blob/master/Programming/PythonVsRepy.md#python-built-ins-not-in-repy), yes you should be able to use whatever you like
- **On the Github it says that filenames can have hyphens and other special characters, but on the pdf it says that filenames can only have lower case letters and numbers. Which is correct?**
  Please follow the pdf's instructions
- **When `Create = True` and the file already exists do we create a new file regardless?**
  No, documentation states that `Create = True` creates a new file if the file does not already exist
- **When `Create = False` and the file does not exist what should we do?**
  If the file does not exist then there is no file to open. Fail silently (The create tag just specifies whether a new file is created if it does not already exist if Create == false with no file then you would not create a new file if there is a file there was never a need to create a file anyway.The assignment also mentions that errors should not be produced by the monitor and that it needs to fail silently)
- **Where do I put/work on my reference monitor file?**
  whichever folder you ran build.py on ie TARGET_FOLDER
- **There is a discrepancy over allowed characters in the github and the class instructions**
  Follow the class instructions, only lowercase letters and numbers are allowed in the filename (not including the extension)