

Assignment 2 Part 2 Instructions

Attack Reference Monitors

- **Goal:** Better understand security mechanisms
- **Task:** Attack other students' Assignment 2, Part 1 reference monitors
- Create multiple test cases, One test per issue
 - **Must output only when a bug is found**
 - Accuracy bug
 - Security bug
 - If your test is wrong, you will lose points!
 - Refer to the instructions on the web-page: <https://github.com/SeattleTestbed/docs/blob/master/EducationalAssignments/ABStoragePartTwo.md>

Extra credit:

Find bugs in the extra credit reference monitors given the altered threat model. You should include more test cases in the extra credit!

How to run your tests on many reference monitors:

If you are using Mac or Linux, you can do something like the following:

- Put all security layer and attack cases in the same directory you were using before to run single security layer and attack program.

Then you can type the following in the bash shell to execute the testcases with the reference monitors:

```
for referencemonitor in reference_*; do for testcase in netid_*.r2py;
do python repy.py restrictions.default encasementlib.r2py $referencemo
nitor $testcase; done; done
```

What to turn in:

- Turn in the test cases used to attack the reference monitors in a zip file. The name of each testcase must start with your NetID in lowercase followed by an underscore. For example: abc321_securitytest1.r2py
- Optionally turn in the test cases used to attack the extra credit reference monitors in a separate zip file. Note that in this case, you can expect that your code is run more than once. In the name of the file, say if it needs to be run multiple times. For example: abc123_run_twice_metadata_removal.r2py

Note:

- **openfile()** and **exitall()** should not be used for the testcases