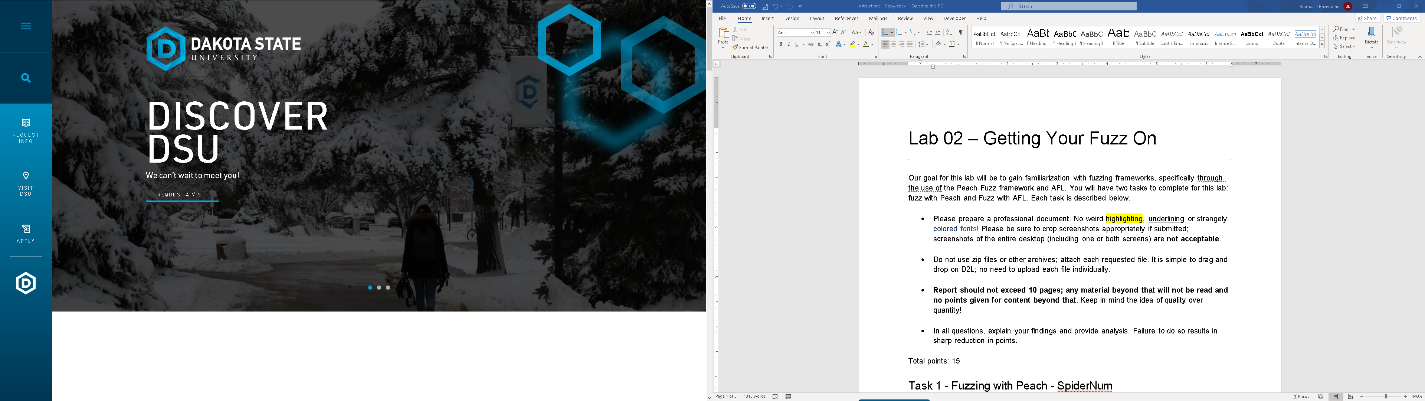
Lab 02 – Getting Your Fuzz On

The goal of this lab is to acquaint ourselves with Boofuzz. Firstly, we want to be able to install it and begin to use it. Secondly, we want to be able to fuzz and obtain some crashes.

* Please prepare a professional document. No weird highlighting, underlining or strangely colored fonts! Please be sure to crop screenshots appropriately if submitted; screenshots of the entire desktop (including one or both screens) are **not acceptable**.



* **Do not use zip files or other archives; attach each requested file.**
* **Report should not exceed 10 pages.**

## Task 1 - Fuzzing with Boofuzz - SpiderCat

Your task is to fuzz SpiderCat Server using input.

* Install Boofuzz. Watch class video and consult available documentation online. Please be sure to watch video carefully for insights into the install process.
* Here are some important web sites:
  + Boofuzz Github: <https://github.com/jtpereyda/boofuzz>
  + Boofuzz Install: <https://boofuzz.readthedocs.io/en/stable/user/install.html>
* You will need to determine if you are going to use Process Monitor or attach with a debugger to catch your crashes. Process Monitor and all its dependencies must be installed, and you will run this as Python 2.7x, whereas Boofuzz will be run as Python 3.x. Thus, with Python 3.x, we would use **py** **file.py**, whereas with Python 2.7x, we would use **python file.py**. Properly installing Process Monitor and getting it to work can be challenging, and it is recommended only for more experienced students.
* The next step is to build your own Boofuzz script. Look to class video for inspiration and guidance as well as provided samples. Remember – if you are using Process Monitor, the syntax has changed.
* Run your tests! Can you obtain a crash? If so, include evidence of the crash
* **[5 points]** Study the binary and experiment to try to get crashes. What crashes can you get? What causes the crashes? Show results from your fuzzing to indicate you were successful. Include screenshots of the scripts you created **and upload the scripts as well** This should be a professional write-up **under 10 pages** and include complete details. However, there are no formatting requirements for this lab. *Table of contents should be avoided.*
* **[3 points EC]** Can you get Process Monitor set up correctly? Include evidence of doing so, such as a narrative of your experience doing so, and screenshots showing success. **Have a text document open in the background with your name visible.**

## Task 2 - Fuzzing Vulnserver with Boofuzz

* Vulnserver has been around for a while! Try your hand at obtaining a crash by fuzzing Vulnserver with Boofuzz. Attack a command other than **kstet** or **trun**. Other methods of obtaining crashes are not accepted.
* **[5 points]** Study the binary and experiment to try to get crashes. What crashes can you get? What causes the crashes? Show results from your fuzzing to indicate you were successful. Include screenshots of the scripts you created, **and upload the scripts as well.**

**Deliverable:**

Turn in your lab report as a Word Document/PDF. **No zip files.**