Cyber Range Lab Assignment 7

Python Code Security

Jon Mahoney

SRA 440W

# General Context

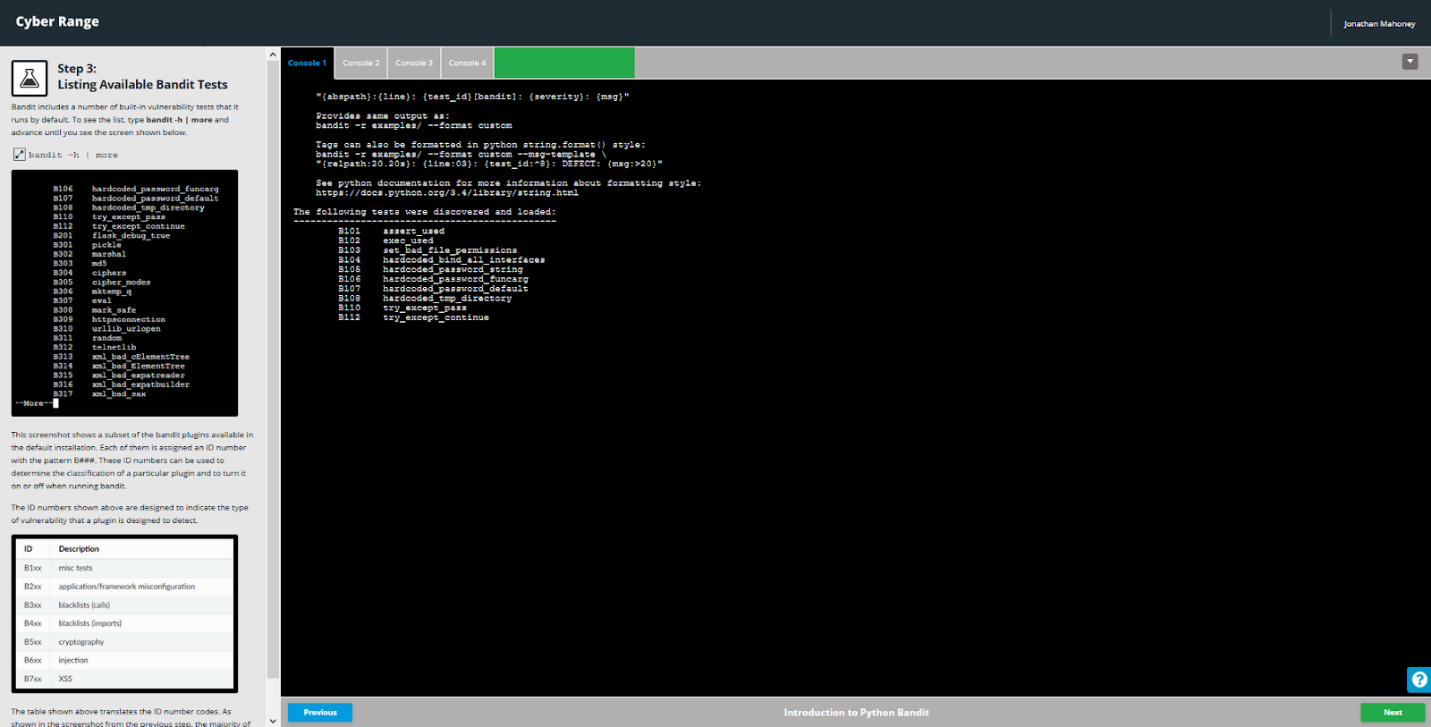
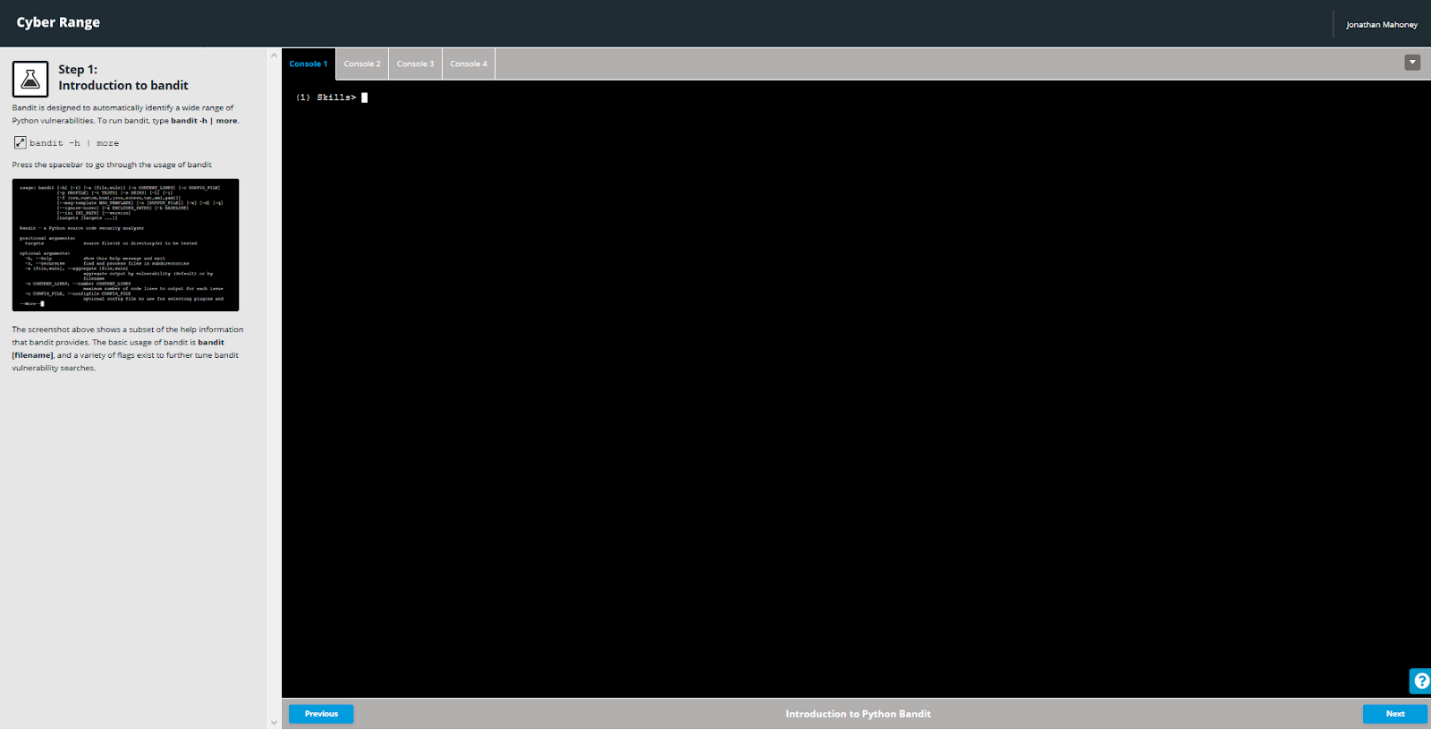
The general theme which the four labs explore can be summarized as examining vulnerabilities and exploits in Python. The first lab, introduction to Python Bandit, explains the usage of the Python security package known as Bandit. Bandit is a static analysis tool used to check Python code for common issues and works by converting code into a tree of nodes to be tested based on user specifications. After Bandit testing, a report is generated. The following lab, XML Attacks in Python, describes the different vulnerabilities that are known in Extensible Markup Language (XML) and shows them for the purpose of identification and remediation. A few of the vulnerabilities described in the lab are related to different utilities that are useful when working with XML. These utilities are external entity expansion (XXE), XInclude, and XSL. The third lab, Cross-Site Scripting in Python, describes one of the most common forms of cyber-attacks which is known as a cross-site scripting attack. The attack relies on including malicious code in sections of webpages that support user input, such as comments or reviews. In the lab, the instructions lead the user to create malicious comments to be used in exploiting a Flask web application. The final lab, Supply Chain Vulnerabilities in Python details the vulnerabilities that are present within a program’s dependencies. Some of the commands used are findimports and pydeps which are used to find imports and dependencies respectively.

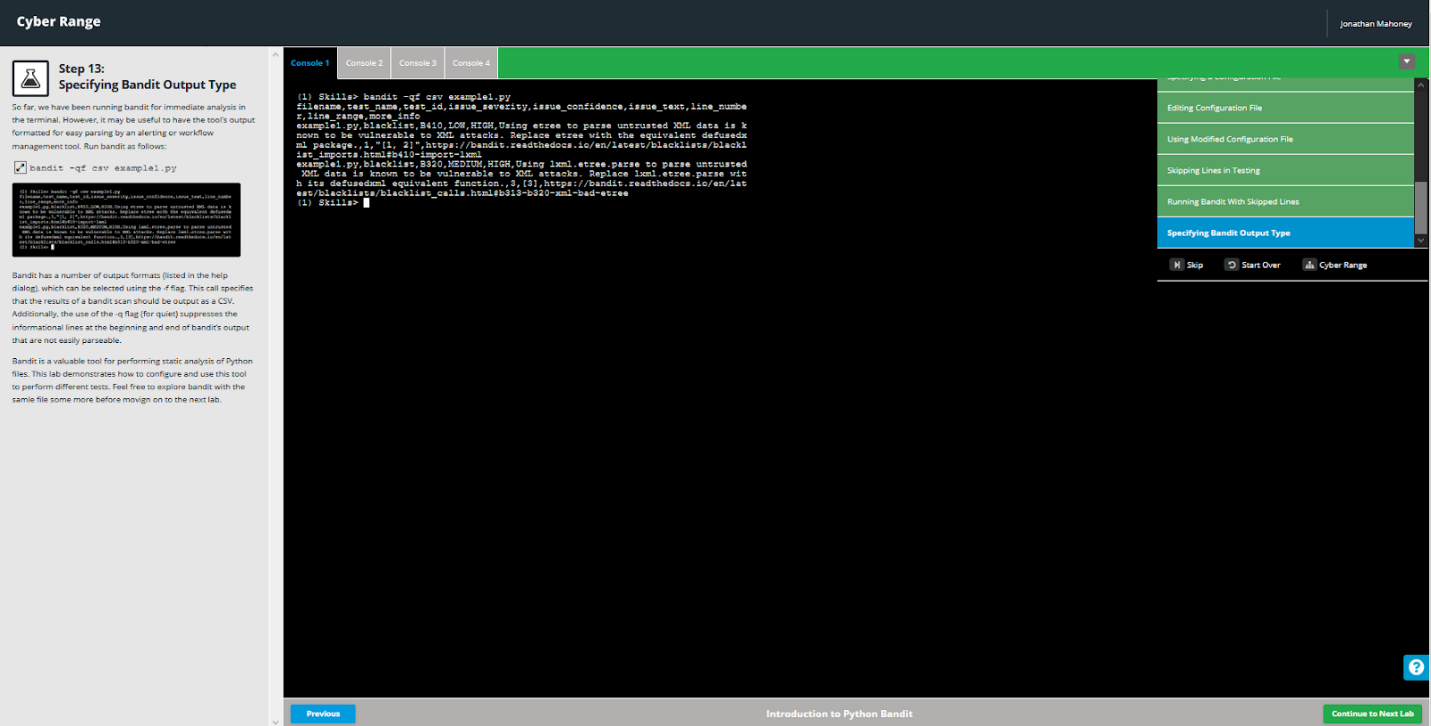
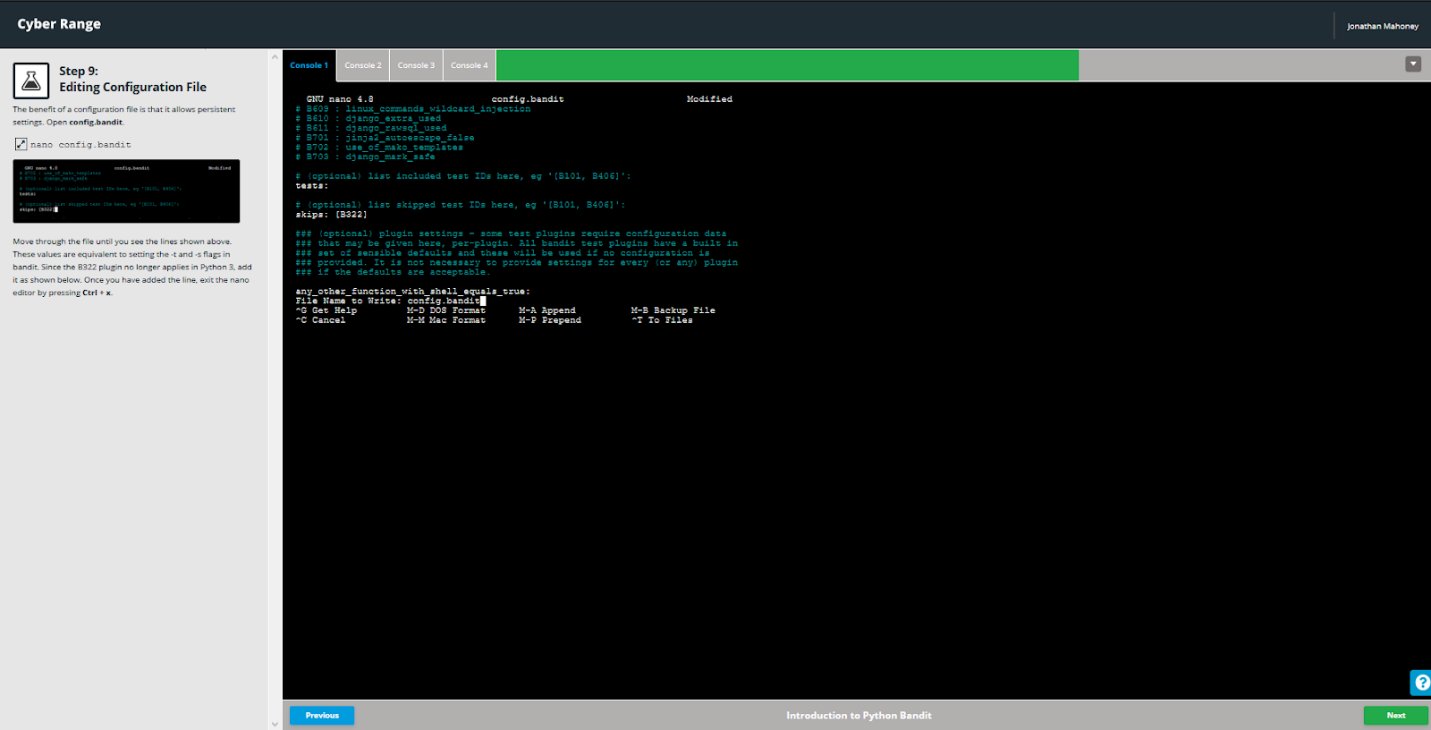
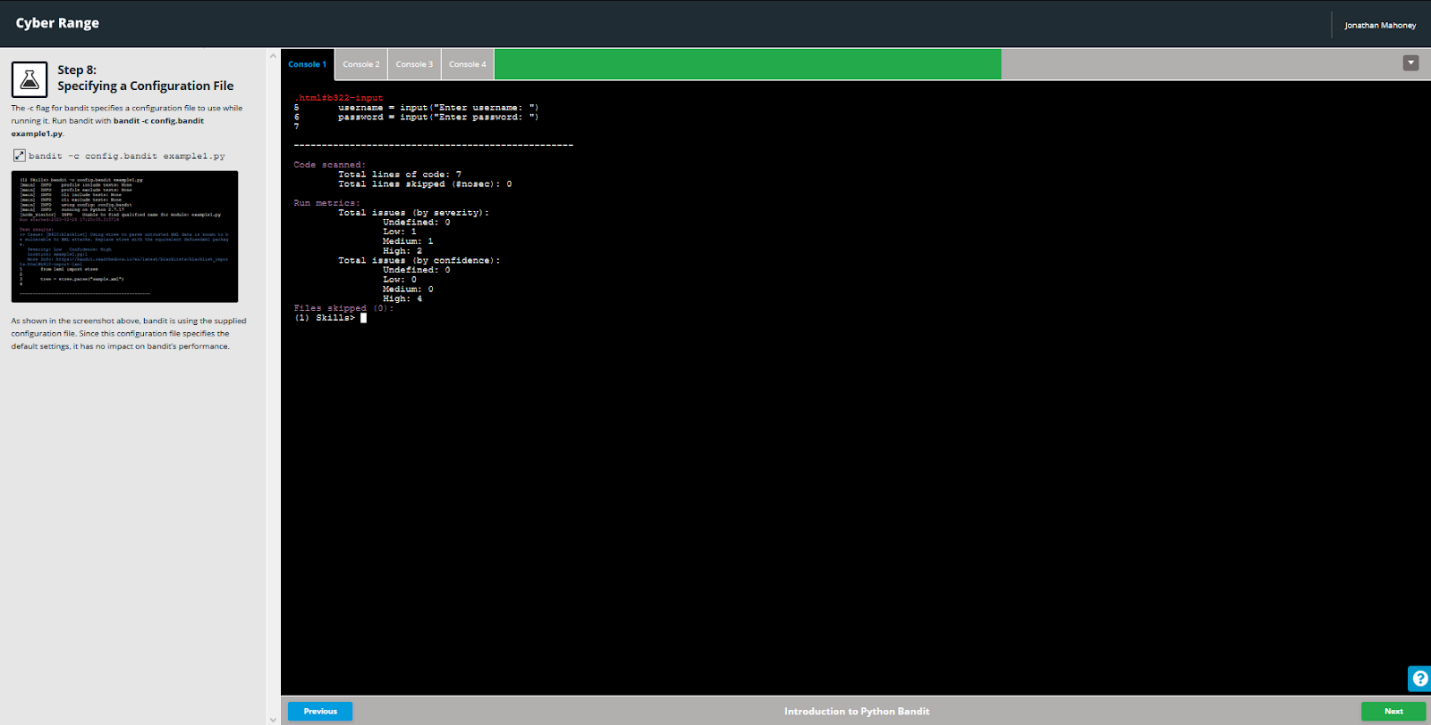
# Solution

Upon beginning the lab assignment, I quickly encountered the section in Introduction to Python Bandit that was described in class where we were told the lab required multiple “Enter” inputs to continue. Fortunately, I recalled the instructions from the professor and proceeded through this section. That being said, I did run into an issue in the section that required the use of Nano for editing text files, I forgot to properly close the text editor as there are three different Nano file menus you must proceed through when saving changes to a file and the lab would send a completion notification on the second menu. I realized there was an issue when I was stuck on a later step. To remediate the issue, I simply returned to the text editor sections and properly saved the changes. After doing so, I was able to complete the remaining steps in the first lab. The only other issue I ran into was during the Supply Chain Vulnerabilities in Python lab where you view Python packages using the pipdeptree command to list the packages as a dependency tree. I scrolled to the section shown in the instruction screen shot but the lab would not immediately progress to the next step. That being said, the final section automatically completed after scrolling to the screen shot shown in the instructions which leads me to believe it may be an error in the lab.

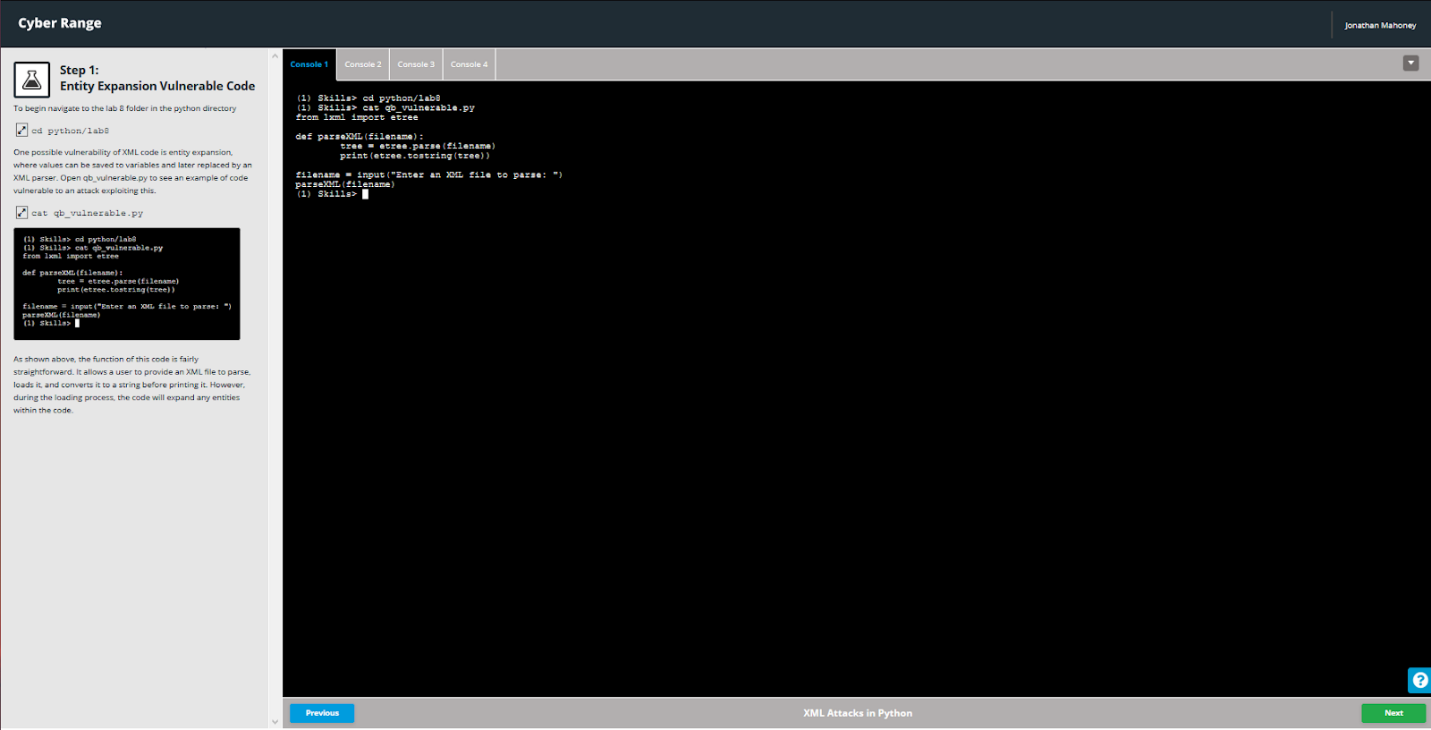
# Screenshots

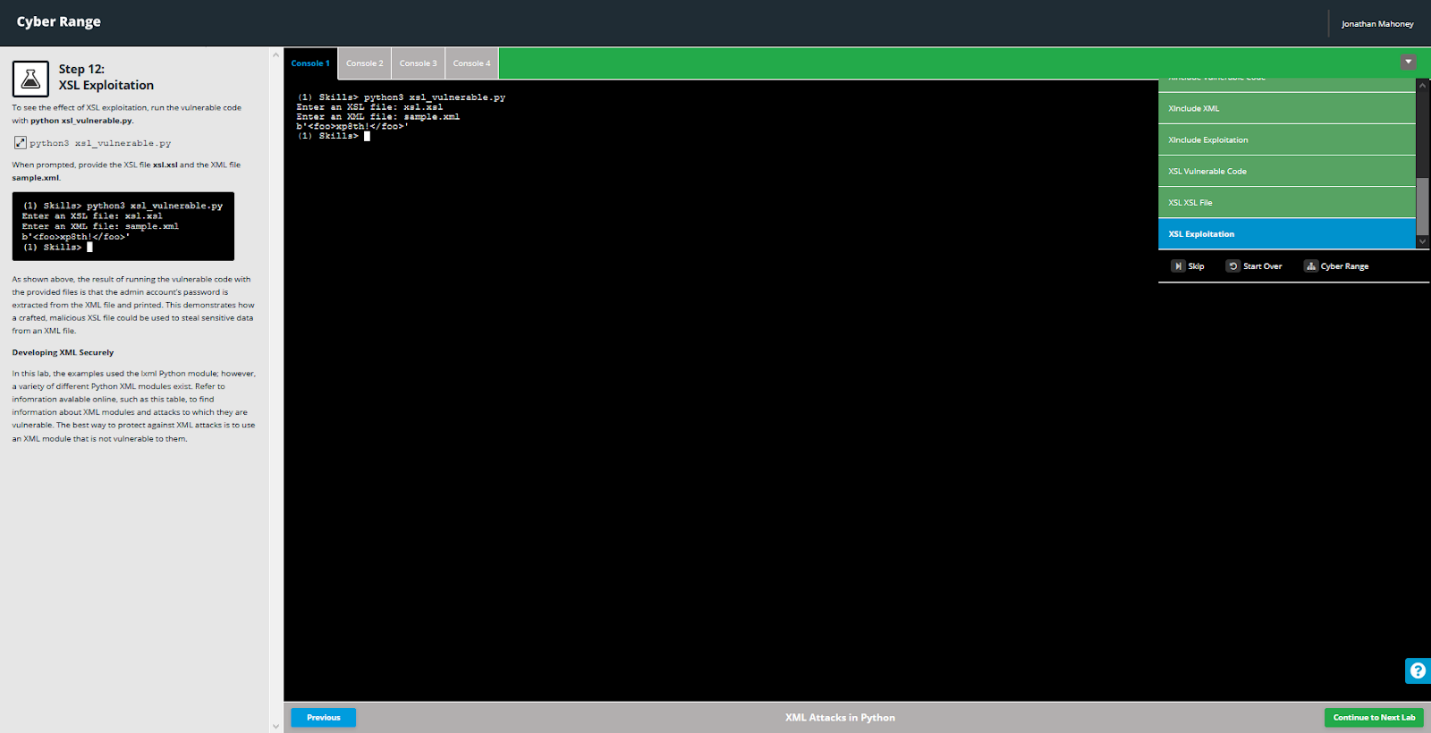
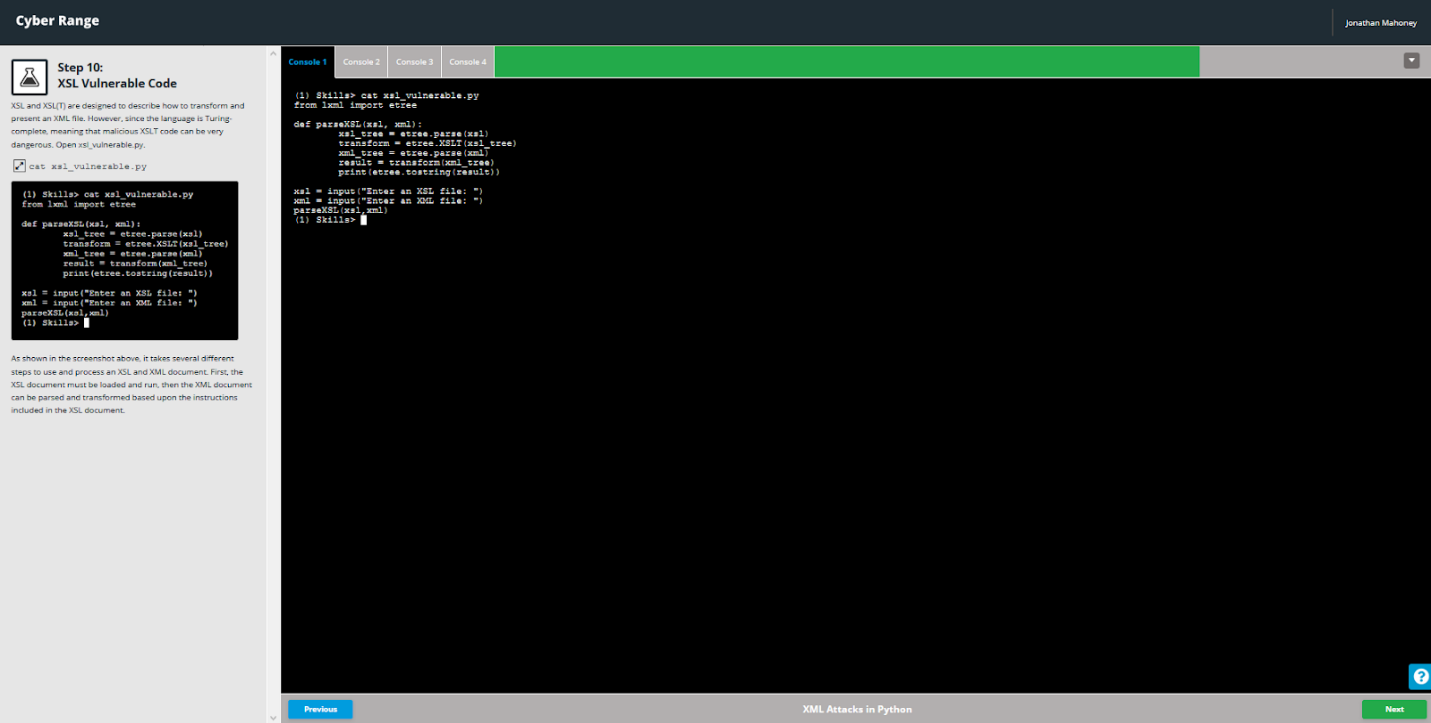
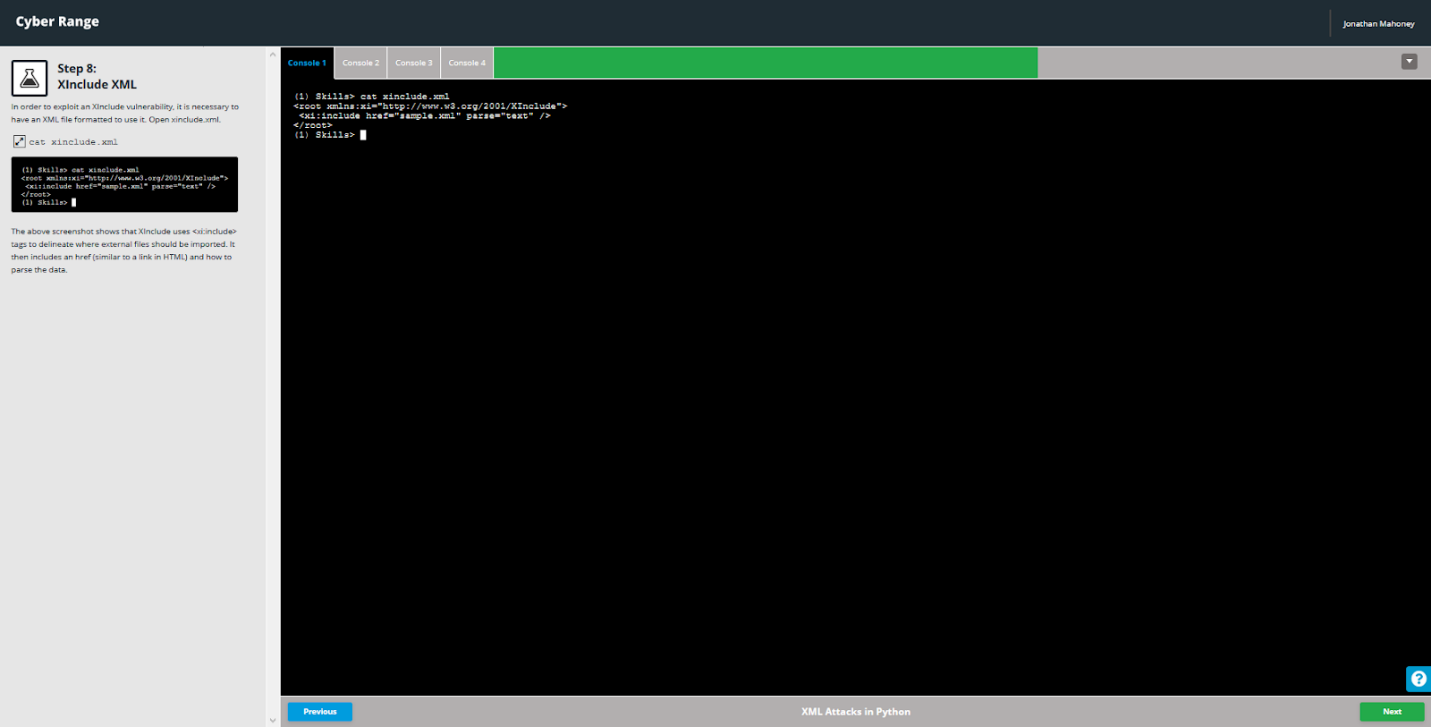
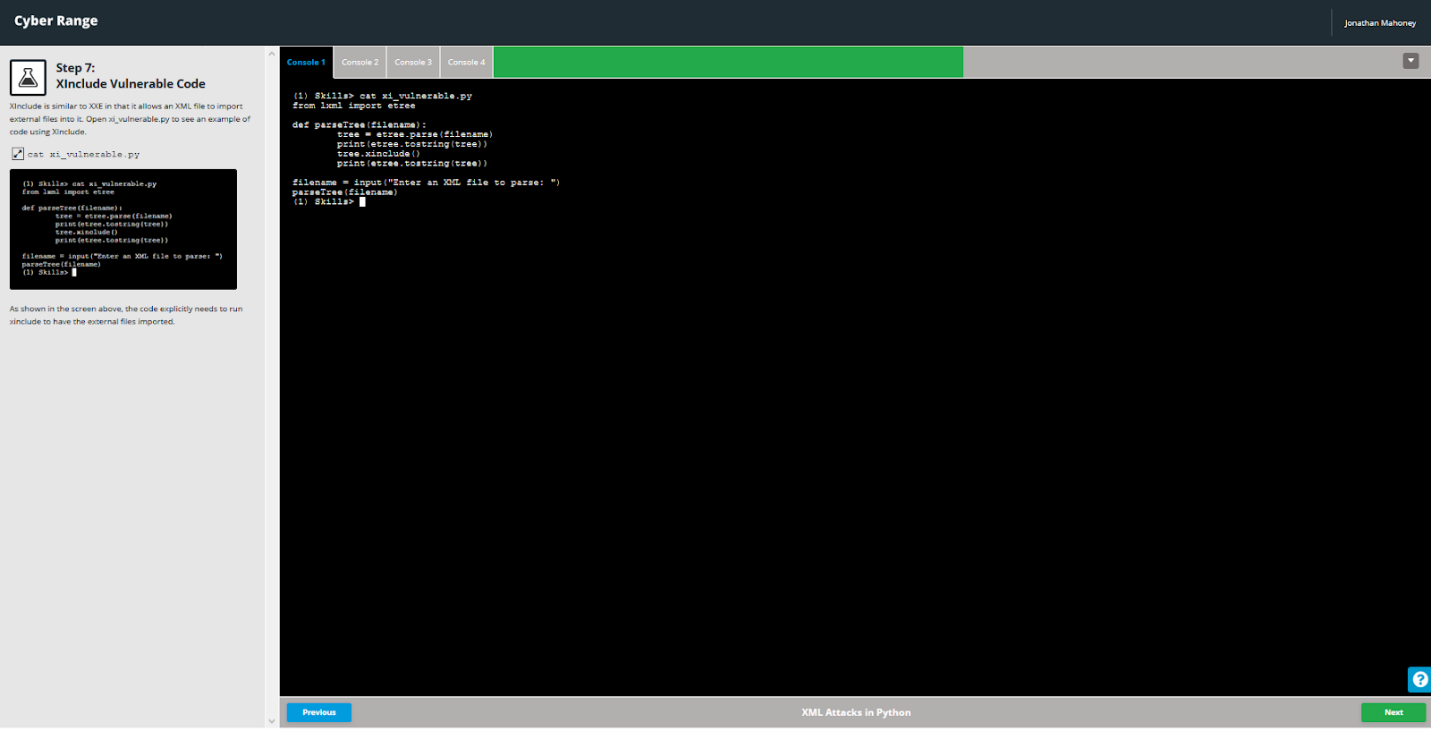
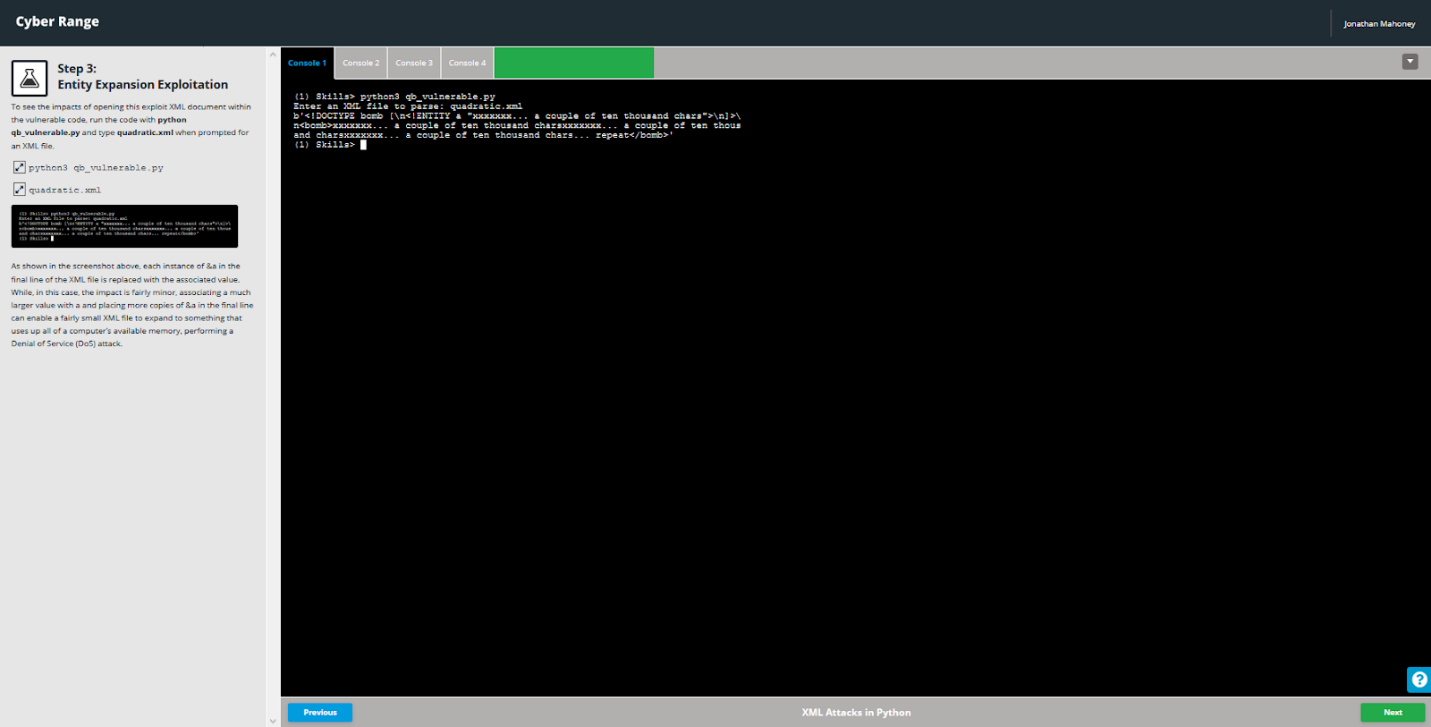
## Introduction to Python Bandit



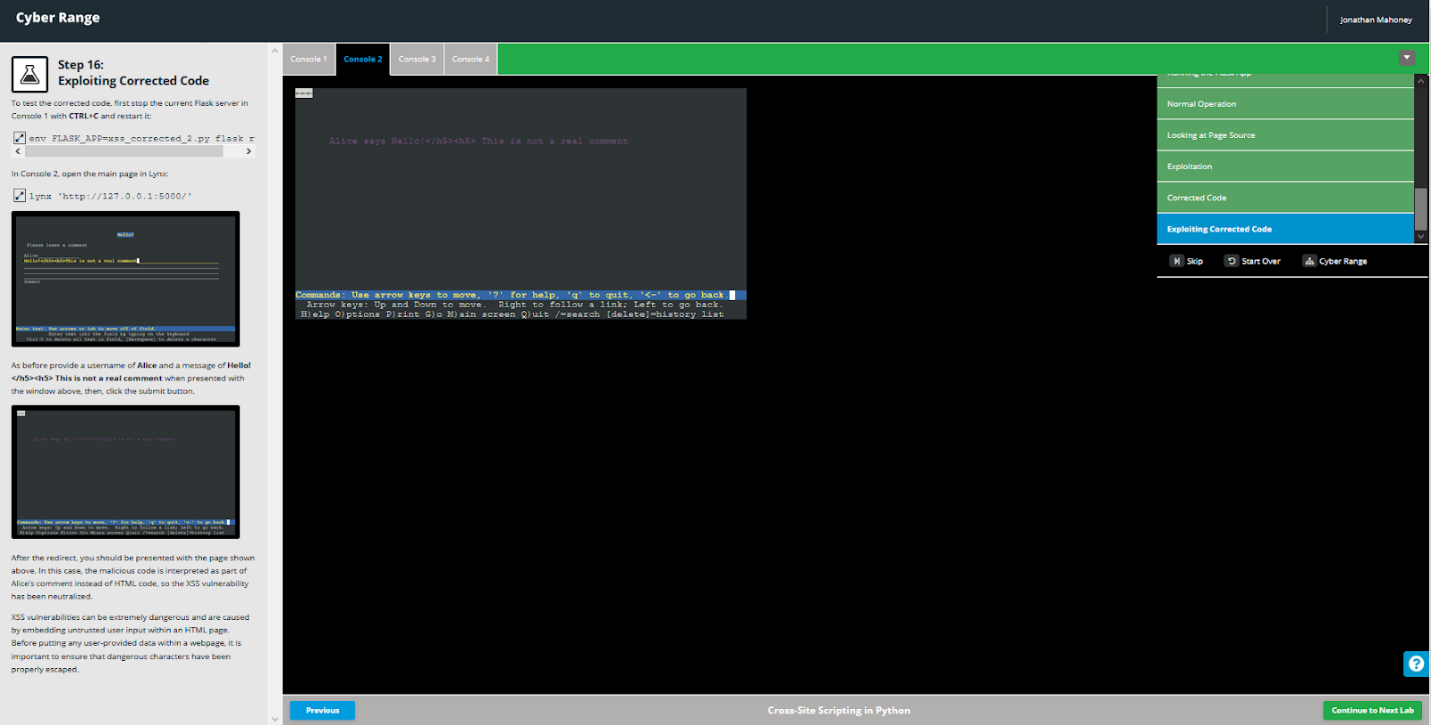
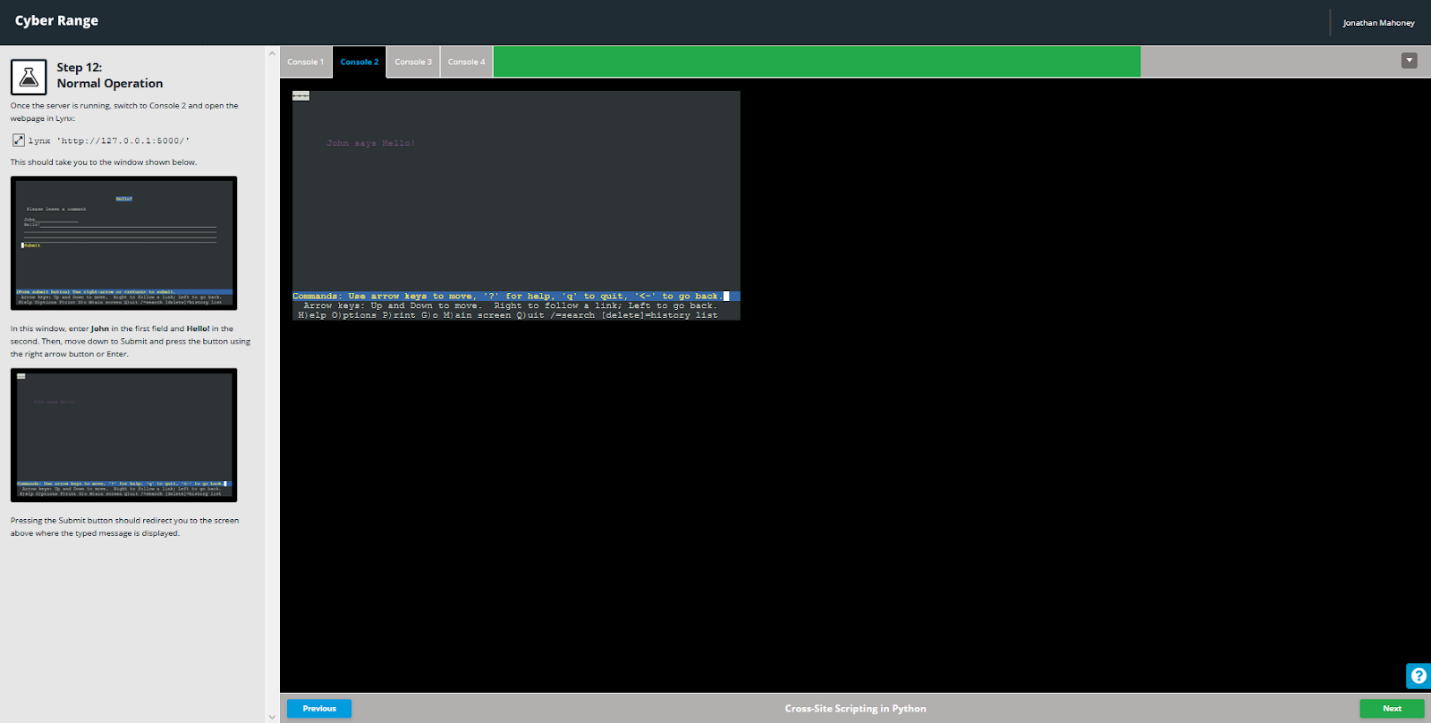
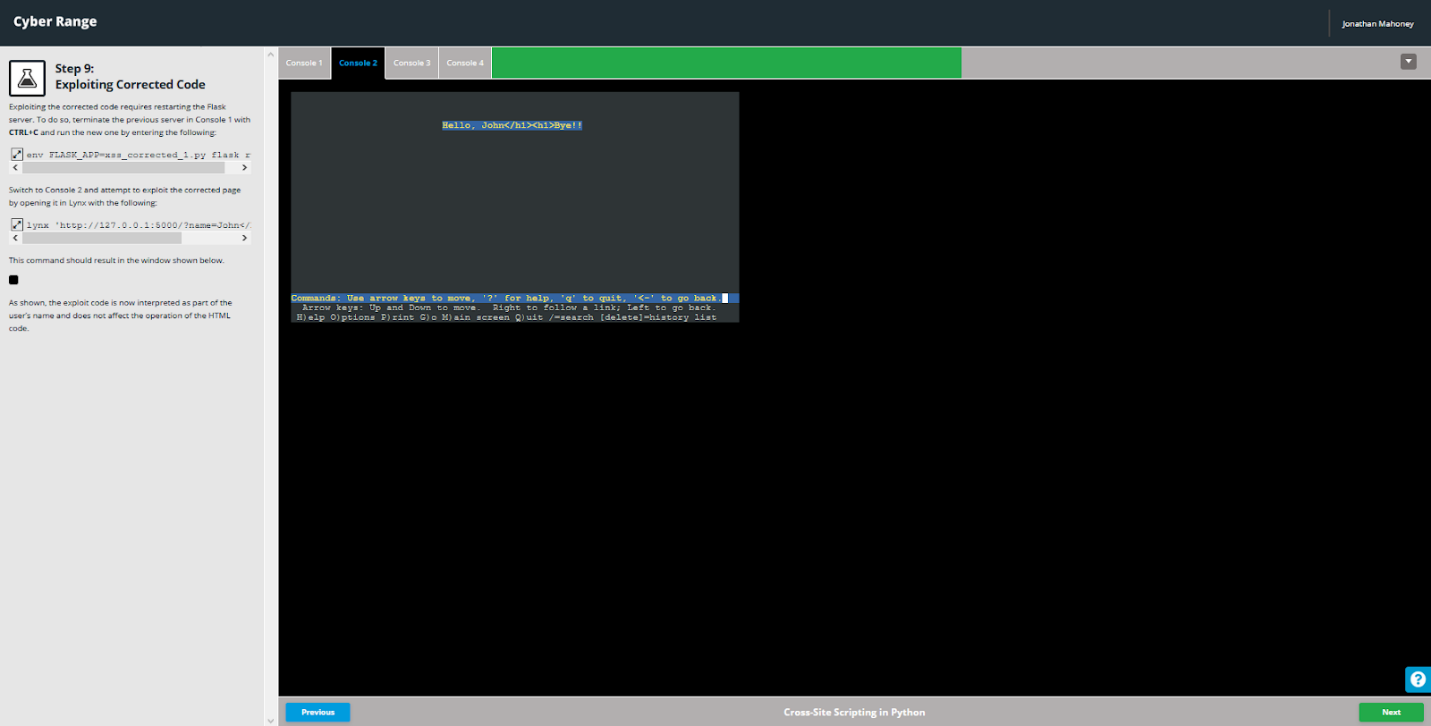
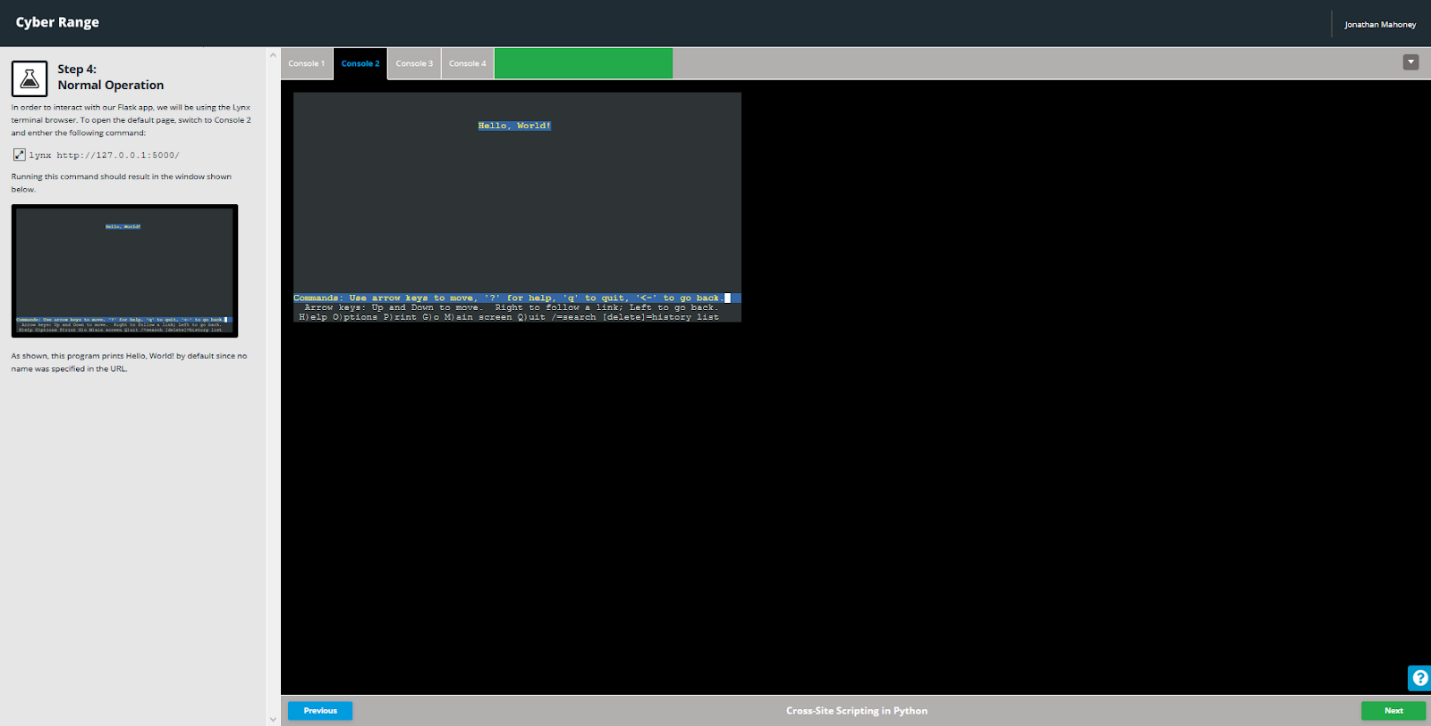
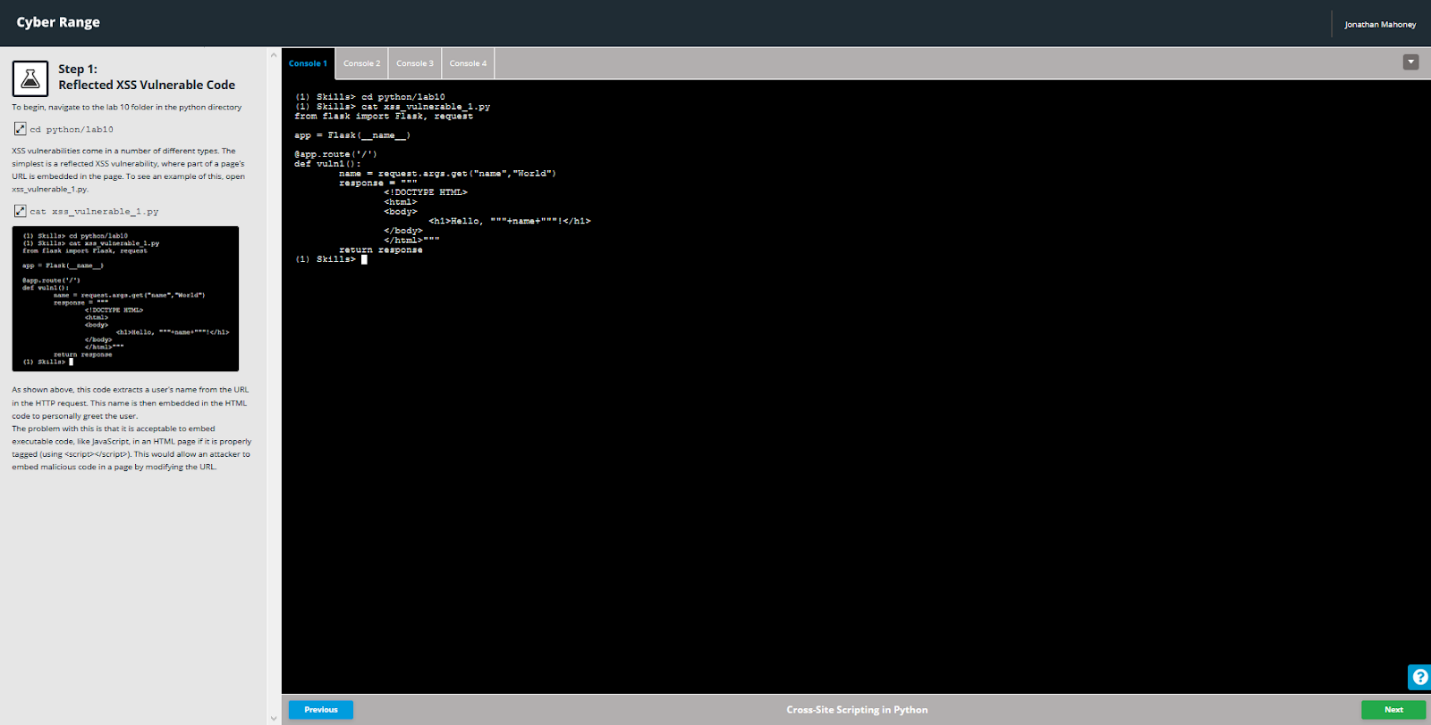


## XML Attacks in Python





## Cross-Site Scripting in Python



## Supply Chain Vulnerabilities in Python

