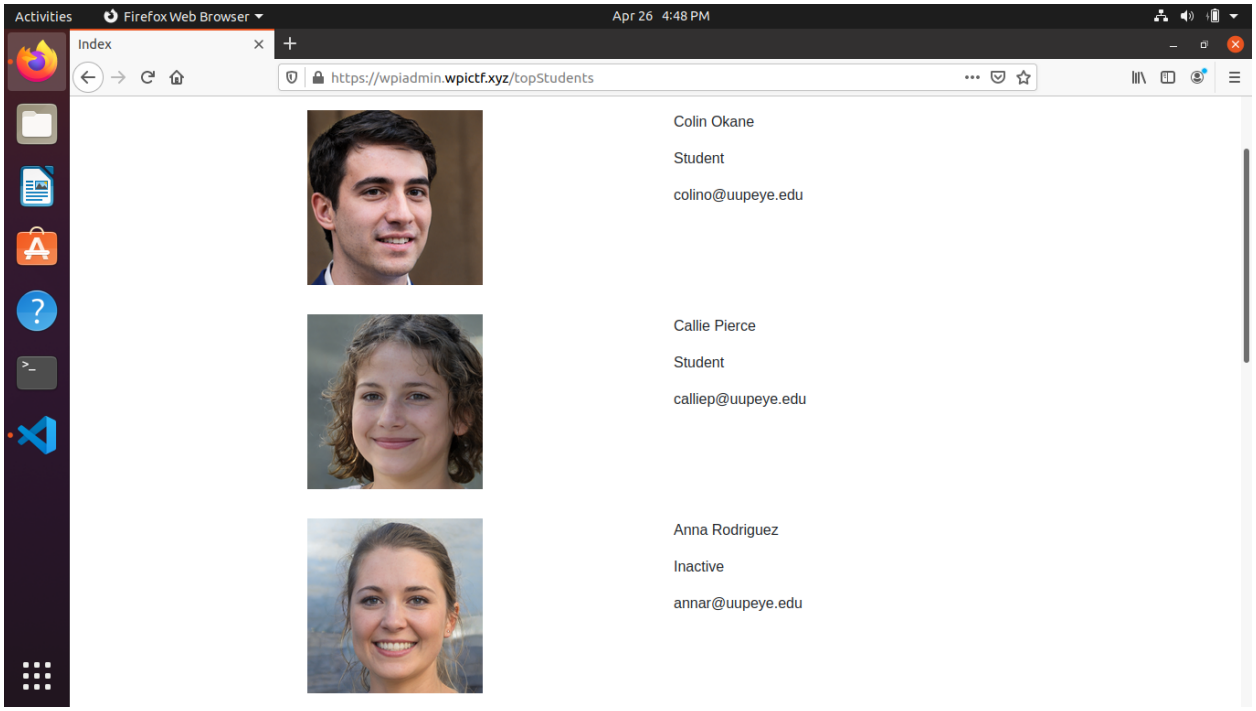
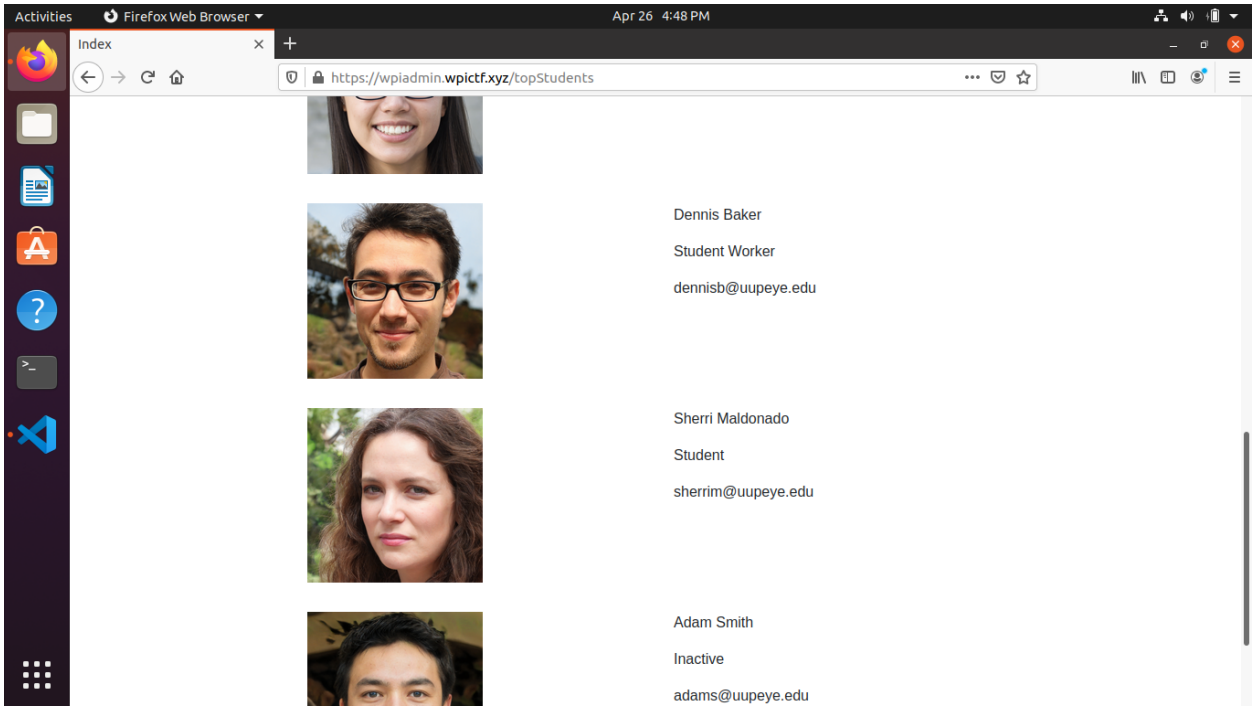
Name: Tristan Gomez
Event: WPICTF 2021

Challenge: WPI-Admin #1

Hint: Some students use bad passwords

-Starting off, I navigated to the challenge website (https://wpiadmin.wpictf.xyz) and explored the different pages. The page that stood out to me was “/topStudents”. Looking at the different students, I picked out “Colin Okane”, “Anna Rodriguez”, and “Dennis Baker” as my targets due to their different roles. I have their email addresses from this page, so that’s one half of their credentials.





-I took the hint to heart and thought, “Okay, how bad can their passwords really be?”. I googled top 10 most common passwords and started manually typing them in. Yes, you heard that correctly. I typed them in manually. It didn’t make sense to programmatically brute force a lot of passwords for a few reasons. First, the admins of the CTF made it clear to NOT brute force this challenge. Lots of people didn’t listen, and the servers kept crashing throughout the entire CTF. Second, they said that the passwords would be really easy to guess (hint: they were right), so I took them at their word. Less than five minutes later, I have access to the following three accounts.

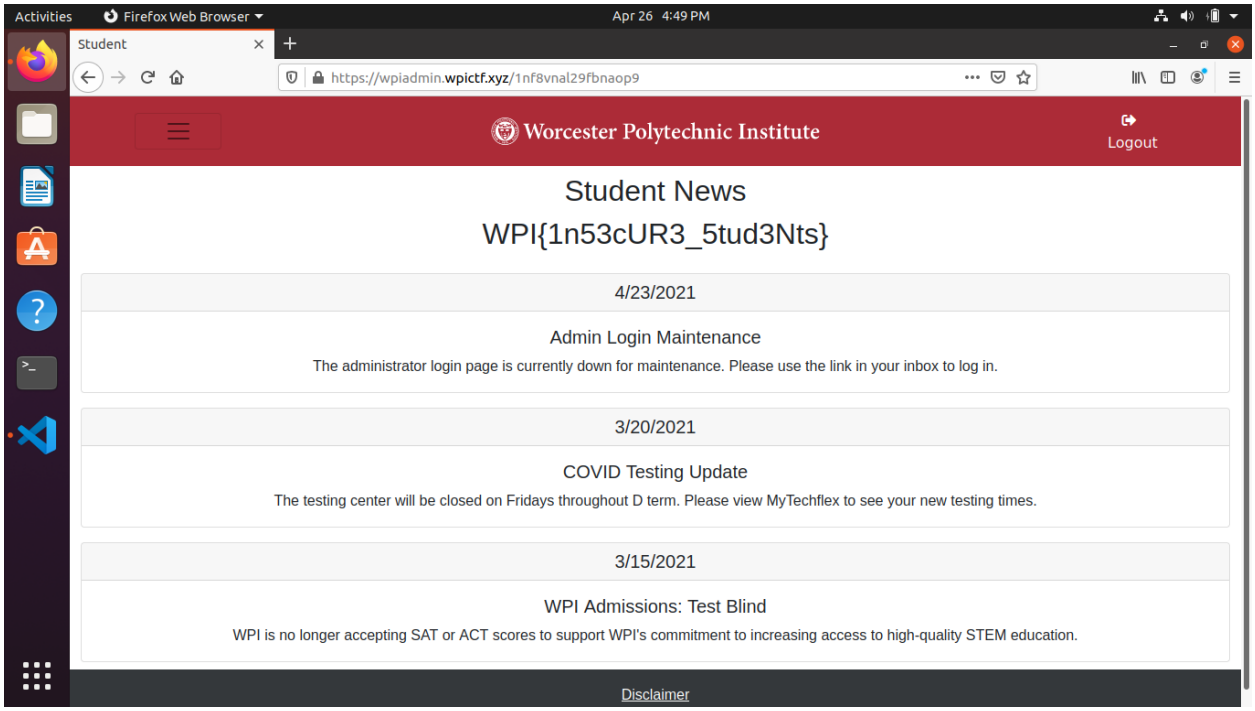
Username: colino@uupeye.edu
Password: 123456
Role: student

Username: annar@uupeye.edu
Password: iloveyou
Role: inactive

Username: dennisb@uupeye.edu
Password: 123123
Role: student worker

-Logging in with the student worker role, reveals the first flag

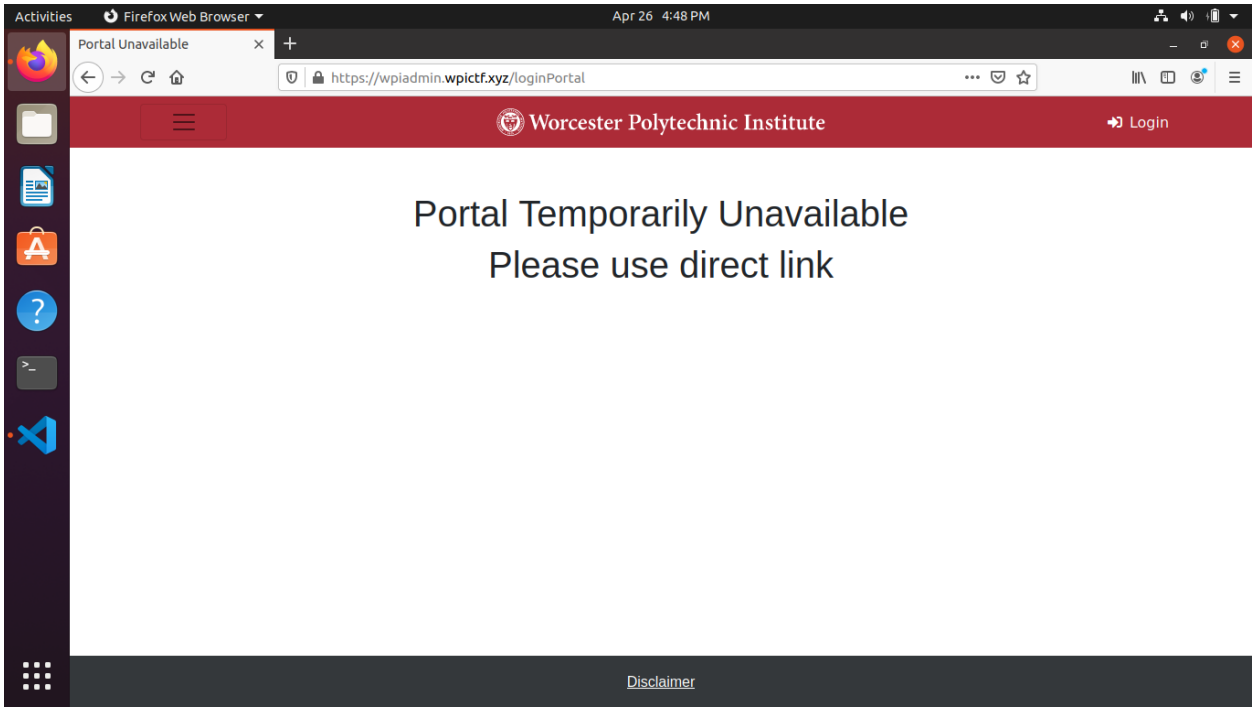
Flag: **WPI{1n53cUR3_5tud3Nts}**



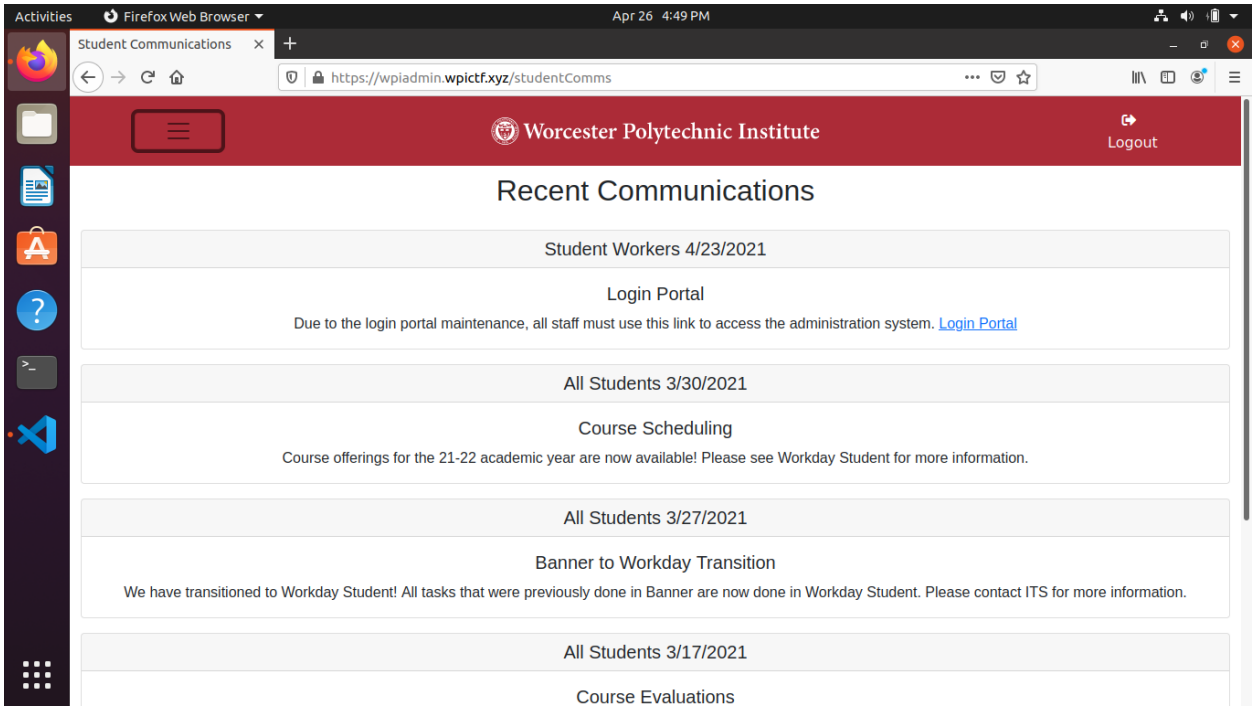
Challenge: WPI-Admin 2

Hint: What are other ways to bypass a login password?

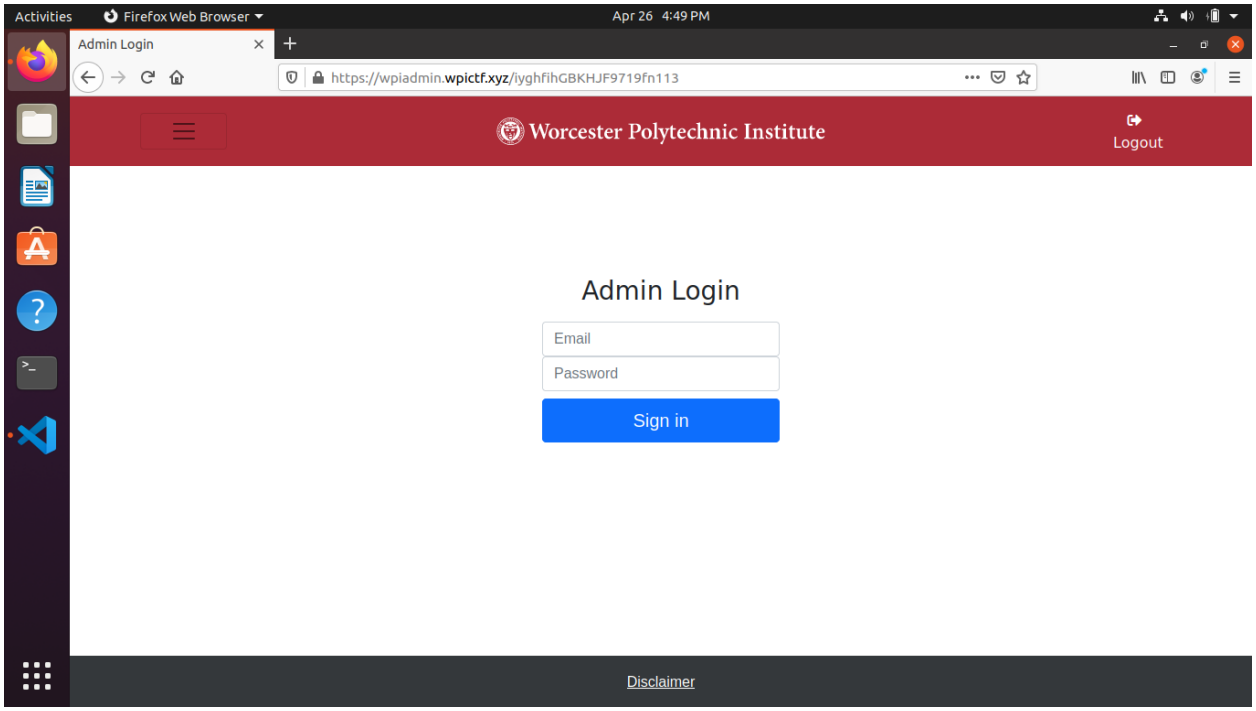
-Now that we're in, we need to login to the admin site, but how? Clicking the admin login link in the navbar shows a dead page, but there is a reference to a direct link somewhere. Hmm, let's go looking for it!



-Clicking through the different links in the navbar, I came across the /studentComms page. Right at the top is our link to the new login page. Bingo!



-Following the link, we are greeted by the admin login page. It looks almost exactly the same as the student login page.



-We don’t have an admin username that we know of at this point, but it may not be an issue. By messing with the password input field, I entered the double quote (“) character, whereas my teammate entered the single quote (‘) character in an attempt to see if we could break the password’s SQL syntax, while also determining if the site used client input in a SQL query without sanitizing it. My teammate got an “Internal Server Error” while I did not. Perfect, now we know how to break the query’s syntax. Let’s get to work.

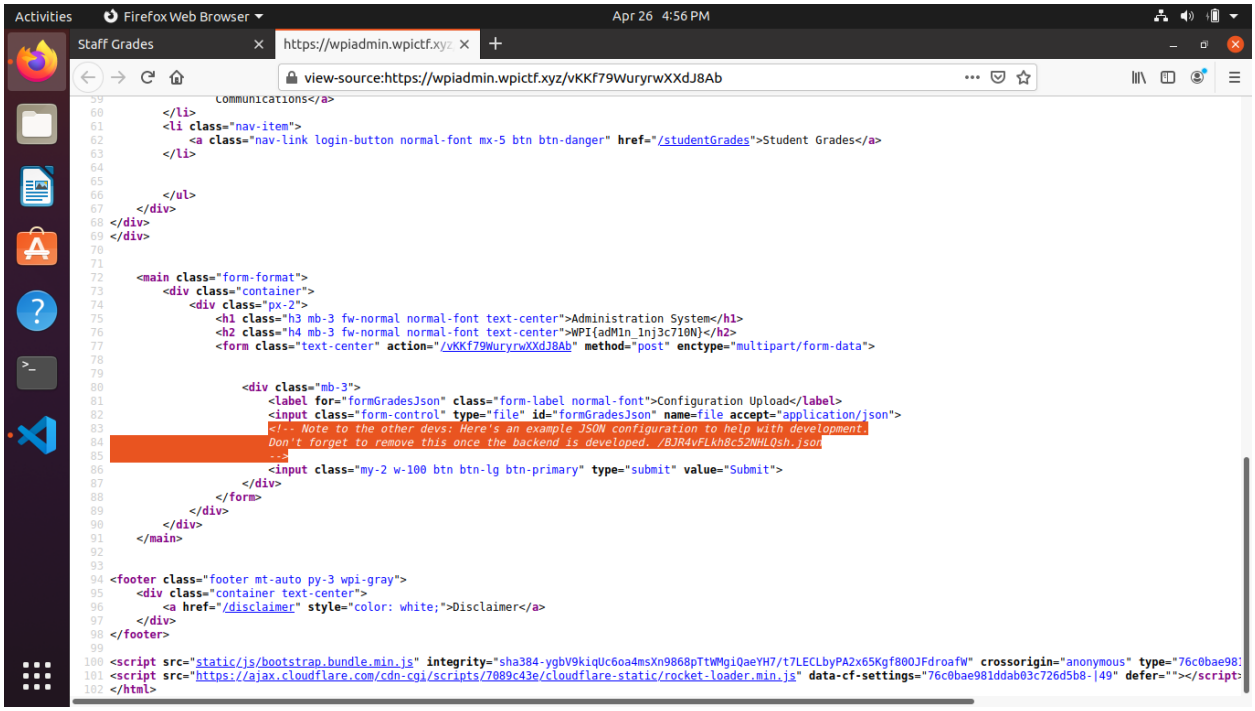
-Entering “**‘ OR 1=1 --**” in the password field, along with “admin@uupeye.edu” lets us force the SQL query to be always true, granting us admin access. As an aside, I also used “dennisb@uupeye.edu” as the username for the admin login and I was still able to get in. I think that any email address will work as the username as long as the password is “**‘ OR 1=1 --**”.

Flag: **WPI{adM1n_1nj3c710N}**

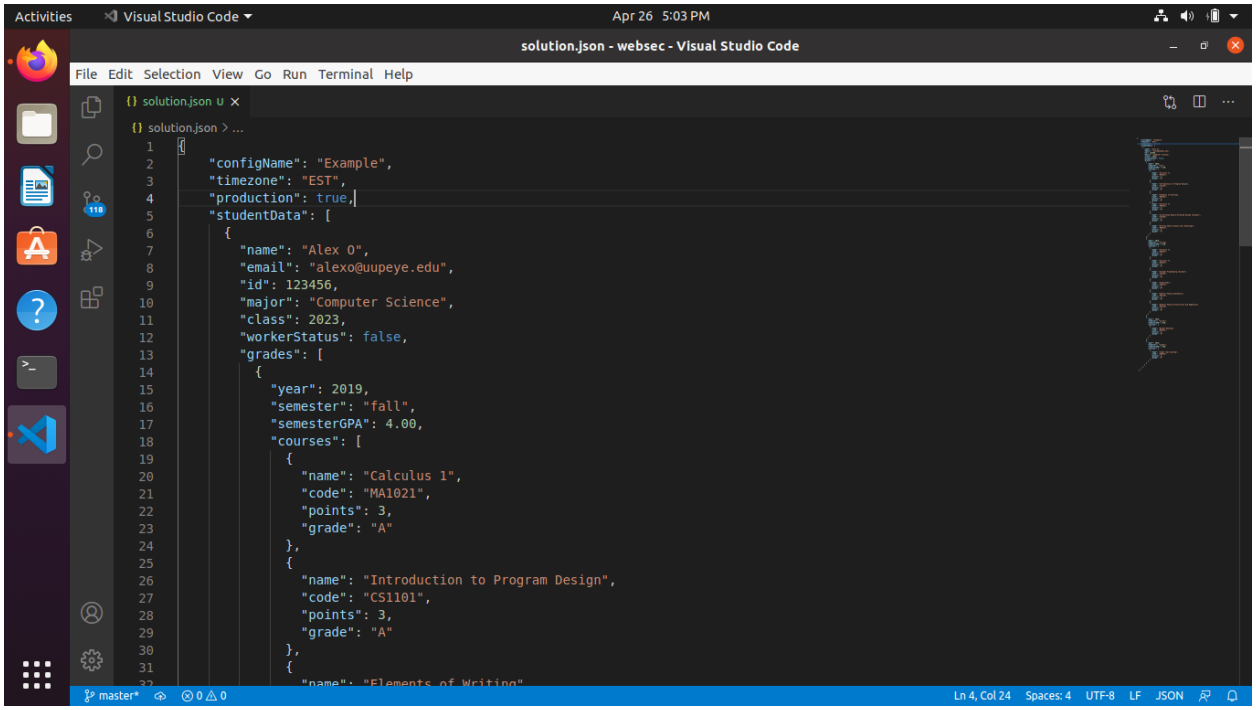
Challenge: WPI-Admin 3

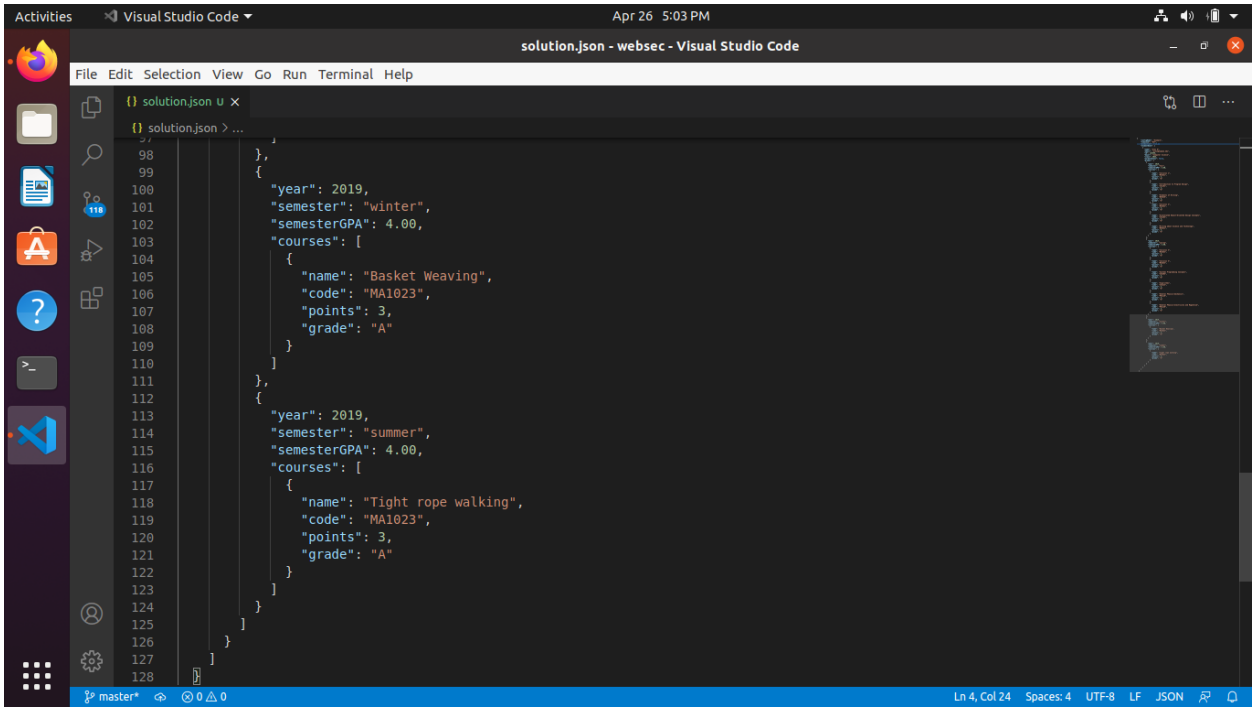
-Now that I am logged in as an admin, I am greeted by a file upload element with the title/heading “Configuration Upload”. Hmm, my mission is to change the grades of my friend, their username is “**alexo@uupeye.edu**”. The file I need to upload to change my friend’s grade is formatted in JSON. I need to find some reference for a valid JSON file for this input or else my file will be rejected by the system.

-Looking at the source code for the page with the file upload element, I can see a left in comment with a URI path to a valid configuration file. The hunt is on!



-I downloaded the JSON file and opened it in my text editor. The challenge states that I need to have 4 terms of grades for my friend. The configuration file comes with two terms of grades. I copied and pasted one existing term's grades twice to create two new terms worth of grades. I changed the semesters of the new sections to "winter" and "summer" respectively. Then I changed some of the class names in the new terms. "Full Contact Linear Algebra" and "Theory of Theory" seem like classes my friend would take. My friend had a really rough year, so I changed all of his grades to **"A"** for each class. Then I changed the term gpa to **"4.00".** This is ***very*** important because the file **WILL NOT** be accepted if the ***letter grades*** and ***gpa*** don't match.





-I added in my friend's name, email, and I changed the "Production" field from false to true. These are all important pieces or else the file won't be accepted into production. With all these fields changed/added in, the third flag reveals itself on a successful file submission.

Flag: **WPI{3xP053D_C0NF1GUR4710N}**