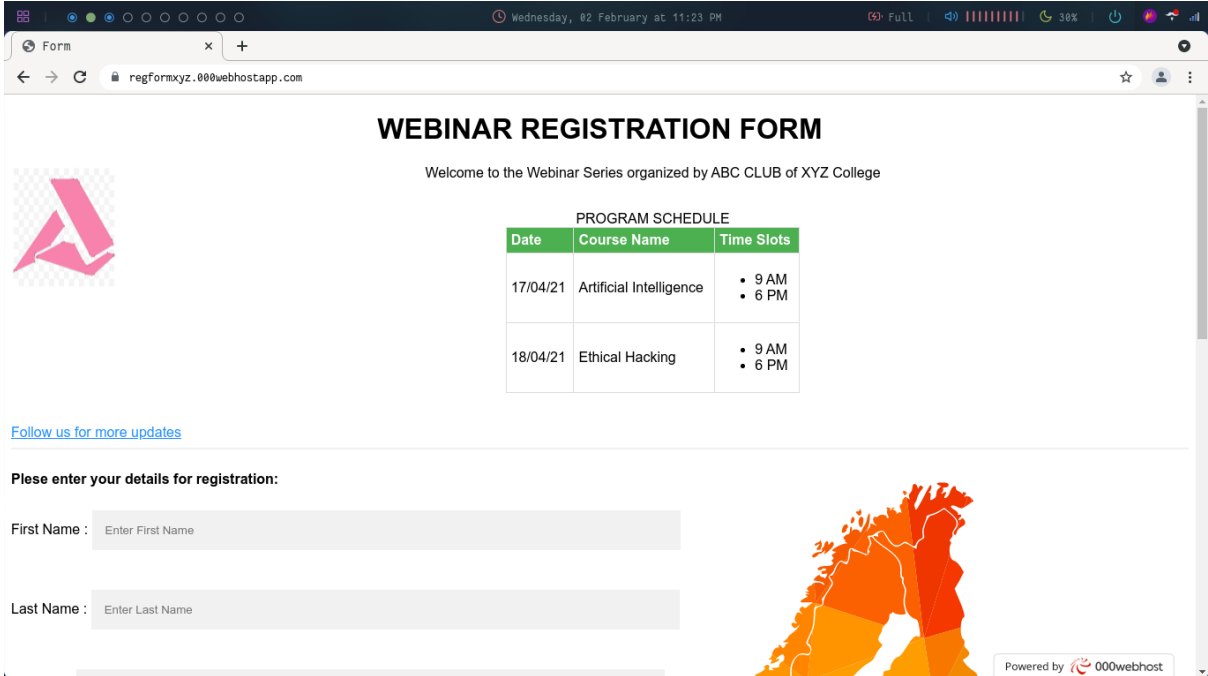


## HEY ELLIOT

This is a challenge which comes under the category of web exploitation. If we visit the link given below we reach this page:




Form

regformxyz.000webhostapp.com

### WEBINAR REGISTRATION FORM

Welcome to the Webinar Series organized by ABC CLUB of XYZ College




PROGRAM SCHEDULE		
Date	Course Name	Time Slots
17/04/21	Artificial Intelligence	<ul style="list-style-type: none"><li>• 9 AM</li><li>• 6 PM</li></ul>
18/04/21	Ethical Hacking	<ul style="list-style-type: none"><li>• 9 AM</li><li>• 6 PM</li></ul>


[Follow us for more updates](#)

Please enter your details for registration:

First Name :

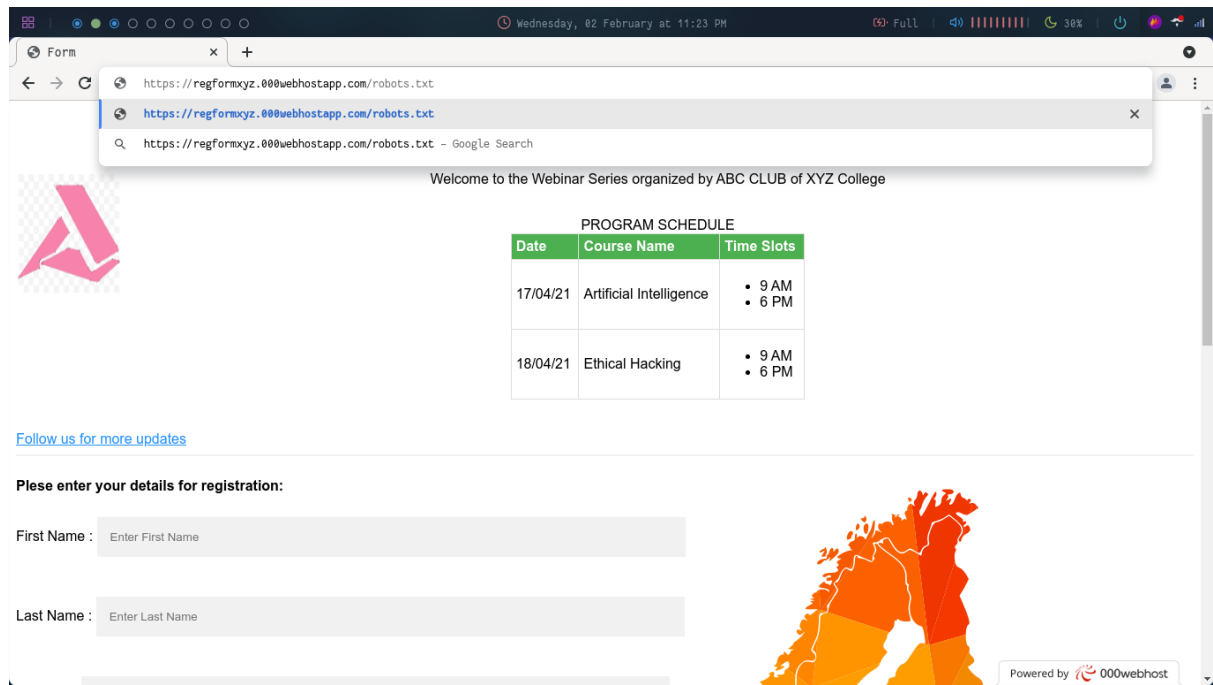
Last Name :



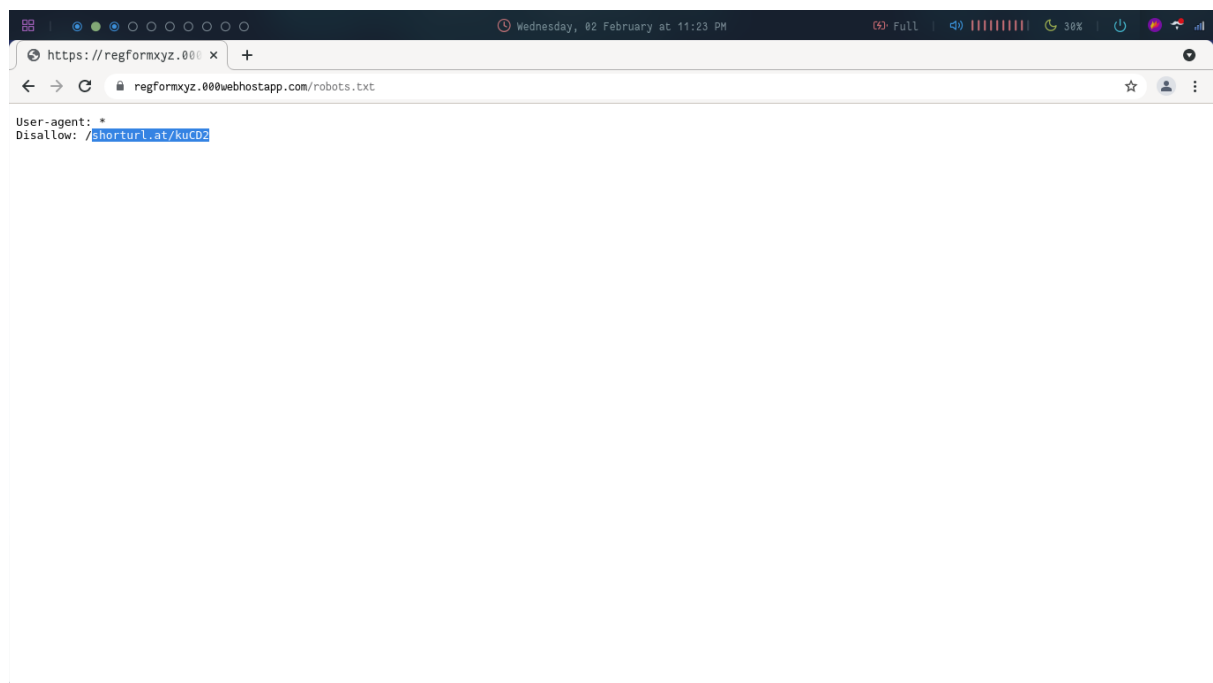
Powered by  000webhost

After inspecting the page we found nothing on index.html

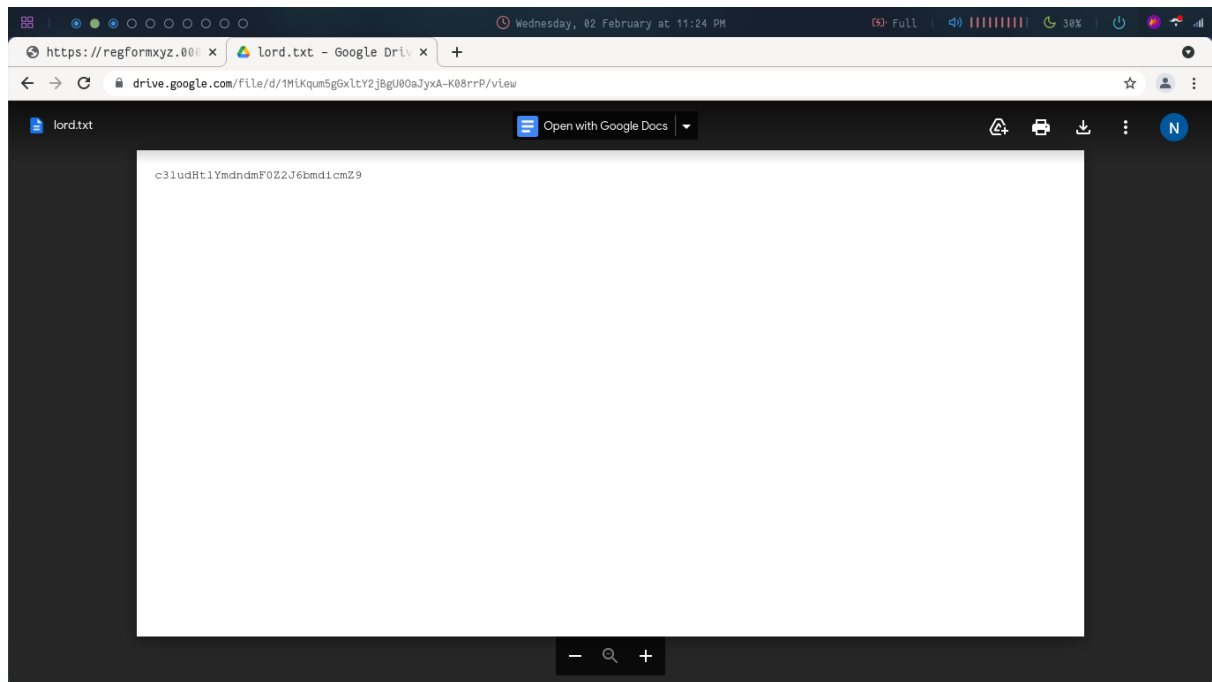
The next type of web exploitation questions come where there may be hidden directories/files (paths) inside the main URL (the most common being robots.txt). Hence on adding robots.txt to the given URL like so:



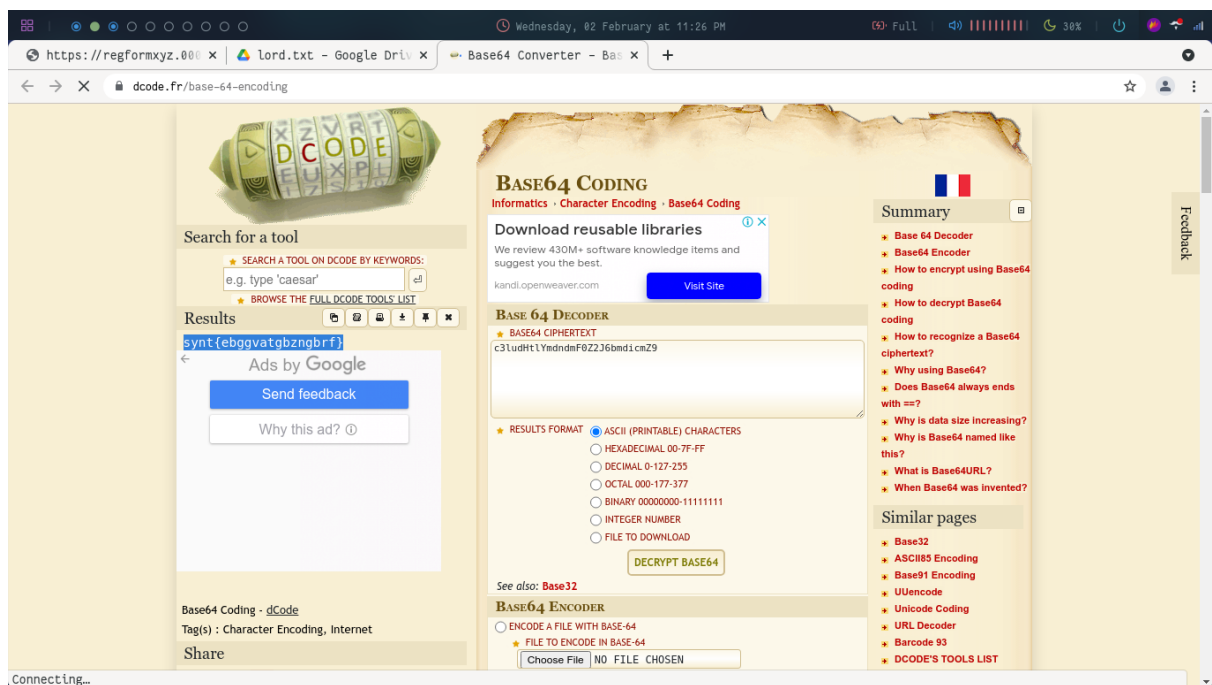
We get to the following page:



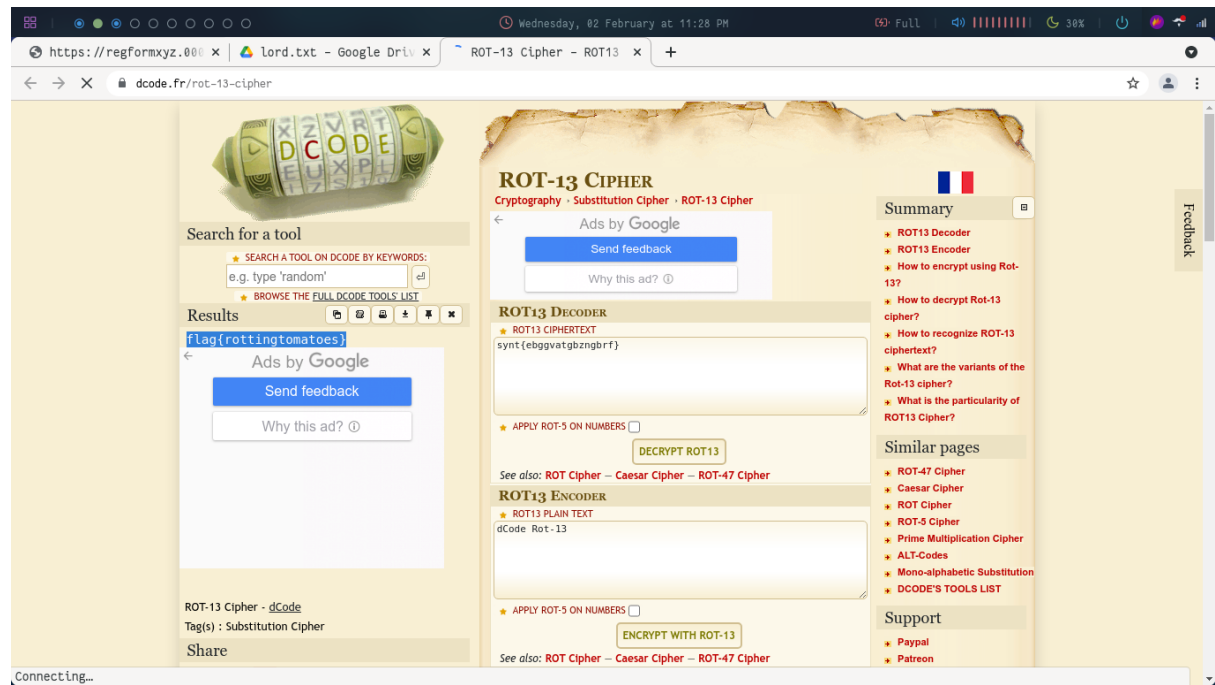
Visit the given link (next to Disallow). Don't include the '/' before the link as it'll search for those inside your computer. So on visiting the given URL you'll be taken to the following page:



Seems like a base64 so let's decode it:



The result (highlighted on the left) again seems to be a cipher. On checking it seems like it is a ROT13 cipher. Let's decode it again:



The result of that (highlighted on the left) is the required flag