# Cyber Tasks Completed

1. X frame/content header Vulnerabilities
   1. Added middleware and helmet to website
2. Input field limits on all forms
   1. Added maxlength attribute of 2500 characters to each input.
3. Login attempts on admin page
   1. Used Django Axes to implement a 1-minute lockout after 3 failed attempts
4. Switch login info, take it out from source code
   1. Moved login credentials into .env file, lets the owner choose secure credentials on deployment
5. Implement https
   1. Done by using a self cert and key in the hosting process
   2. Also use TLS 1.3 to prevent SSL stripping attacks
6. Manage.py vulnerabilities
   1. Added protections to prevent arbitrary code execution through sys.argv
   2. Added restrictions on who can execute management commands
7. Student could see mentor view through direct url
   1. Added an unauthorized page view and added authorization to each page

# Cyber Tasks Remaining

1. verify=False in authapp.py: This makes it so that when the backend authapp.py makes a GET request to one of our api endpoints (also backend), the authapp script doesn’t check the certificate to see if the response from the endpoint isn’t coming from an attacker. So an attacker can spoof our IP and return