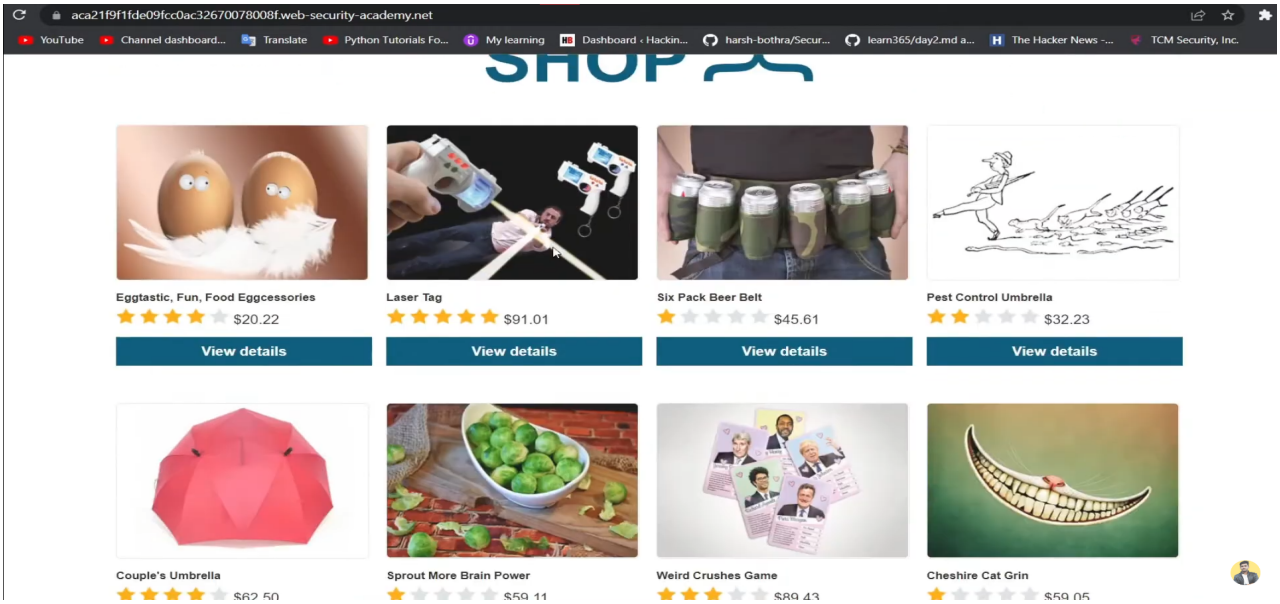
ASSIGNMENT – 1

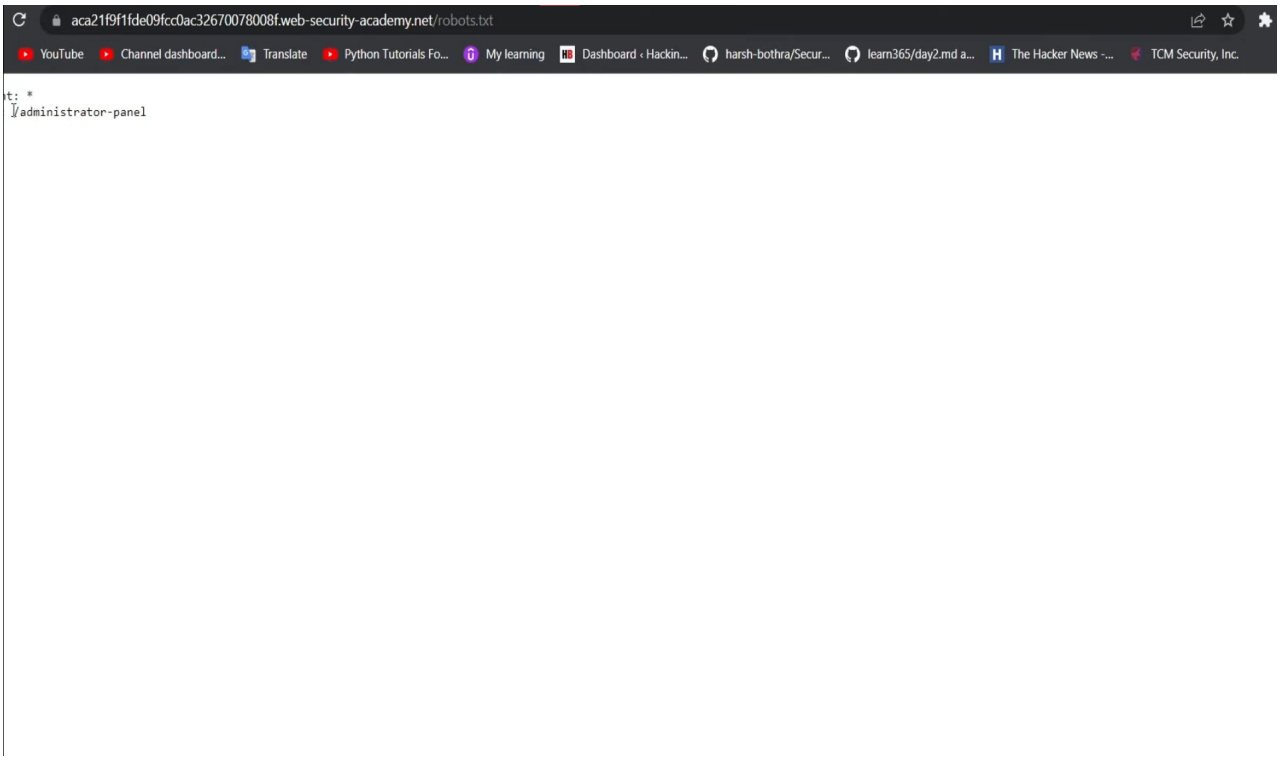
CHECKING THE TOP 5 CWE VULNERABILITIES 2021

Name: Harsh Pravin Gharlute

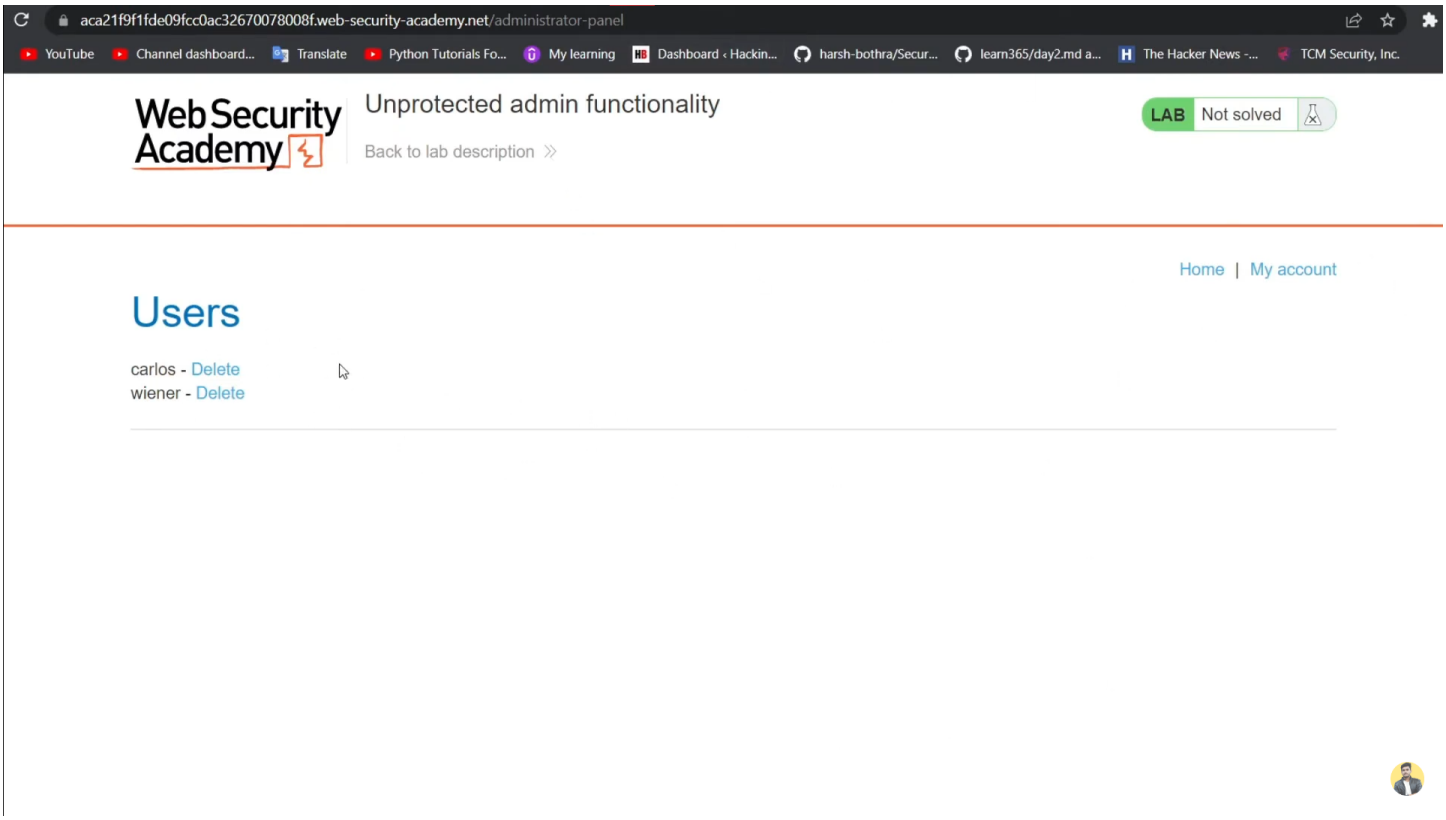
Email: harshpravin.gharlute2021@vitstudent.ac.in

BROKEN ACCESS CONTROL:





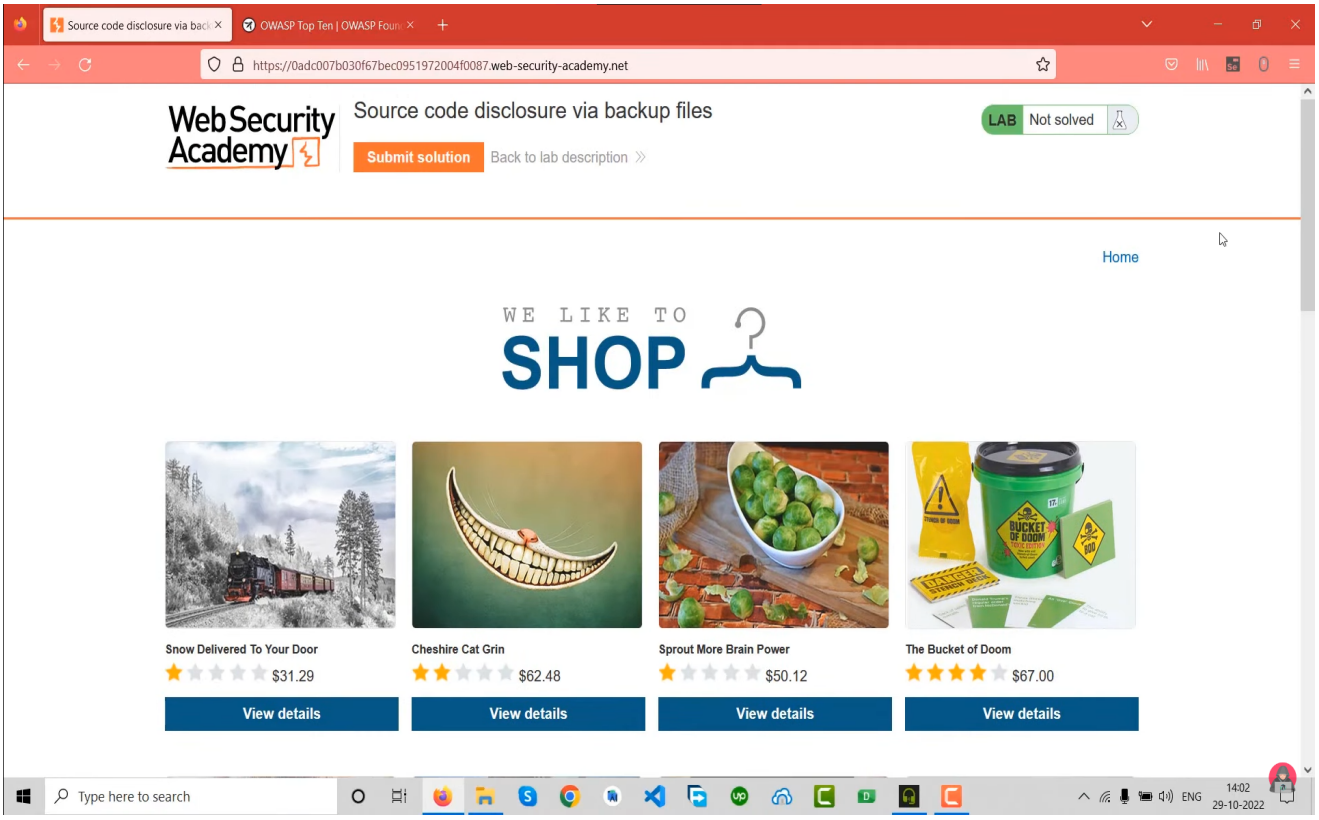
i.e., the site has a vulnerability of broken access control. Because we can use the Admin panel URL is given in the .txt URL



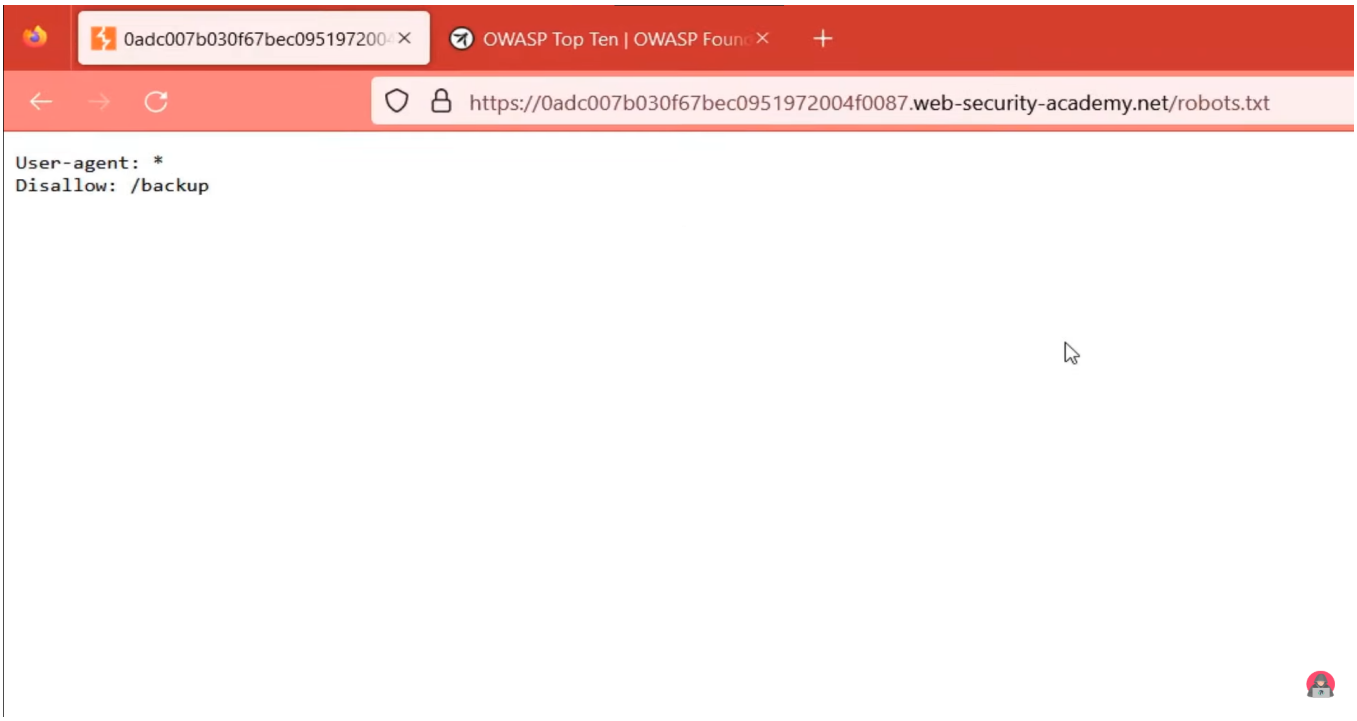
Therefore, this website has a broken access control vulnerability.

CRYPTOGRAPHIC FAILURES:

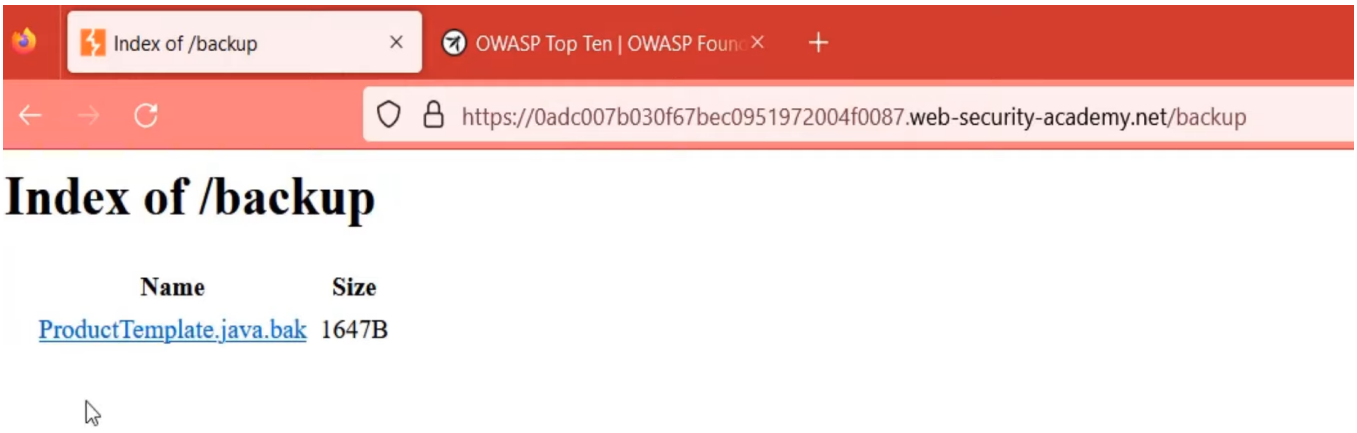
Visit a website.



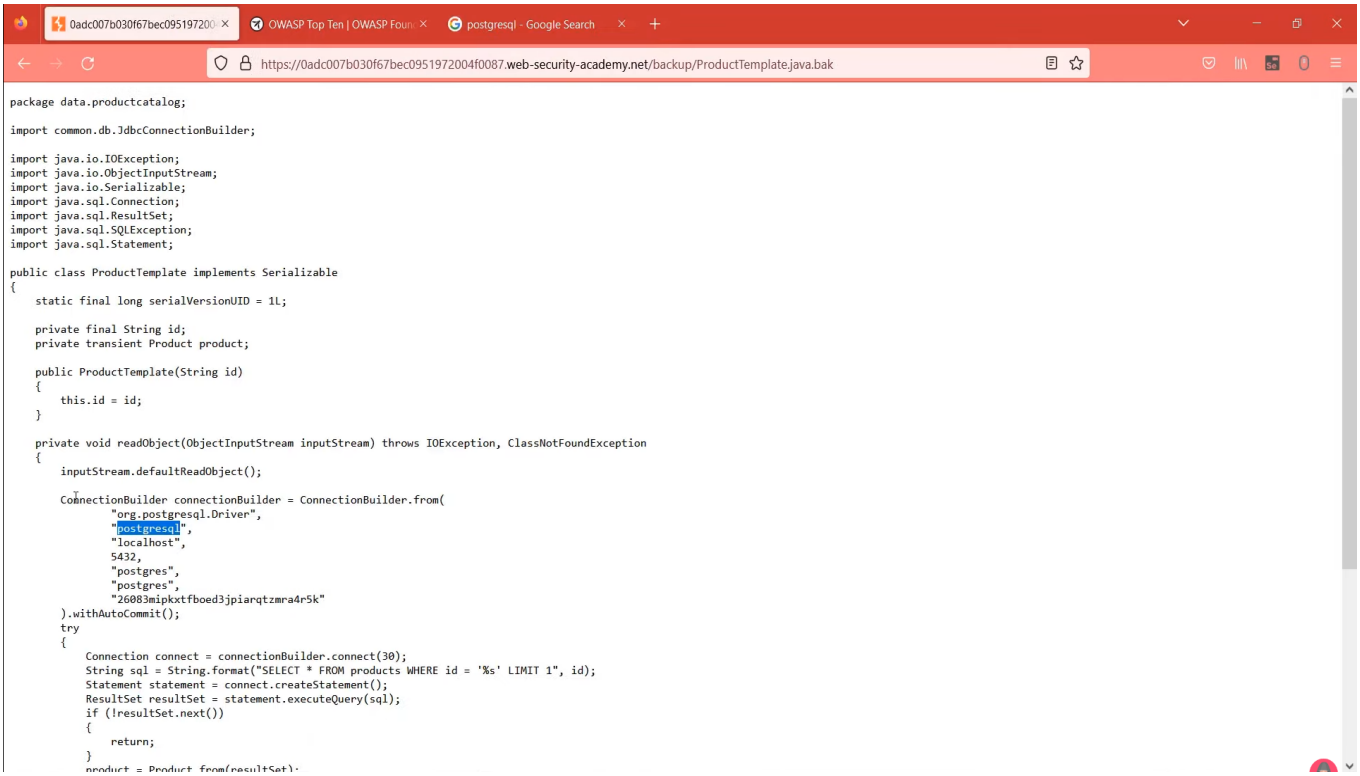
Change the URL of the website and add /robots.txt to find if there is some description.



We get a disallowed URL containing a link of backup file.



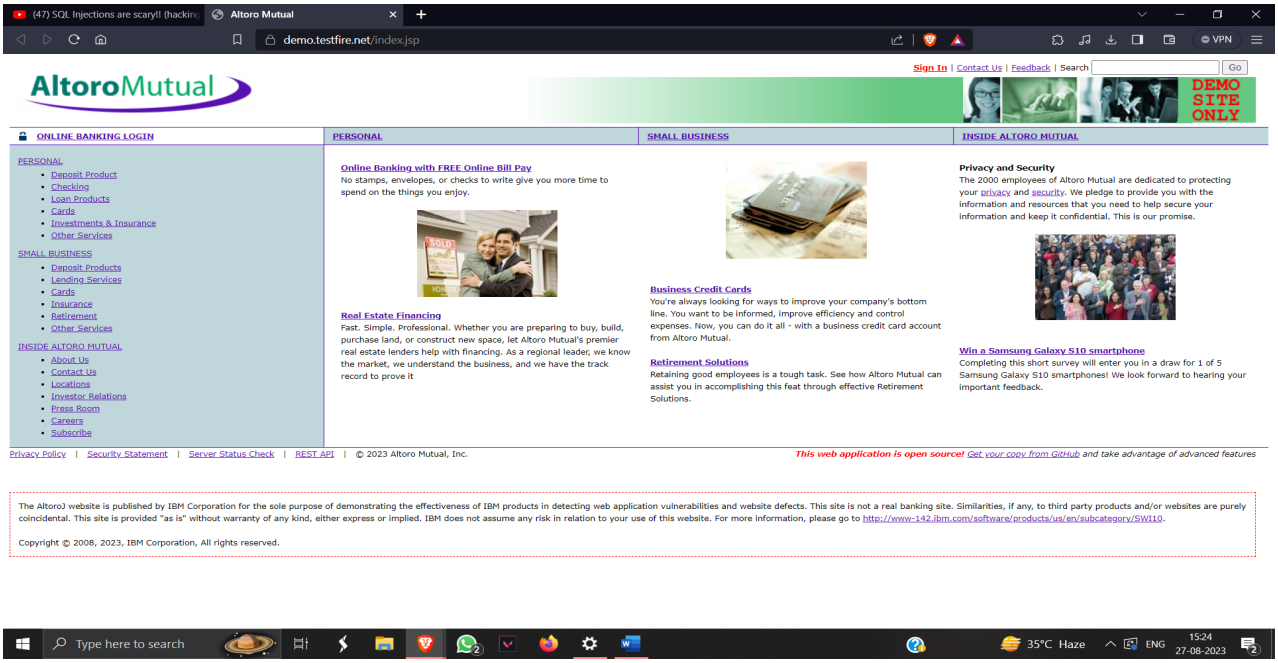
We use the URL in the SITE and get the decrypted password for the backup storage of website.



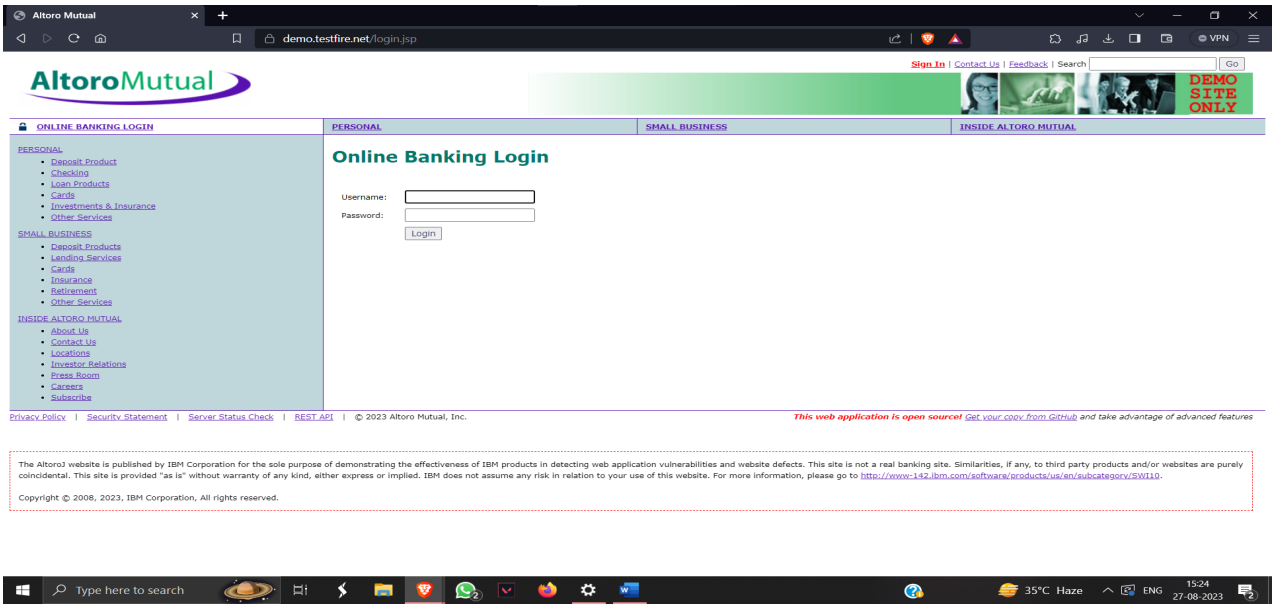
Therefore, we can say that the website has vulnerability in cryptographic failures as the password was not stored in encrypted manner.

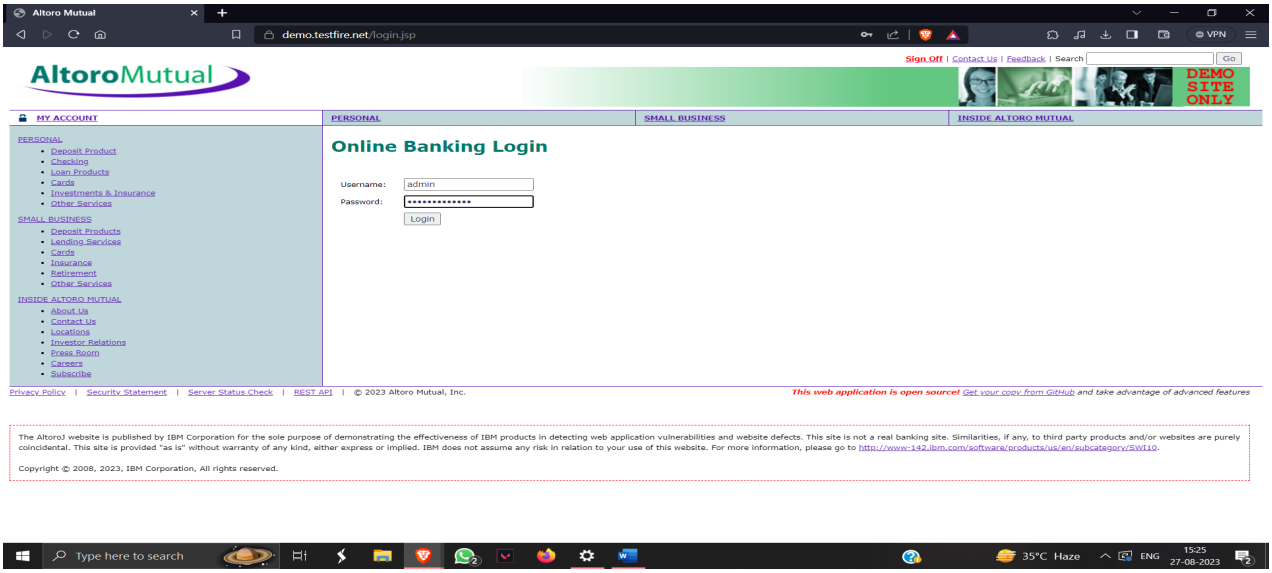
INJECTION:

Visit a website. E.g.AltotoMutual

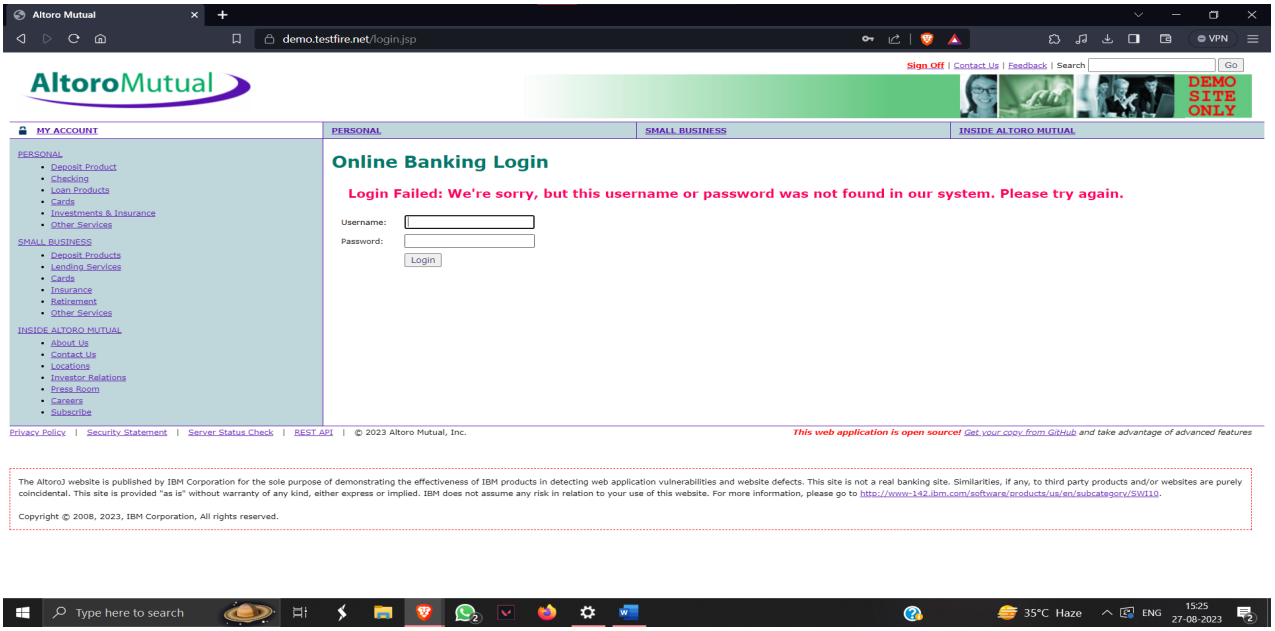


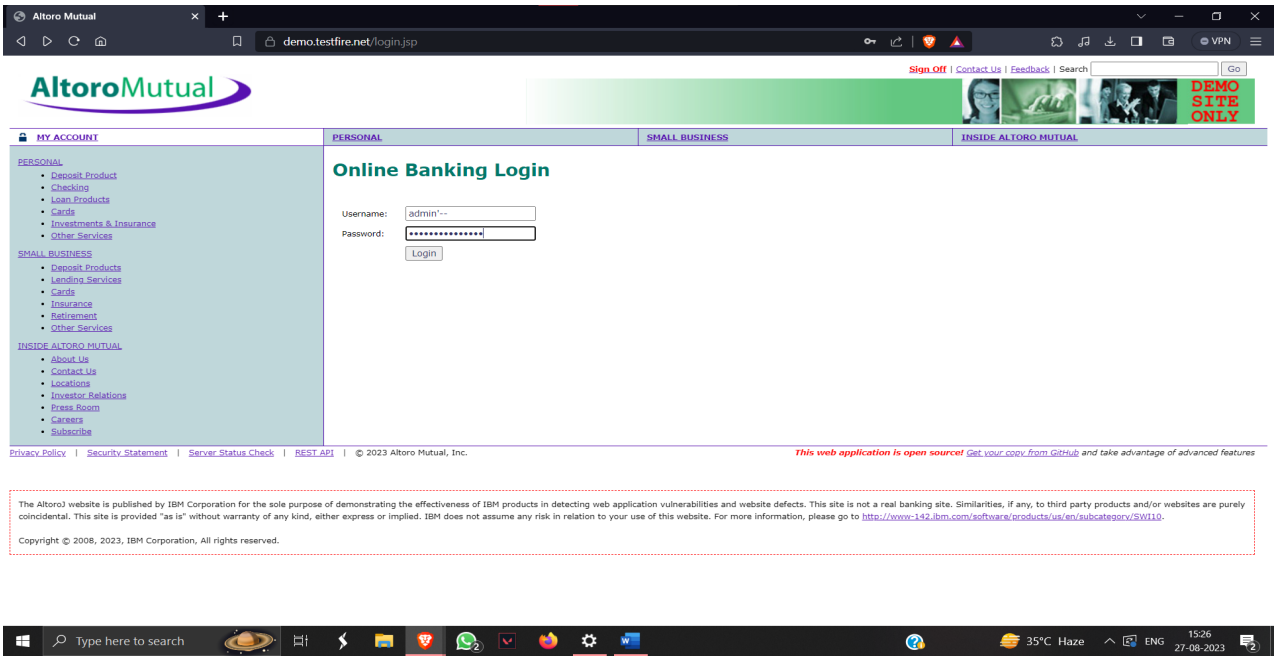
Go to the log in page:



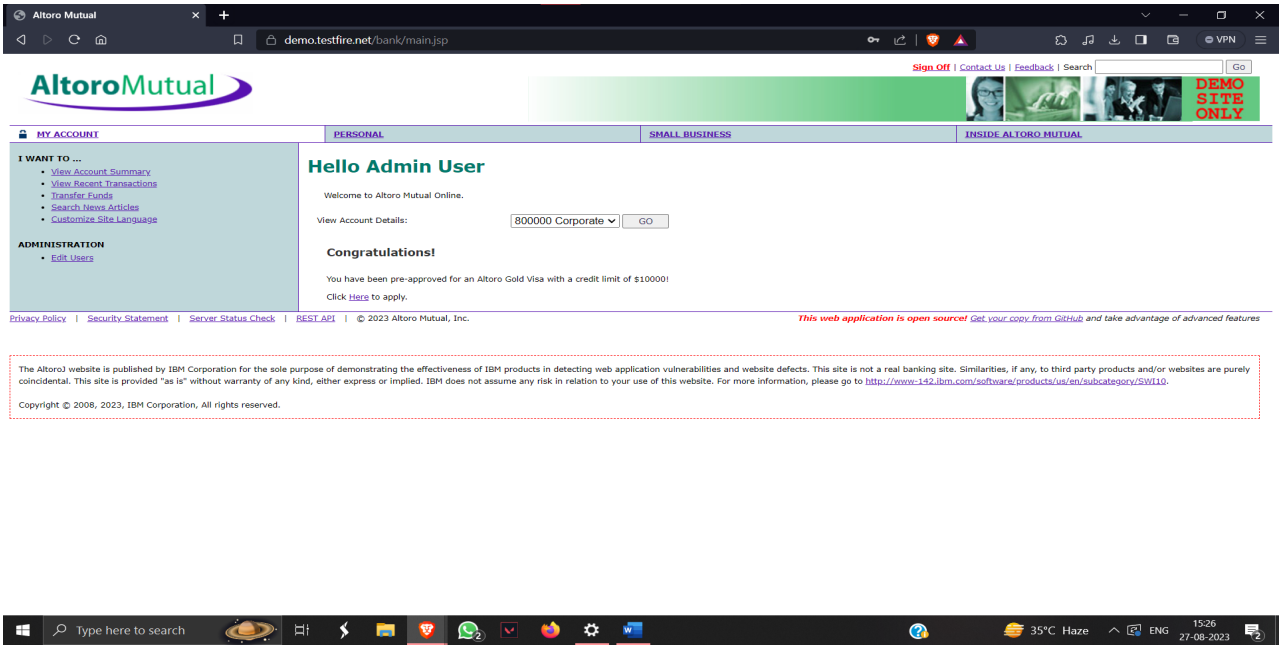


We get error saying wrong username and password.





We successfully log in!!



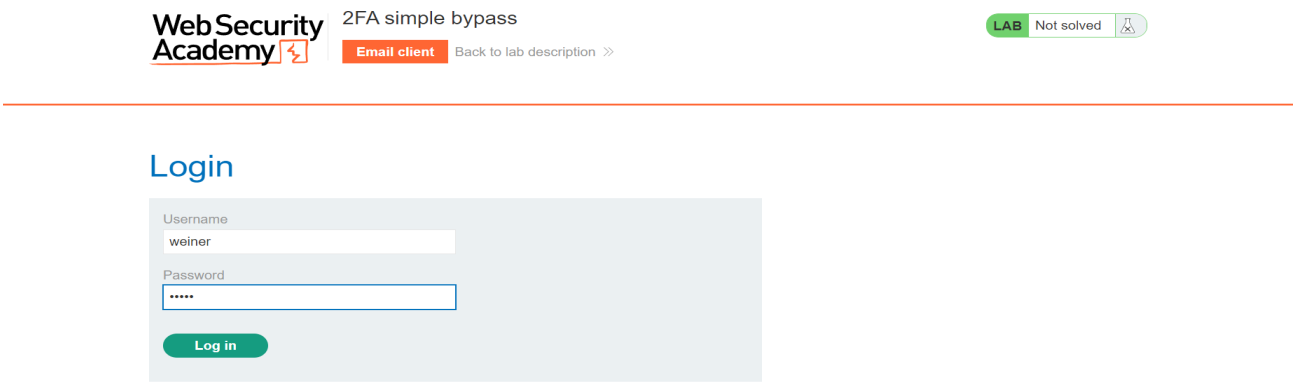
Therefore, this website has SQL injection vulnerabilities.

INSECURE DESIGN:

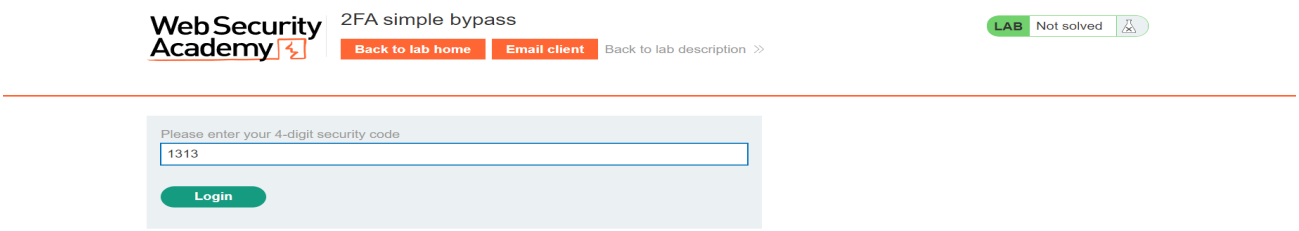
SECURITY MISCONFIGURATION:

We got to a Blog wesbiste:

LOG IN USING THE GIVEN CREDENTIALS:

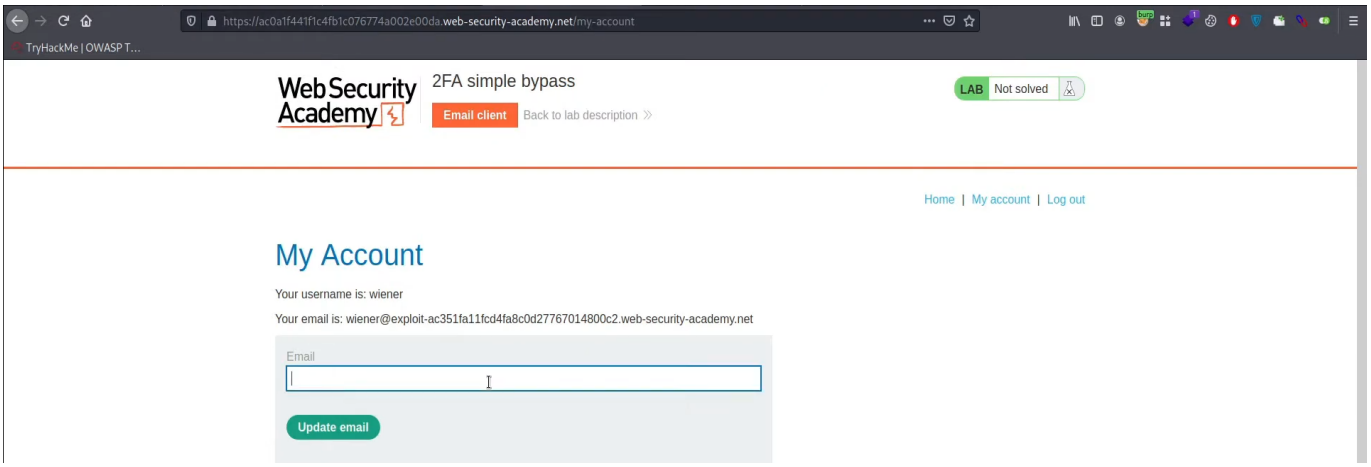


Enter the OTP given in the email:

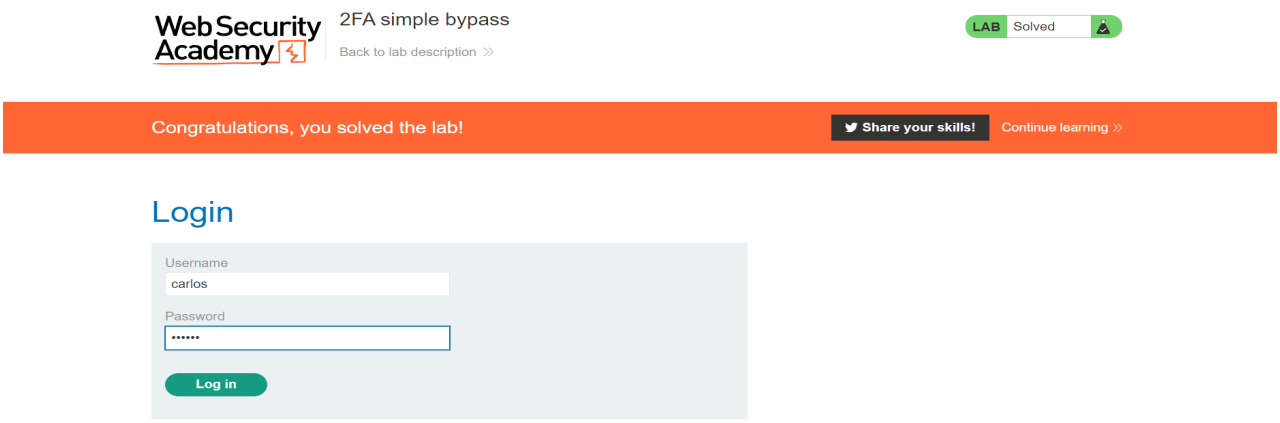


We logged in successfully.

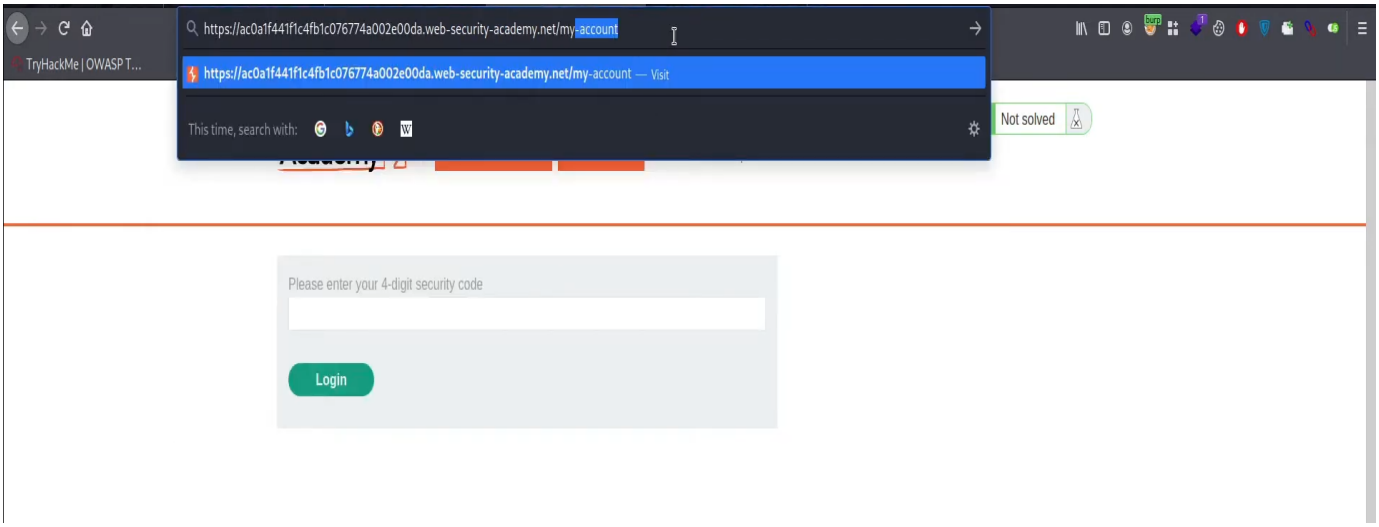
Now we notice the URL of the logged in account.



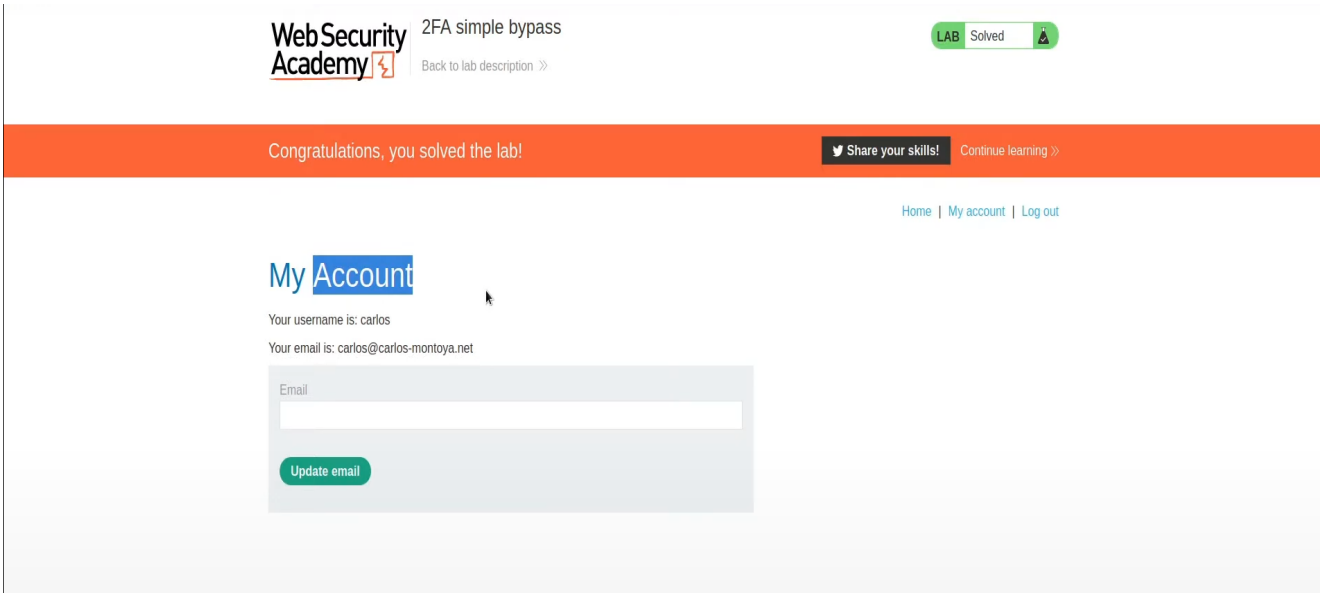
Now we log in with victim's credentials,



we change the URL to the same URL of that of the logged in account.



WE LOG IN SUCCESSFULLY !!!



Therefore, this website has Security misconfiguration vulnerability.