

Name : Challenge 1

Domain :Information Disclosure

Author: Rushi Balapure

Description :

When a site makes delicate and sensitive data available to guests , it is termed as information disclosure.

This can be intentional or unintentional and can lead to identity theft, fraud, or even reputational damage.

Information disclosure might result in leaking of login credentials or sensitive information.

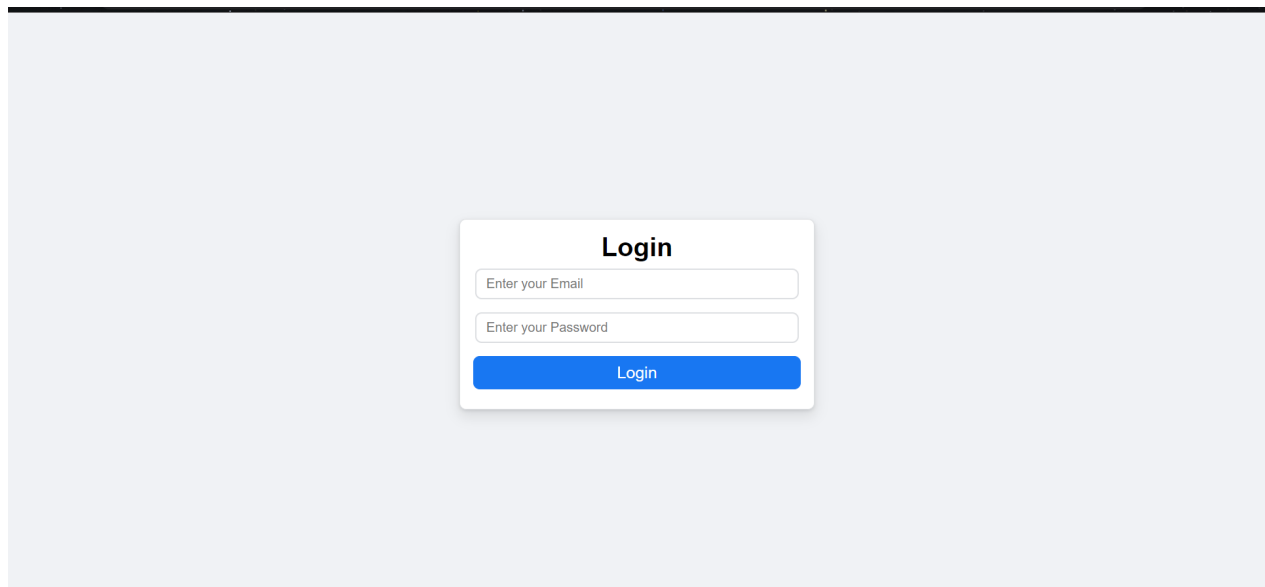
How does information disclosure vulnerabilities arise?

- 1) Failure to remove internal content from public content.
- 2) Insecure configuration of the website and related technologies.
- 3) Flawed design and behaviour of the application.

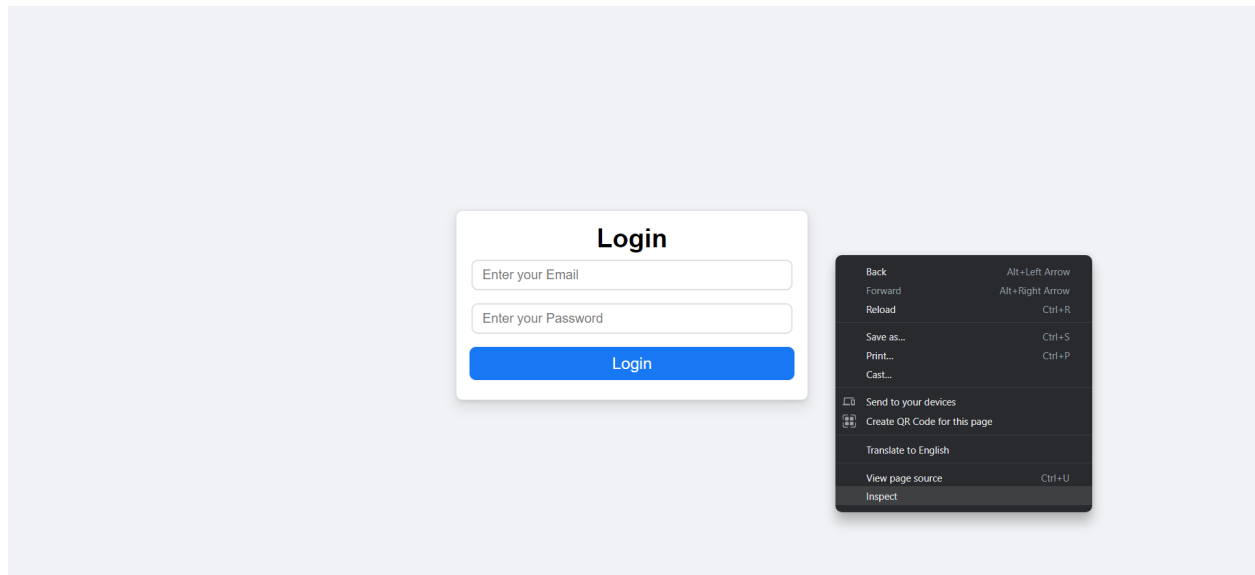
Files Given: website : <https://minictf-challenge1.netlify.app/>

Writeup:

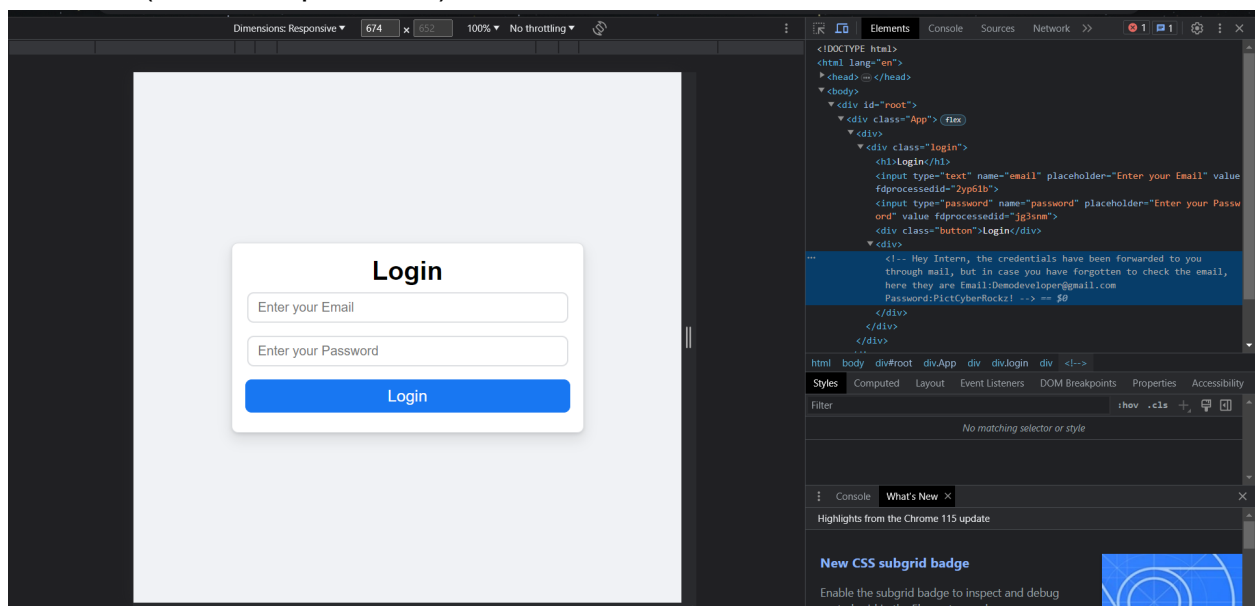
Visit the given link,Login Page will open.



Right click on the page and select inspect option



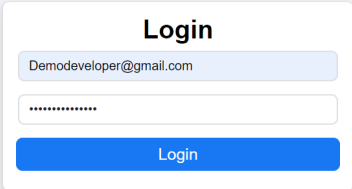
After selecting inspect option,go through the code.Text (comment) contain the login credential(email and password) for the website.



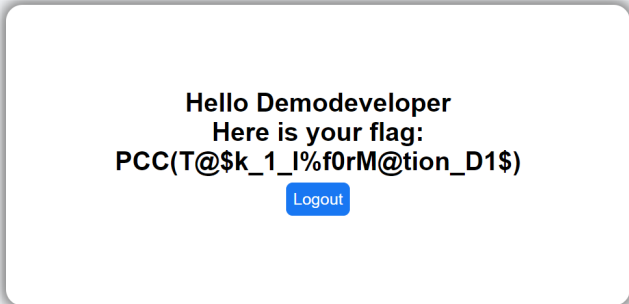
Enter the login credential.

Email: Demodeveloper@gmail.com

Password: PictCyberRockz!

A login form titled "Login" is centered on a light gray background. The form has a white background and a subtle shadow. It contains two input fields: the first is for the email address, which already contains "Demodeveloper@gmail.com", and the second is for the password, which is masked with "*****". Below the input fields is a blue button with the text "Login" in white.

After successful login, a message with the flag will be displayed

A white message box with rounded corners and a subtle shadow is centered on a light gray background. The box contains the following text: "Hello Demodeveloper", "Here is your flag:", and "PCC(T@\$k_1_I%f0rM@tion_D1\$)". Below the text is a small blue button with the text "Logout" in white.

Flag is: PCC(T@\$k_1_I%f0rM@tion_D1\$)