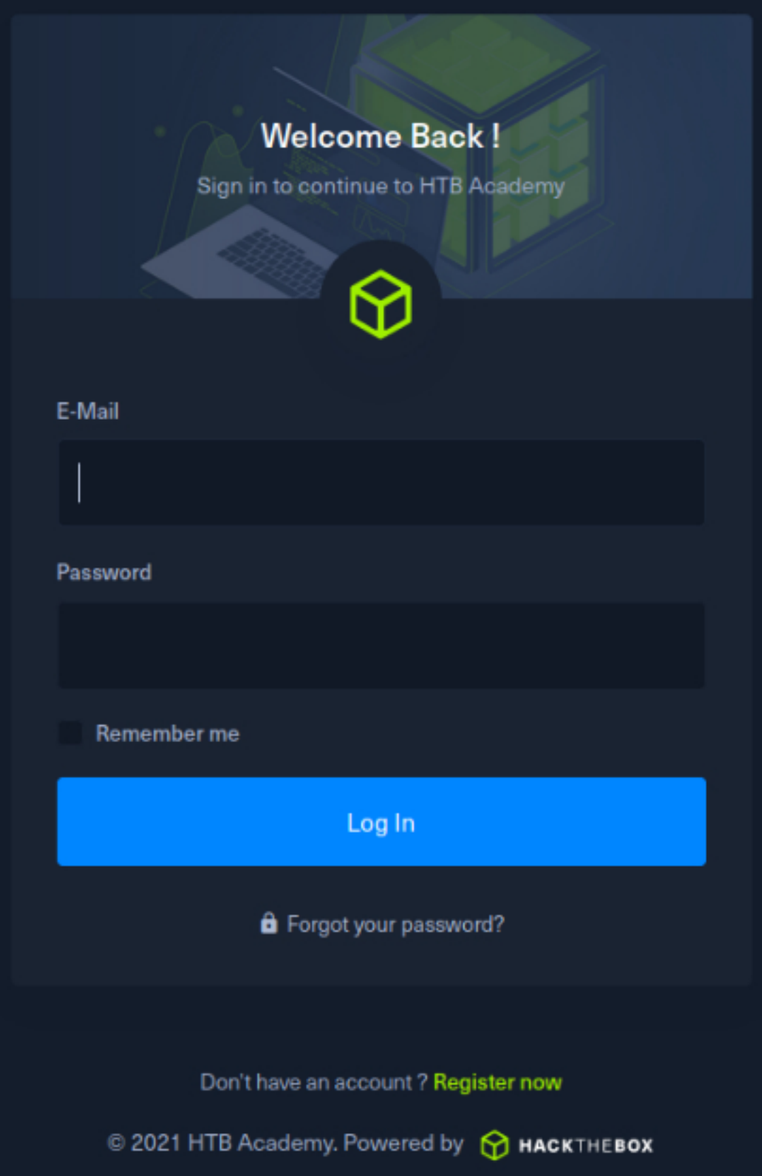
What is Authentication

Authentication is defined as `the act of proving an assertion`. In this module's context, which revolves around application security, authentication could be defined as the process of determining if an entity (a user or an automated application) is who it claims to be.

The most widespread authentication method used in web applications is `login forms`, where a user enters their username and password to prove their identity. Login forms can be found on websites such as HTB Academy and Hack the Box to email providers such as Gmail, online banking, members rewards sites, and the vast majority of websites that offer some service. On HTB Academy, the login form looks like this:



Authentication is probably the most widespread security measure, and it is the first line of defense against unauthorized access. While it is commonly referred to and shortened as "`auth`," this short version is misleading because it could be confused with another essential security concept, `Authorization`.

Authorization is defined as `the process of approving or disapproving a request from a given (authenticated) entity`. This module will not cover authorization in-depth. Understanding the difference between the two security concepts is vital to approach this module with the right mindset.

Assume that we have encountered a login form while performing a penetration test for our Inlanefreight customer. Nowadays, most companies offer certain services for which their customers have to register and authenticate.

Our goal as third-party assessors is to verify if these login forms are implemented securely and if we can bypass them to gain unauthorized access. There are many different methods and procedures to test login forms. We will discuss the most effective of them in detail throughout this module.

Next ➜ Mark Complete & Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left