

API Rate Limiting

Background

API rate limiting is an important mechanism to control the number of requests coming from clients within a specified time window. DDoS attacks can cause critical issues, especially if an API call triggers a Python program on the computer, potentially exhausting resources. By setting up API rate limiting, we can prevent DDoS attacks and abuse in a short period, ensuring fair usage of resources among all users.


Action items

- ☒ Install required requirements to implement API rate limiting
- ☒ Implement rate limiting for the `login` endpoint.

Decisions

-  Set up the maximum attempts within in a time window

Demonstration

 Login failed: Too many requests, please try again later. 