Cyber Sapiens Internship Task 16

No Rate Limit

What is Rate Limit?

Rate limiting is a strategy for limiting network traffic. It puts a cap on how often someone can repeat an action within a certain timeframe – for instance, trying to log in to an account. Rate limiting can help stop certain kinds of malicious bot activity. It can also reduce strain on web servers. However, rate limiting is not a complete solution for managing bot activity.

How does Rate Limiting work?

Rate limiting runs within an application, rather than running on the web server itself. Typically, rate limiting is based on tracking the IP addresses that requests are coming from, and tracking how much time elapses between each request. The IP address is the main way an application identifies who or what is making the request.

A rate limiting solution measures the amount of time between each request from each IP address, and also measures the number of requests within a specified timeframe. If there are too many requests from a single IP within the given timeframe, the rate limiting solution will not fulfill the IP address's requests for a certain amount of time.

Essentially, a rate-limited application will say, "Hey, slow down," to unique users that are making requests at a rapid rate. This is comparable to a police officer who pulls over a driver for exceeding the road's speed limit, or to a parent who tells their child not to eat so much candy in such a short span of time.

What is No Rate Limit?

Rate limiting is a process to limit requests possible. It is used to control network traffic. Suppose a web server allows upto 20 requests per minute. If you try to send more than 20 requests, an error will be triggered. This is necessary to prevent the attackers from sending excessive requests to the server.

What is the impact and mitigation?

Impact :

Let’s take an OTP situation. Now suppose, the length of otp is 3 digits and an attacker is guessing the otp for successful transaction theft. If no rate limiting is implemented in the web application, the hacker can manually type 000-999 values on otp to check which one is correct. This method is a little bit cumbersome, so the hacker can use a burp suite tool to do the same job in less time.Hence, after 30min, the otp gets unlocked and the attack is successful.

Now, in the same scenario, if rate limiting was implemented in a web application, suppose allow only 5 attempts or a time limit of 2 minutes. In this case, it’s almost impossible for the hacker to crack the otp . Thus,preventing the attack from happening.

Mitigation :

- Monitoring API activity against your rate limit.
- Catching errors caused by rate limiting.
- Reducing the number of requests.
- Extra precautions are taken with login, otp, vouchers etc.

References :

https://www.geeksforgeeks.org/no-rate-limiting-flaw-in-cyber-security/#:~:text=No%20rate%20limit%20is%20a,gets%20suspended%20for%20some%20hours.