Muhamad Hidayat Follow
Jul 4, 2022 · 4 min read

Save

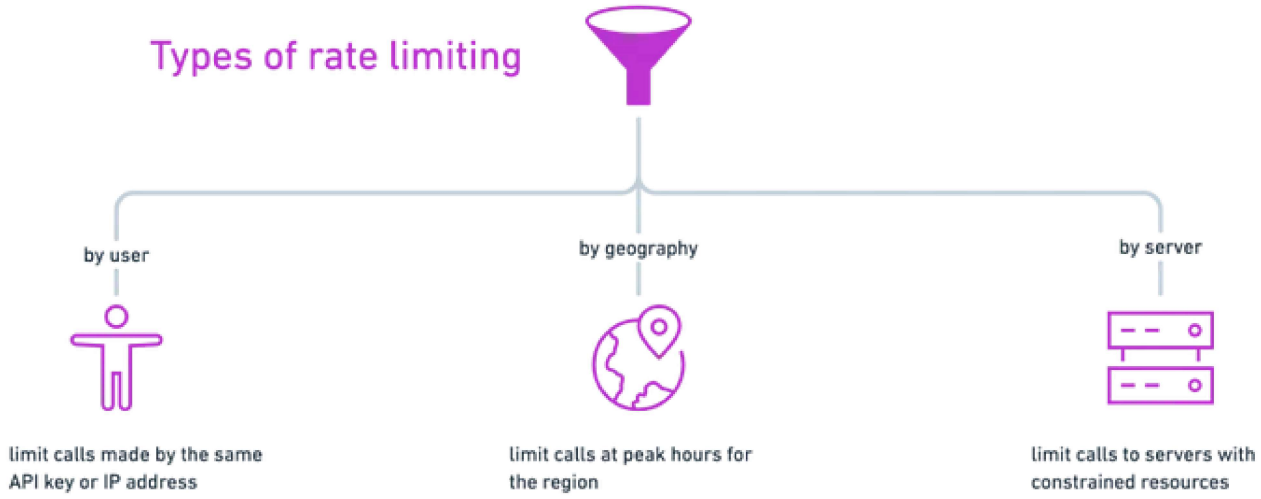
OWASP API Security (Offensive Prespective) : Lack of Resource & Rate Limiting #4

Go 언어 — 속도 제한 (Rate Limiting) (velog.io)

Assalamualaikum Wr. Wb

Rate Limit adalah sebuah pembatasan pengiriman sebuah request, yang berarti backend akan membatasi pengiriman request bertubi-tubi yang akan menggangu, serta mencegah adanya bot pada aplikasi.

Ketika melakukan konfigurasi rate limit pada sebuah api, terdapat beberapa varian metode dan parameter, rate limit tergantung dari konfigurasi seperti apa yang kita inginkan, pembatasan seperti apa yang ingin kita buat, diketahui terdapat 3 tipe ratelimit yang di kategorikan oleh **KeyCDN**.



API rate limiting with Node and Redis — DEV Community

User rate limiting, sebuah pola rate limit yang sering digunakan di banyak API. Pola tersebut dibentuk untuk membatasi request / penggunaan api untuk pengguna dalam batas penggunaan tertentu. Request akan tertolak jika telah melibihi batas penggunaan tersebut, Akan bisa digunakan kembali apabila kurun waktu tertentu, ratelimit akan ter-reset kembali.

Geographic rate limiting, sebuah pola rate limit untuk lebih meningkatkan keamanan di wilayah geografis tertentu, seperti penerapan rate limit akan nonaktif di waktu dimana pengguna sedang di waktu yang tidak begitu aktif seperti tengah malah sampai jam 7 pagi , untuk mereduksi ancaman, serta aktifitas mencurigakan.

Server rate limiting, Sebuah pola rate limit yang menggunakan cara menurunkan limit sebuah trafik berbasis level pada server, seperti menurunkan trafik limit pada server A, lalu meningkatkan limit pada server B (server yang sering digunakan).

Bagaimana Rate Limit Bekerja??

Rate Limit bekerja didalam sebuah aplikasi, ketimbang pada web servernya. pengidentifikasian rate limit bisa berdasarkan identitas user seperti email,userid, username, ada juga berbasis ip address serta user-agent. gunanya untuk menidentifikasi dari mana request berasal dan emncari tau rentang waktu pengiriman antara satu request dengan request selanjutnya.

Rate Limit digunakan untuk menghandle issue mengenai rentang waktu tiap request di tiap Identifier dan juga menghandle terkait jumlah request di tiap rentang waktu tertentu. Jika request yang dikirim dari tiap identifier melebihi

rentang waktu yang ditentukan maka Rate Limit tidak akan memproses request tersebut.

Rate limit seperti hal nya dokter yang melarang kita memakan obat lebih cepat dari interval waktu yang ditentukan. Kita diberikan obat demam untuk dimakan 2x sehari, tiap obat yang dikonsumsi untuk mengkonsumsi obat ke 2 terdapat interval waktu 5 jam untuk menurunkan kadar darah, lalu agar dapat meminum obat kembali. jika kita mencoba meminumnya dokter/orang tua akan mengambil paksa hak kita untuk meminum obat saat itu, dan kita tidak bisa meminum obat tersebut sementara waktu.

Aktivitas yang dicegah oleh Rate Limit?

Rate limit mencegah bot dengan kecenderungan buruk atau perilaku buruk yang akan memiliki dampak pada aplikasi, serangan tersebut bisa berupa:

- Brute Force Attack
- DoS dan DDOS Attackts
- Web Scrapping

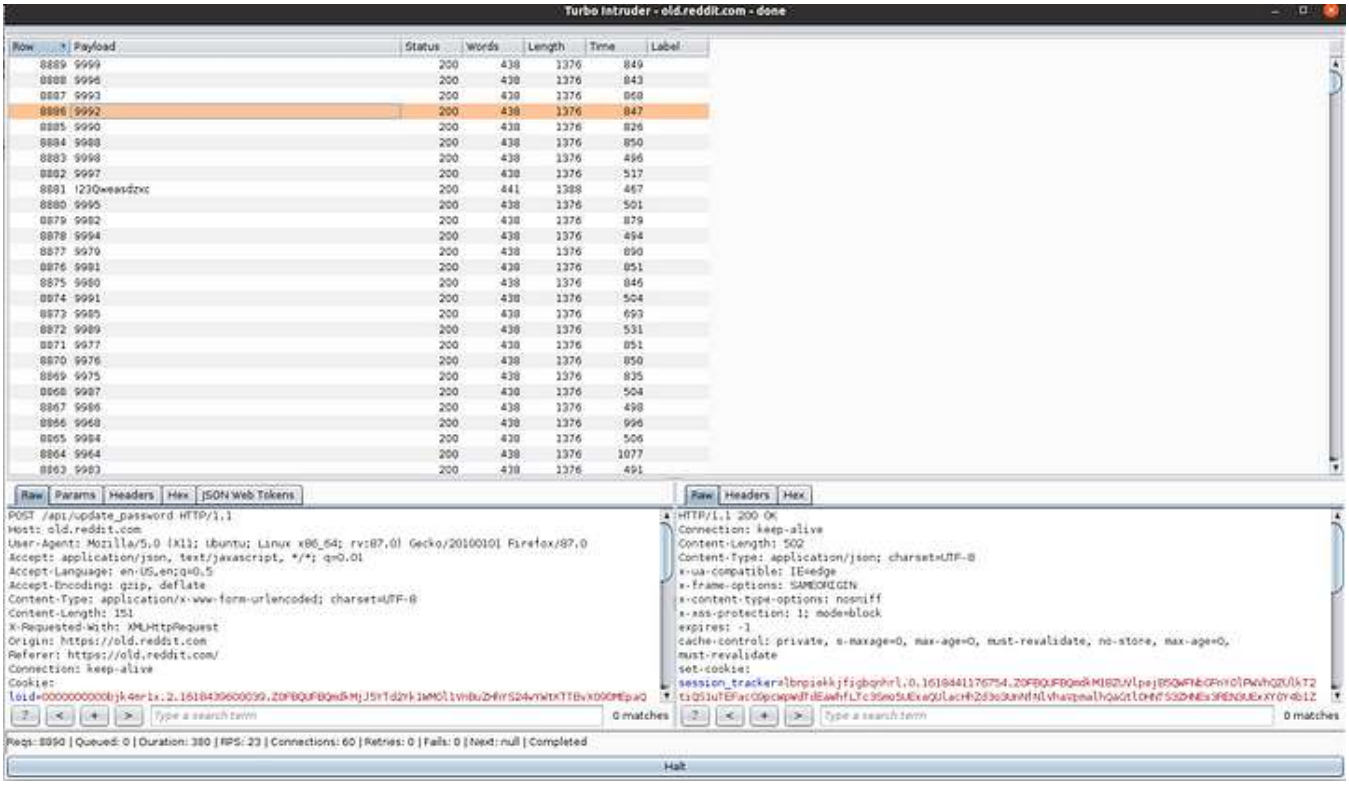
Apa itu Lack of Resource & Rate Limiting

Kerentanan yang disebabkan karna tidak adanya rate limit yang diterapkan pada aplikasi, yang dapat mengakibatkan gangguan pada aplikasi atau server oleh attacker yang melakukan request dalam jumlah besar dalam waktu singkat, yang dimana server atau aplikasi tidak dapat menampung keseluruhan request tersebut, dapat juga mengakibatkan resiko percobaan bruteforcing attack.

Variasi Tehnik Serangan

- BruteForcing Attack
- DoS / DDoS Attack
- Web Scrapping

Brute Forcing Attack — #1165285 No Rate limit on change password leads to account takeover (hackerone.com)



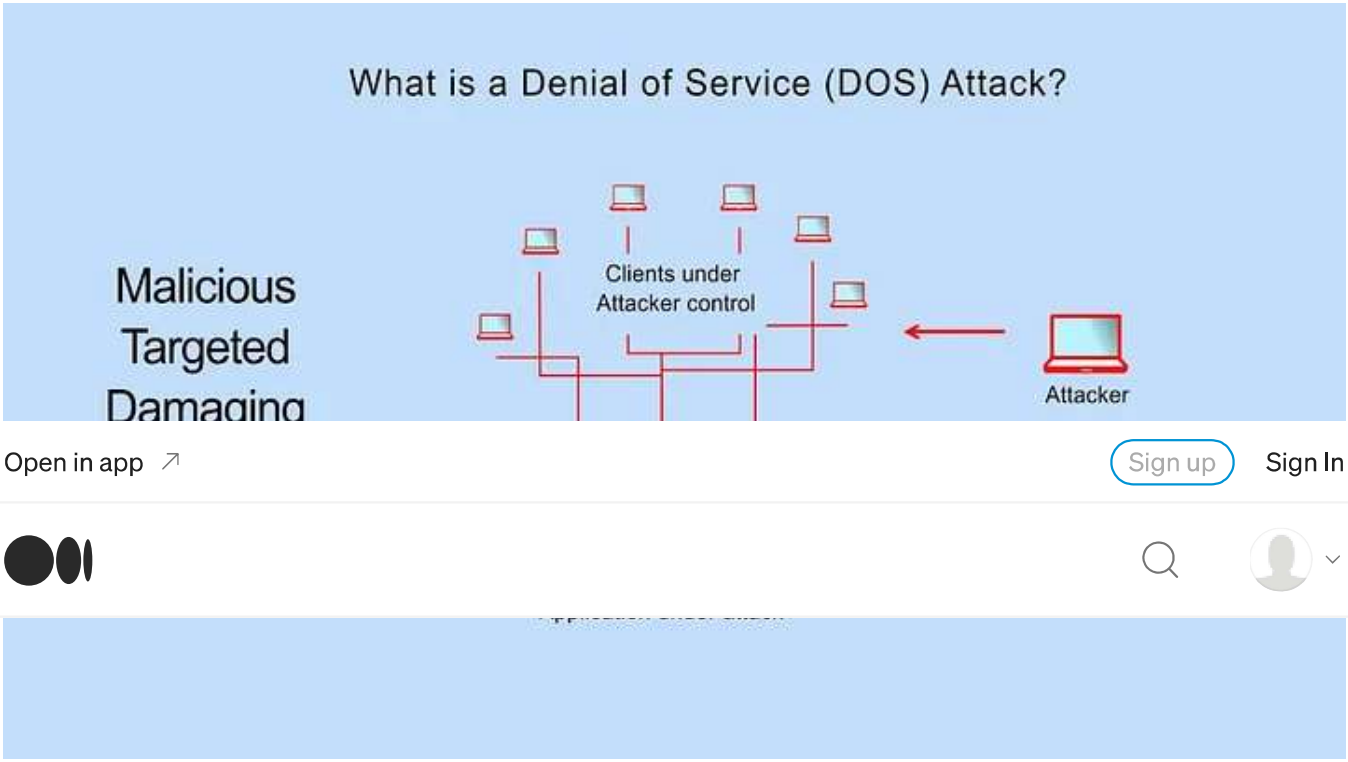
Brute Forcing attack adalah tehnik penyerangan yang dilakukan dengan cara generating angka / wordlist yang nantinya akan digunakan untuk menebak pin / code / password.

Pada kasus ini attacker mencoba melakukan brute forcing attack pada sistem OTP, untuk melakukan pergantian password, sebelum pergantian password aplikasi

melakukan autentikasi terlebih dahulu dengan cara melakukan verifikasi OTP. Kode OTP yang akan dikirimkan ke devices atau email nantinya akan diinputkan kembali pada kolom verifikasi kode OTP sebelum pergantian password.

Seperti yang terlihat pada gambar, attacker mencoba menebak 4 angka code OTP yang dikirimkan ke device atau email korban, dan Attacker dapat melakukan pergantian password.

DoS (Denial of Services) — #223542 Abuse of Api that causes spamming users and possible DOS due to missing rate limit on contact form (hackerone.com)



Mitigating Application-level DoS attacks with LoadMaster® | France (kemptechnologies.com)

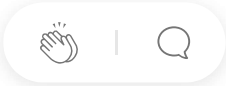
DoS adalah salah satu bug terkait dengan lack of resource. Serangan DoS terjadi ketika user mencoba untuk memperlambat / mematikan service aplikasi secara total. bisa dengan cara melakukan flooding request API.

Pada kasus ini attacker mencoba melakukan flooding pada endpoint API, memanfaatkan ketiadaan rate limit yang berlaku pada aplikasi tersebut.

Bagaimana Cara Pencegahanya?

- **Token Bucket**, menggunakan limitasi token request dengan rentang waktu tertentu.
- **Leaky Bucket,** Melakukan storing request pada jumlah tertentu, sampai bucket tersebut sudah mencapai batas maksimal, maka request selanjutnya akan tertolak, lalu request yg sudah di simpan tadi, dileatakan pada sebuah antrian data, yg nanti nya 1 per 1 akan di proses.
  tujuanya agar sebanyak apapun request yg masuk nanti nya, akan tetap di tampung tapi dalam batas tertentu, dan masuk antrian.
- **Rate limit implementation**
- **Captcha**

Lebih kurangnya mohon maaf, semoga bermanfaat.
wassalam



Rate Limiting Owasp Top 10 Owasp Api Security Top 10 Exploitation Hacking