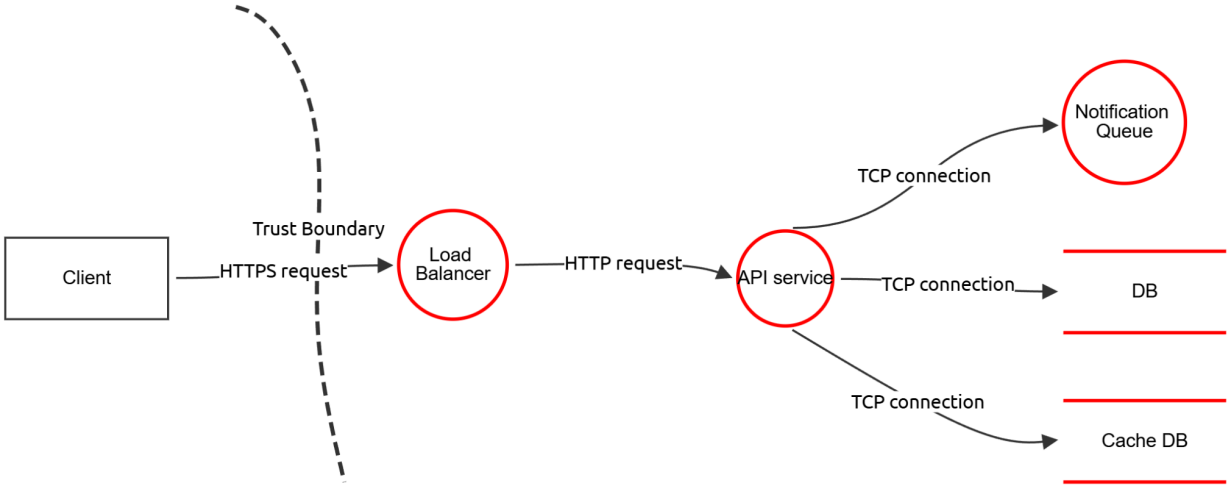
For the Threat Model we have used OWASP Threat Dragon.

Threat Model diagram with 5 flows:



We have got 16 threads:

Id	Type	Description	Mitigations	Score	Severity
1	Tampering	Using speed to violate explicit or implicit assumptions about the application's normal use to achieve unfair individual gain	Defences include providing enforcement of behavioral workflow and anti-automation	7	High
2	Informati…	Using speed to violate explicit or implicit assumptions about the application's normal use to achieve unfair individual gain	Defence includes providing anti-automation	3	Low
3	Elevation …	Usage may resemble legitimate application usage but leads to exhaustion of resources	Mitigation or prevention such as providing backoff, resource management and avoiding forced deadlock	8	High
4	Tampering	Using speed to violate explicit or implicit assumptions about the application's normal use to achieve unfair individual gain	Defences include providing enforcement of behavioral workflow and anti-automation	9	Crit…
5	Informati…	Systematic enumeration and examination in order to find weaknesses and points where a security vulnerability might exist	Defence includes providing anti-automation	5	Me…
6	Elevation …	Usage may resemble	Mitigation or prevention	6	Me…

		legitimate application usage but leads to exhaustion of resources	such as providing backoff, resource management and avoiding forced deadlock		
7	Informati…	Information gathering with the objective of learning as much as possible about the composition, configuration and security mechanisms of the application	Defences include shutting down unnecessary services/ports and excluding information that could identify and compromise security of the organisation	2	Low
8	Tampering	Using speed to violate explicit or implicit assumptions about the application's normal use to achieve unfair individual gain	Defences include providing enforcement of behavioral workflow and anti-automation	4	Me…
9	Informati…	Systematic enumeration and examination in order to find weaknesses and points where a security vulnerability might exist	Defence includes providing anti-automation	3	Low
10	Elevation …	Usage may resemble legitimate application usage but leads to exhaustion of resources	Mitigation or prevention such as providing backoff, resource management and avoiding forced deadlock	5	Me…
11	Informati…	Collecting accessible data and/or processed output from the application	Detect fake or compromised accounts, ensure information is accessible only with authentication and authorisation	10	Crit…
12	Elevation …	Automated repeated clicking or requesting or submitting content, affecting application based metrics such as counts, and measures of frequency and/or rate	Defences include control of interaction frequency or proper enforcement of a single unique action	7	High
13	Elevation …	Storing malicious such as malware, Iframe distribution, photographs & videos, advertisements, referrer spam and tracking/surveillance code	Defences include detecting embedded malicious code, controling interaction frequency and enforcement of a single unique action	8	High
14	Informati…	Collecting accessible data and/or processed output from the application	Detect fake or compromised accounts, ensure information is accessible only with	8	High

			authentication and authorisation		
15	Elevation …	Automated repeated clicking or requesting or submitting content, affecting application based metrics such as counts, and measures of frequency and/or rate	Defences include control of interaction frequency or proper enforcement of a single unique action	4	Me…
16	Elevation …	Storing malicious such as malware, Iframe distribution, photographs & videos, advertisements, referrer spam and tracking/surveillance code	Defences include detecting embedded malicious code, controlling interaction frequency and enforcement of a single unique action	6	Me…