# Detecting Web DDoS

DoS attack : generate many requests : impact is capped by its CPU

Types of DoS Attacks :

slowloris : Sending many partial HTTP requests to tie up server resources

HTTP Flood : Sending a large number of HTTP requests to overwhelm the server

central delivery network

Cache Bypass : Bypassing CDN edge servers and forcing the origin server to respond

Oversized Query : Forcing the serves to process large, resource-intensive requests

Login/Form Abuse : Overloading authentication with logic attempts or password resets.

Faulty input Validation Abuse : Exploiting poorly designed input handling.

## Possible Attack Motivations:

Financial Loss :- Disrupt services to stop or reduce sales and revenue

Extortion : Demand paymend to stop a current attack.

Hacktivism : Disruption for social or political protest

Distraction : Redirect defenders' attention while other attacks take place

Competition : Disrupt a rival's service

Denial of Wallet : Force the victim to rack up service usage costs

Reputational Damage : Cause customers to lose trust in a company

## Log Analysis

By examining these logs, can uncover patterns that help distinguish Between normal and malicious activity

## Indicators

High Request Rate
Odd user-agents
Geographic anomalies
Burst Timestamps
Server Errors (5xx) 500-511
Logic Abuse

## Targeted Resources

- likely focus on endpoints that consume the most server resources per request or are most critical to maintain site functionality.

## Defense

### Application Defense

- Secure Development Practices
- Challenges CAPTCHA

### Network and Infrastructure Defenses

- Content Delivery Network
- Web Application Firewall (WAF)

### Large-Scale Mitigation

### Bypassing Security Measures