# Denial of service

**Primeri za našu aplikaciju:**

* Napadač pokušava da optereti sistem na aplikativnom nivou (HTTP) tako što šalje veliki broj legalnih GET zahteva za nekim resursema kao što su spisak akata i amandmana, pojedinačnim aktima odnosno amandmanima.
* Prilikom razvoja aplikacije može se slučajno zaboraviti neophodnost zatvaranja konekcije sa bazom podataka koja se otvara da bi se izvrsila određena komunikacija sa bazom podataka. Napadač to može iskoristiti da pokrene veći broj istih radnji i time otvori veliki broj veza sa bazom podataka pri čemu te veze nikad korektno neće biti zatvorene.
* Prilikom razvoja aplikacije se na sesiju zakači velika količina podataka pa usled velikog broj korisnika, količina podataka koja se čuva na sesiji se povećava i sistem se usporava.
* Napadač koristeći UDP neprestano šalje zahteve ka svim mogućim portovima čime primorava server da nazad napadaču šalje ICMP poruke. Ukoliko napadač šalje veliki broj UDP paketa sistem će biti primoran da šalje veliku količinu podataka nazad.
* Napadač koristi SYN DDoS (SYN flood DoS) napad i time preopterećuje TCP transmisioni nivo tako što neprestano šalje SYN zahteve ciljanom sistemu pokušavajući da konzumira što više resursa žrtve i time ne uspe da reaguje na legitimni saobraćaj.

**Odbrana:**

* Koristiti hardveri koji će registrovati neuobičajne radnje i suspendovati sumnjiv pristup sistemu.
* Stalna analiza koda i testiranje performansi sistema odnosno izdržljivosti.
* Ograničiti veličinu dokumenta koji se može poslati na server.
* Obezbediti veći protok.
* Rezultate pretrage ne kačiti na sesiju.
* Ograničiti broj rezultata pretrage koji se isporučuju korisniku u jednoj interakciji.
* Isključiti UDP i ograničiti na koje portove server radi.
* Validirati unete podatke.