**Spoofing**-predstavlja mogućnost lažnog predstavljanja naivnim korisnicima sa namerom da im se ukradu kredencijali ili neki drugi resursi koji je poverljiv za korisnika koji se napada.

Deli se na : E-mail spoofing, IP spoofing, URL spoofing

**E-mail spoofing**-zasnovan je na kreiranju lažne poruke i menjanja zaglavlja sama poruke kako bi se korisnik prevario. Mail koji stiže korisniku uglavnom je napisan tako da izgleda kao da je došao od poverljive osobe, a tekst ima neku važnost i mora se odraditi ono što piše kako se ne bi desila neka ozbiljna šteta (gubljenje lozinke, pražnjenje računa...)

Najbolji način za odbranu od ove vrste spoofing napada je da korisnici budu obazrivi kada dobiju čudne poruke i da pre nego što odu na linkove koji se nalaze u poruci provere o čemu se tačno radi i koliko su bezbedni.

**Primeri za našu aplikaciju:**

* Odbornik može dobiti email poruku u kojoj će se pošiljalac predstaviti kao čovek od poverenja ili kao neko ko ima veće nadležnosti od njega tražeći da predlože neki akt ili amandman.
* Može se desiti da odbornici dobiju email poruku u kojoj će biti link uz pomoć kojeg će se povući predloženi amandman ili akt.
* Predsednik skupštine može dobiti email poruku sa linkom kojim prihvata neke akte i amandmane, a da to prethodno nije izglasano.

**IP spoofing**-sve što se radi na internetu radi se sa paketima, a svaki paket nosi adresu svog pošiljaoca. Ideja kod ove vrste spoofinga je da se stvore paketi sa lažnom adresom izvora i samim tim se zavara trag i sa tim mogu steći neovlašćeni pristup sistemu za autentifikaciju.

Najbolji način da se sačuva od ove vrste spoofing napada je da se ruter dobro konfiguriše kako bi se pazilo koje pakete će primati, enkripcija i autentifikacija.

**URL spoofing**-predstavlja pokušaj da se URL neke zlonamerne stranice prikaže kao URL neke poznate stranice i samim tim zavara korisnik koji se napada. Ovaj napad se obično ugrađuje u E-mail spoofing napad.

Najbolja zaštita od ovog napada je korišćenje najnovijih web pretraživača koji donose dosta poboljšanja i ispravki u domenu zaštite.

**Tampering with data**-predstavlja maliciozno menjanje podataka sa ili bez autorizacije. Posledica može biti formatiranje diska, ubacivanje malicioznih podataka u sistem ili u mreznu komunikaciju kao i neprimetna promena osetljivih podataka.

Najbolja zaštita od ovog napada je da se osetljivi podaci ne izlažu direktno, treba ih kriptovati i tako kriptovane smeštati u bazu podataka.

**Primeri za našu aplikaciju:**

* Može se desiti neovlašćena promena akata ili amandmana i to na mestima gde napadačima odgovara kako bi mogli da izvode neke druge napade.
* Može izazvati pad sistema i samim tim odlaganje rada i donošenje drugih akata i amandmana.