**Spoofing**

***E-mail spoofing***

**Odbrana -** 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. Ako je pristigli e-mail sumnjiv na bilo koji način ne treba ga otvarati.

**Primeri za našu aplikaciju:**

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

***IP spoofing***

**Odbrana -** 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.

**Primeri za našu aplikaciju:**

* Napadač može da stvori maliciozne pakete sa lažnom adresom izvora i samim tim zavara svoj trag i stekne neovlašćen pristup sistemu za autentifikaciju.

***URL spoofing***

**Odbrana -** Najbolja zaštita od ovog napada je korišćenje najnovijih web pretraživača koji donose dosta poboljšanja i ispravki u domenu zaštite. Uvek treba direktno kucati URL u pretraživač kako bi se izbegla mogućnost redirektovanja na maliciozne sajtove. Ne treba ostavljati poverljive podatke na sumnjivim sajtovima. Pre odlaska na neki sumnjivi sajt prvo treba lično proveriti da li je bezbedan ili ne.

**Primeri za našu aplikaciju:**

* Korisnik može dobiti e-mail poruku sa url-ovima koji liče na poznate adrese, ali iza njih su skriveni maliciozni sajtovi koji mogu napadacu da omoguće izvršavanje malicioznog koda i samim tim napadač može da dobije pristup poverljivim podacim, , kao i manipulaciju sa postojećim podacima. Mogućnost da predlaže, povlače ili usvajaju akte i amandmane.

**Tampering with data**

**Odbrana -** Najbolja zaštita od ovog napada je da se osetljivi podaci ne izlažu direktno, treba ih kriptovati i tako kriptovane smeštati u bazu podataka. Treda podatke koji se prikupljaju sa formi validirati i na front-end i na back-end strani kako se ne bi mogli poslati maliciozni podaci.

**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.
* Ubacivanjem malicioznog koda može se izazvati formatiranje diska, a posledica toga je prestanak rada skupštine dok se podaci ne povrate ukoliko su oni pre toga uspešno sačuvani na drugom mestu ili potpuni gubitak podataka ako nisu sačuvani.
* Ubacivanjem nevalidiranih podataka napadač može da pošalje maliciozan kod koji će se izvršiti na bazi, back-end ili front-end strani naše aplikacije i tako ugroziti našu aplikaciju i podatke koje naša aplikacija obrađuje.