Elevation of privilege

**Narušavanje povlastica**(*elevation of privilege* ili *privilege escalation*)

Narušavanje povlastica se javlja u dva oblika:

1. **Vertikalno povećanje povlastica**(*Vertical privilege escalation* ili *privilege elevation*) Kao primer za ovakav slučaj u našoj aplikaciji se može navesti situacija da običan građanin, dakle ne odbornik ili predsednik skupštine, može da pristupi resursima, za koje on nema odobrena prava pristupa(usvajanje akata, amandmana, povlačenje akata ili amandmana, kao i samo predlaganje istih).

Mogućih strategija za ublažavanje ovakvih problema ima nekoliko.

* [*Principle of least privilege*](https://en.wikipedia.org/wiki/Principle_of_least_privilege) kod koga je ideja da svaki modul (korisnici, procesi, sama aplikacija) mogu da koriste samo one resurse koji su im potrebni za normalan rad i funkcionisanje.
* Omogućiti da se odradti validacija, kako na klijentskoj strani, tako i na serverskoj, odnosno potvrda samih informacija i resursa koji se primaju i koji se šalju(*Shell injection*).
* Onemogućiti korišćenje skripti web pretraživača pre korišćenja aplikacije. Neke aplikacije su tako napisane da omogućavaju funkcionisanje bez korišćenja bilo kakvih *client-side-scripts*.
* *WEB application firewall* koji postavlja određena pravila u HTTP konverzaciji. Na ovaj način, pravilo konfigurisan, mogu se prepoznati i blokirati XSS napadi. Čak se ide i korak dalje, omogućavajući da se prepoznaju novi napadi, tako što se uočavaju nepoznati šabloni.

**2. Horizontalno povećanje povlastica**(Horizontal privilege escalation)

Kao primer u našoj aplikaciji, može se navesti situacija da drugi odbornik na neki način preuzme kontrolu nad resursima drugog odbornika ili možda čak i predsednika skupštine, čime dobija dodatne mogućnosti za manipluaciju.

Mogućih strategija za ublažavanje ovakvih problema ima nekoliko.

* Prilikom kreiranja samih lozinka, biti barem malo maštovit, upotrebiti neka od [pravila](http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/) za kreiranje lozinki, kao i samo [merenje](https://howsecureismypassword.net/) jačine lozinke.
* Koristiti TLS prilikom HTTP komunikacije.
* Istražiti postojeća i proverena rešenja