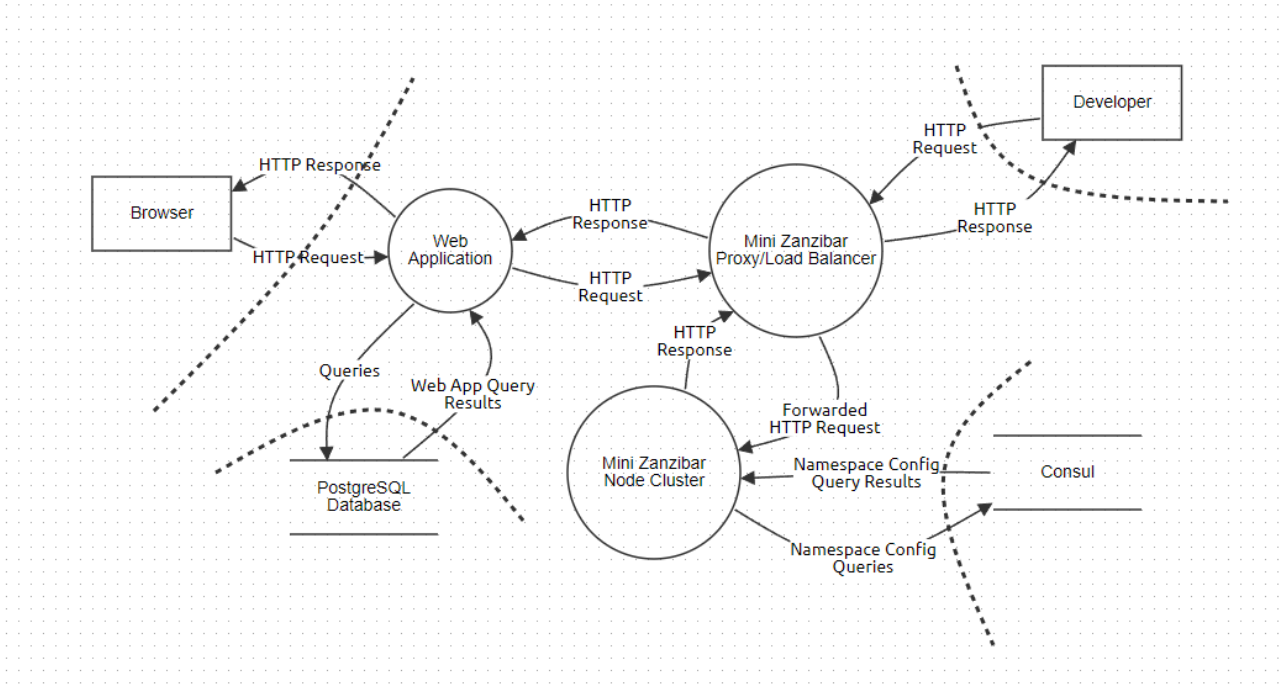
Model Pretnji

Uvod

Predmet ovog rada je model i analiza pretnji za infomacioni sistem koji se sastoji iz aplikacije za deljenje dokumenata i aplikacije za autorizaciju (u nastavku Mini Zanzibar). Izvorni kod aplikacije za deljenje dokumenata i Mini Znazibara može se naći na sledećem linku: https://github.com/vdevic01/MiniZanzibar. Aplikacija za deljenje dokumenata omogućava korisnicima da upload-uju dokumente na sistem i dele ih sa drugim korisnicima. Da bi korisnik izvšio upload potrebno je da bude registrovan. Vlasnik dokumenta može da podeli dokument sa drugim registrovanim korisnicima. Prilikom provere da li neki korisnik ima određena ovlašćenja za neki dokument koristi se mini zanzibar, tako što se sa serverskog sloja aplikacije za deljenje dokumenata šalje HTTP zahtev na Mini Zanzibar API koji proverava da li zadati korisnik ima određene dozvole za određeni resurs/dokument.
Mini Zanzibar je zamišljen kao jedinstven sistem za autorizaciju koji može biti deljen između različitih softverskih proizvoda jedne kompanije. U okviru ovog rada, aplikacija za deljenje dokumenata predstavlja jedan proizvod hipotetičke kompanije. Za svaki softverski proizvod, potrebno je definisati *namespace* konfiguraciju. *Namespace* konfiguracije je objekat koji se čuva u Consul ključ-vrednost bazi podataka. Mini Zanzibar koristi ovu konfiguraciju prilikom kreiranja i provere ovlašćenja. Pored same aplikacije koja koristi Mini Zanzibar za autorizaciju korisnika, korisnici Mini Zanzibara su i programeri u hipotetičkoj kompaniji koji ga koriste za definisanje novih *namespace* konfiguracije. Prilikom kreiranja novog softverskog proizvoda potrebno je kreirati novu *namespace* konfiguraciju koja definiše koje sve uloge postoje u tom sistemu i kako se međusobno odnose.
Dijagram toka podata je prikazan na slici ispod:



Aplikacija za deljenje dokumenata

Motivacija napadača

Prema motivaciji napadači su podeljeni u sledeće klase:

- Napadači motivisani krađom privatnih informacija - Ovo su pojedinci ili grupe čija je meta nije sam sistem već korisnik ili grupa korisnika sistema. Cilj napada može biti krađa dokumenata koje je žrtva postavila na sajt.
- Konkurentske organizacije i zlonamerni pojedinci - Cilj ove grupe napadača je da naštete samoj kompaniji, najčešće kroz DOS ili DDOS napade.

Imovina(Assets)

Imovina predstavlja sve informacije i resurse koji imaju neku vrednost za kompaniju. Imovina aplikacije za deljenje dokumenata obuhvata dokumente koji korisnici postavljaju na sistem, šifre korisnika i liče informacije koje korisnici ustavljaju prilikom registracije.

Ulazne tačke napada

Ulazne tačke za napda na aplikaciju za deljenje dokumenata:

- Web klijent
- REST API
- Baza podataka

Analiza pretnji

Spoofing of identity

Aplikacija koristi JWT za autnetifikaciju korisnika što sprečava krađu identiteta. JWT se čuva unutar locastorage-a što može biti problem u slučaju XSS napada. U slučaju da je JWT ukraden, napadač može izvšiti privilegovane akcije u ime korisnika čiji je identitet ukrao. Možemo povećati sigurnost sistema tako što ćemo JWT čuvati kao cookie sa uključenim svim sigurnosim mehanizmima - HttpOnly, Secure, SameSite.

Tampering

Rizik od ove pretnje postoji ukoliko napadač presretne zahtev i izmeni ga. Može se iskoristiti da se napadaču daju privilegije na određene dokumente koji mu ne pripadaju.Zaštita može biti sprovedena korišćenjem HTTPS komunikacije između web klijenta i web servera i web servera i PostgreSQL baze podataka.

Repudiation

Repudiation predstavlja svojstvo sistema da korisnik ne može da negira izvšravanje neke akcije. U našem sistemu korisnik bi mogao da negira davanje dozvola za deljenje dokumenta ili samo upload-ovanje dokumenta. *Repudiation* se može obezbediti implementacijom sistema logovanja.

Information Disclosure

Information Disclosure predstavlja osobinu sistema da zaštiti informacije od neovlašćenog pristupa. Ovo je obezbeđeno postavljanjem jake šifre za bazu podataka. Takođe vođeno je računa da poruke greške koje server šalje ne sadrže osetljive informacije. Prilikom implementacije sistema za logovanje voditi računa da sami log zapisi ne sadrže osetljive informacije o korisnicima.

Elevation of Privilege

Elevation of privilege je osobina sistema da spreči napadača da dobije veća ovlašćenja nego što mu pripadaju. Napadač može pokušati da dobije veća ovlašćenja za dokumenta nego što ima. Zaštita od ove vrste napada je delegirana na Mini Zanzibar. Potrebno je voditi računa o SQLi napadima koji mogu napadaču dati mogućnost da izvršava upite nad bazom podataka. Zaštita se vrši sanitizacijom korisnički unetih podataka.

Mini Zanzibar

Motivacija napadača

Pošto je sam sistem poprlično prost ne postoji mnogo razloga za napad. Glavna funkcionalnost sistema je provera da li neki korisnik ima određenu dozvolu. Napadač bi mogao da napadne sistem sa namermo da poveća svoje privilegije kako bi dobio pristup određenim resursima/dokumentima.

Imovina(Assets)

Acl koje se čuvaju u LevelDB bazi podataka ne sadrže osetljive podatke jer je sve izraženo preko id obeležja. Slično acl, *namespace* konfiguracije ne sadrže informacije koje nisu već poznate krajnjim korisnicima. Ono što sistem treba da zaštiti je mogućnost izmene acl ili *namespace* konfiguracija. Algoritam koji Mini Zanzibar koristi je javno dostupan, te nema potrebe ulagati dodatne resurse u njegovu zaštitu.

Ulazne tačke napada

Ulazne tačke za napda na aplikaciju za deljenje dokumenata:

- REST API
- Baza podataka za čuvanje acl
- Baza podataka za čuvanje *namespace* konfiguracija

Pošto je korišćena LevelDB baza koje ne radi u posebnom servisu već je ugrađena u sam Mini Zanzibar sistem, dovoljno je zaštiti server na kome se sistem nalazi kako bi se zaštitili od potencijalnih spoljnih napadača. Iako baza nije dostupna preko interneta potrebno je zaštiti podatke od zaposlenih u hipotetičkoj kompaniji koji imaju pristup samom serveru.

Analiza pretnji

Spoofing of identity

Iako Mini Zanzibar API nije javno dostupan i namenjen je isključivo za upotrebu unutar kompanije, njegovi endpointi se i dalje mogu pogoditi. Kako bi uvek znali ko pristupa sistemu u našem rešenju iskorišćen je API ključ koji je potrebno uključiti u zaglavlje svakog HTTP zahteva. Sigurnije rešenje bi bilo da se dozvoli pristup samo sa određenih ip adresa. Sistem trenutno funkcioniše sa jednim API ključem koji se koristi u svim aplikacijama koje koriste Mini Zanzibar. U slučaju da vrednost API ključa bude kompomitovana, potrebno je promeniti API ključ u svim ovim aplikacijama. Bolje rešenje bi bilo da se svakoj aplikaciji dodeli unikatan ključ. U to slučaju određenim ključevi se mogi izbrisati ukoliko se ustanovi da su kompromitovani.

Tampering

O ovome je bilo već reči u poglavlju “Ulazne tačke napada”. Ukoliko je server na kome se nalazi Mini Zanzibar zaštićen, sistem je bezbedan od spoljašnjih napadača. Što se tiče zaposlenih koji imaju pristup bazi podataka, poželjno je implementirati sistem logovanje tako da svaka akcija koju neko od zaposlenih izvrši nad sistemom bude sačuvana.

Repudiation

Repudiation predstavlja svojstvo sistema da korisnik ne može da negira izvšravanje neke akcije. Kao i u aplikaciji za deljenje dokumenata potrebno je obezebediti sistem logovanja za sve izemene acl i *namespace* konfiguracija.

Information Disclosure

Information Disclosure predstavlja osobinu sistema da zaštiti informacije od neovlašćenog pristupa. O ovome je takođe bilo reči u poglavlju “Ulazne tačke napada”. Čitanje samih informacija o acl ili *namespace* konfiguracijama nije problematično. Sistem je potrebno zaštiti od izemena tih podataka.

Elevation of Privilege

Elevation of privilege je osobina sistema da spreči napadača da dobije veća ovlašćenja nego što mu pripadaju. Pošto Mini Zanzibar nema role dovoljno je da napadač dođe u posed API ključa kako bi dobio mogućnost obavlanje svih akcija nad sistemom. Iz tog razloga treba uložiti napore u zaštitu API ključa. Dodatna mogućnost je da se ključevima pridruže role. Pošto aplikacije koje koriste Mini Zanzibar nemaju potrebu da kreiraju nove *namespace* konfiguracije ima smisla ograničiti im tu funkcionalnost. Takođe zaposleni u kompaniji nemaju potrebe da koriste funkcionalnosti sem pravljenja *namespace* konfiguracija. Iz ovoga sledi da ima smisla napraviti deve role, jedna za aplikacije koje koriste acl i jedna za zaposlene koji upravljaju *namespace* konfiguracijama.