1. Analiza sistema

Opis sistema:

- Mini-Zanzibar je globalni sistem autorizacije koji podržava fleksibilan konfiguracioni jezik za definisanje politika kontrole pristupa.
- Skladišti i evaluira liste kontrole pristupa (ACLs) koristeći Google LEVEL DB i ConsulDB za verzionisanje konfiguracija.
- Omogućava konzistentne i skalabilne odluke o autorizaciji sa niskim kašnjenjem i visokom dostupnošću.

Ključne komponente:

- **Model podataka:** Relacione torke za skladištenje ACL-ova.
- **Konfiguracija namespace-a:** Definisanje različitih tipova pristupa i pravila prepisivanja skupa korisnika.
- **API:** Endpointi za kreiranje/izmenu ACL-ova, provera ACL-a i kreiranje/izmenu namespace-ova.

2. Definisanje bezbednosnih zahteva prema OWASP ASVS

V1: Arhitektura, dizajn i modelovanje pretnji

- **V1.2:** Arhitektura autentifikacije
  - Proveriti da sve komponente sistema imaju najmanje privilegije
- **V1.4:** Arhitektura kontrole pristupa
  - Za zaštitu podataka i resursa treba korisiti proveren mehanizam kontrole pristupa
  - Proveravati da li korisnik ima pravo pristupa na nekom funkcionalnošću i podacima
- **V1.5:** Arhitektura ulaza i izlaza
  - Upotreba serijalizacije sa pouzdanim klijentima
  - Vršiti proveru validnosti ulaznih podataka
- **V1.7:** Greške, logovanje i revizija arhitekture
  - Vršiti logovanje sistema

V2: Autentifikacija

- **V2.1:** Osigurati da svi korisnici koriste jake lozinke koje su šifrovane u bazi podataka.
- **V2.4:** Skladištenje kredencijala
  - Koristiti funkcije za heširanje koje uzimaju lozinku, so i *cost factor* prilikom generisanja heša lozinke

Ne ćemo implementirati višefaktorsku autorizaciju, reCaptcha, reset password, pošto je to sve rađeno na prošlom kursu.

V3: Upravljanje sesijama

- **V3.1:** Fundamentalna bezbednost upravljanja sesijom
    - Aplikacija ne sme da okriva tokene sesije u URL parametrima
- **V3.2:** Vezivanje sesija
    - Prilikom svake korisnikove autentifikacije, kreira se novi token sesije
    - Pobrinuti se o bezbednosnim mehanizmima za bezbedno čuvanje tokena
- **V3.3:** Automatski završiti sesije nakon perioda neaktivnosti kako bi se smanjio rizik od zloupotrebe

V4: Kontrola pristupa

- **V4.2:** Osigurati da se sve operacije autorizacije loguju i redovno pregledavaju

V5: Validacija, sanitizacija i enkodiranje

- **V5.1:** Validirati sve unose korisnika da bi se sprečili napadi kao što su SQL Injection i XSS.
- **V5.3:** Kodiranje izlaza i sprečavanje injection-a
    - Koristiti bezbedne API-je za izvršavanje komandi i validirati sve ulaze
    - Izbegavati direktno izvršavanje komandi sa korisničkim unosom
- **V5.5:** Bezbedna deserijalizacija

V6: Skladištena kriptografija

- **V6.1:** Šifrovati sve osetljive podatke
- **V6.2:** Koristiti snažne kriptografske algoritme za zaštitu podataka
- **V6.4:** Bezbedno upravljati tajnama kao što su API ključevi i lozinke

V7: Rukovanje greškama i evidencija

- **V7.1:** Sadržaj logovanja
    - Evidentirati sve sigurnosno relevantne događaje i greške
- **V7.3:** Zaštita loga
    - Proveriti da li bezbedno logovanje, bez otkrivanja nekih osetljivih podataka
    - Provera o zaštiti logovanja tako da ne možemo da im pristupi niko ko nije autorizovan za to, kao ni da vrši izmene
- **V7.4:** Prikazivati generičke poruke o greškama korisnicima, bez otkrivanja detalja koji bi mogli biti korisni napadačima

V8: Zaštita podataka

- **V8.1:** Šifrovati sve osetljive podatke kako u mirovanju, tako i tokom prenosa

V9: Komunikacija

- **V9.1:** Bezbedna komunikacija sa klijentom
- **V9.2:** Sigurnost komunikacije servera
    - Korišćene tls sertifikata
    - Dodati sigurnu vezu između aplikacije i baza

V10: Maliciozni kod

- **V10.1:** Analizirati kod alatom koji može da detektuje maliciozni kod
- **V10.2:** Manuelna provera postojanja malicioznog koda

V13: API i web servisi

- **V13.1:** Generička bezbednost veb servisa
    - Proverite da li sve komponente aplikacije koriste ista kodiranja i parsere
    - Proverite da li su zahtevi koji sadrže neočekivane ili nedostajuće tipove sadržaja odbijeni sa odgovarajućim zaglavljima
- **V13.2:** Osigurati da su svi API endpointi zaštićeni jakim autentifikacionim mehanizmima

V14: Konfiguracija

- **V14.2:** Zavisnosti (*dependency*)
    - Koristiti najnovije biblioteke
- **V14.4:** Obezbediti sigurnost HTTP zaglavlja
- **V14.5:** Provera zaglavlja HTTP zahteva

Implementacijom ovih bezbednosnih zahteva prema OWASP ASVS standardu biće omogućeno da sistem Mini-Zanzibar bude adekvatno zaštićen od različitih pretnji. Ovim smernica možemo da osiguramo visoku sigurnost, pouzdanost i dostupnost sistema.