Elektrotehnički fakultet Banja Luka
Katedra za računarstvo i informatiku
Sigurnost na internetu
Projektni zadatak

Zadatak

Realizovati internet forum u okviru kojeg će registrovani korisnici moći razmjenjivati mišljenja po pitanju različitih tema. Teme su podijeljene po oblastima, a forum podržava minimalno sljedeće oblasti/sobe: *Nauka*, *Kultura*, *Sport* i *Muzika*.

Web aplikacija se sastoji iz tri dijela, koji su dostupni korisnicima u zavisnosti od korisničke grupe kojoj pripadaju. Korisnici se dijele u tri grupe: *Administrator*, *Moderator* i *Forumaš*.

Administratorskom dijelu aplikacije može da pristupi samo grupa *Administrator* i u ovom dijelu aplikacije se upravlja korisničkim nalozima:

- odobrava/zabranjuje se pristup registrovanom korisniku,
- definiše se grupa kojoj će pripadati registrovani korisnik,
- definiše se skup permisija koje će registrovani korisnik imati (dodavanje, izmjena, brisanje komentara za neku oblast itd.).

Moderatorskom dijelu aplikacije mogu da pristupe grupe *Administrator* i *Moderator* i u ovom dijelu aplikacije se upravlja komentarima forumaša, pri čemu se novi komentar može objaviti (sa ili bez prilagođavanja) ili zabraniti.

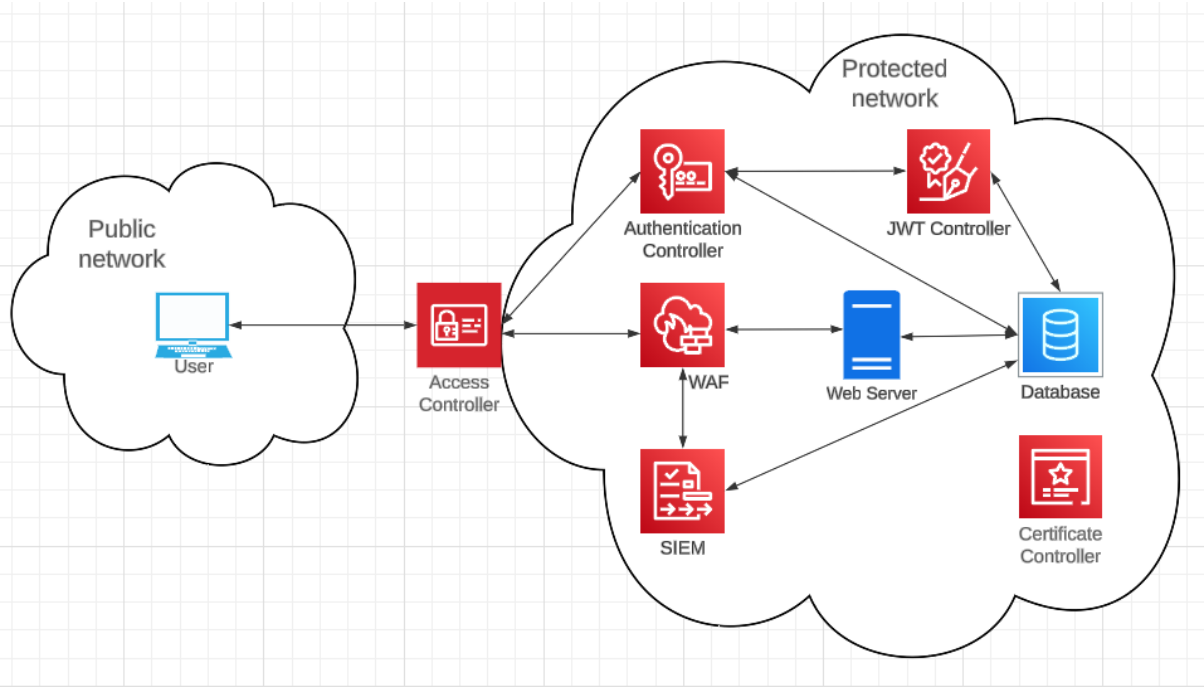
Forumskom dijelu aplikacije mogu da pristupe sve korisničke grupe i on je organizovan po sobama/oblastima. Za svaku oblast prikazuje se lista posljednjih 20 komentara, pri čemu se minimalno prikazuje sadržaj komentara, ime korisnika i vrijeme objavljivanja.

Novi korisnik se registruje na forum, nakon čega *Administrator* može da odobri registraciju, pri čemu korisnik dobija odgovarajuće obavještenje putem *e-mail*-a. Nakon registracije, korisnik se može prijaviti na sistem, pri čemu se koristi dvo-faktorska autentikacija. U prvom koraku korisnik unosi korisničko ime i lozinku, nakon čega dobija verifikacioni kod putem *e-mail*-a, koji je potrebno unijeti u narednom koraku prijave.

Na slici 1 je ugrubo prikazana arhitektura sistema. *Access Controller* je komponenta koja prihvata svaki korisnički zahtjev, komunicira sa ostalim komponentama i vraća odgovor korisniku. *Authentication Controller* vrši autentikaciju korisnika i autorizaciju korisničkih zahtjeva. Nakon uspješne prijave, korisnik dobija JWT token, koji se dalje koristi za praćenje korisničke sesije. Komponenta zadužena za izdavanje i validaciju tokena je *JWT Controller*. WAF (*Web Application Firewall*) je komponenta koja skenira saobraćaj prema *web* serveru i propušta samo benigne zahtjeve, a odbija potencijalno maliciozne. WAF prati usklađenost sadržaja zahtjeva sa definisanim pravilima koja se odnose na korisnički unos (na primjer, maksimalna dužina teksta, sekvence koje se mogu pojaviti itd.). U slučaju da korisnik pošalje zahtjev koji nije u skladu sa definisanim politikama, *Access Controller* može automatski da zatvori sesiju sa korisnikom.

Komunikacija između korisnika i sistema, kao i komunikacija između pojedinih komponenata sistema, treba da bude zaštićena. *Certificate Controller* je komponenta

zadužena za izdavanje, praćenje i povlačenje digitalnih sertifikata za sve komponente. Rad sa sertifikatima može da bude realizovan pomoću eksternog alata. SIEM komponenta je zadužena za praćenje i logovanje svih sigurnosno osjetljivih zahtjeva.



Slika 1 – Arhitektura sistema

Pored standardnog načina prijave korisnika, potrebno je omogućiti i prijavu na sistem pomoću OAuth2 *framework*-a, pri čemu se za prijavu u tom slučaju koristi neki eksterni korisnički nalog (Google, GitHub i sl).

Sve detalje zadatka koji nisu precizno specifikovani realizovati na proizvoljan način. Detalje korisničkog interfejsa realizovati na proizvoljan način. Sistem treba da bude *web* baziran. Dozvoljena je upotreba proizvoljnog programskog jezika, kao i proizvoljnih tehnologija neophodnih za realizaciju tehničkih detalja.

Studenti koji uspješno odbrane projektni zadatak stiču pravo izlaska na usmeni dio ispita. Prije odbrane, potrebno je postaviti kompletan izvorni kod projektnog zadatka na *moodle*. Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2024. godine i vrijedi do objavljivanja sljedećeg projektnog zadatka.