Potrebno je izraditi **web-aplikaciju** koja će omogućiti potencijalnom napadaču korištenje **dvije različite tehnike sigurnosnih napada**, odnosno dvije ranjivosti web-aplikacija, iz dolje navedenih kategorija.

Za svaku je potrebno implementirati:

- funkcionalnost kojom se **omogućuje** ranjivost
- funkcionalnost kojom se **onemogućuje** ranjivost

Npr. napraviti "prekidač" (npr. *checkbox*, tipka ili padajući izbornik) kojim se ranjivost po želji uključuje i isključuje.

Ugrađene ranjivosti (sigurnosne nedostatke), s njima povezane napadačke tehnike i implementirane funkcionalnosti moraju biti dostupne kroz korisničko sučelje web-aplikacije tako da:

1. napadi se mogu pokrenuti kroz sučelje web-aplikacije
2. učinak napada bude vidljiv u korisničkom sučelju (npr. prikladnim ispisom niza izvršenih akcija, ispisom izmijenjenog sadržaja baze podataka, prikazom *javascript:alert* standardnog dijaloga s podacima o korisničkoj sjednici *document.cookie* itd.).

Za eventualno slanje ili primanje e-mail poruka sa malicioznim linkom koristiti neki od servisa s privremenim poštanskim sandučićima (npr. https://www.mailinator.com/).

Web-aplikaciju je potrebno postaviti u oblak, a izvorni kod nužan i dovoljan za pokretanje aplikacije pohraniti na GitHub ili GitLab.

Napomena: Ako iz nekog razloga nećete moći izvesti ranjivost u cloud instalaciji (npr. ako sustav sam blokira brute-force napad ili odabrani radni okvir onemogućuje SQL umetanje) onda morate napisati kratke i jasne upute kako instalirati i pokrenuti sustav lokalno, po mogućnosti što jednostavnije npr. npm i && npm run server.

Potrebno je implementirati ranjivosti:

1. **Cross-site scripting (XSS) - jedan tip XSS napada po izboru (bilo koji)**
2. **Loša kontrola pristupa (Broken Access Control)**

Napomene:

Aplikaciju postaviti u oblak (preporuča se besplatna opcija na *Renderu*), a kao odgovor na ovo pitanje isporučiti redom:

- adresu git repozitorija s web-aplikacijom (repozitorij može biti privatni, ali omogućiti pravo pristupa nastavnicima). Korisnički računi nastavnika za GitHub i Gitlab su : *mekterovic*, *mhorvat* i *boris612*
- adresu web-aplikacije
- popis implementiranih ranjivosti - kratka lista od <= 2 zapisa
- napomene (npr. "sve je uspješno implementirano", ili "nisam uspio/-la implementirati", itd.)
- kratke upute kako pokrenuti i isprobati aplikaciju *(ako je potrebno, navesti korisnička imena potrebna za testiranje)*