OWASP Top 10 - 2021

1. A01:2021-Broken Access Control

- Kršenje principa najmanjih privilegija ili zabrane po defaultu, gde bi pristup trebalo da bude odobren samo za određene sposobnosti, uloge ili korisnike, ali je dostupan svima.
- Zaobilaženje provera kontrole pristupa modifikovanjem URL-a (manipulacija parametrima ili forsirano pregledavanje), internog stanja aplikacije, ili HTML stranice, ili korišćenjem alata za napad koji modifikuje API zahteve.
- Dozvoljavanje pregleda ili uređivanja tuđeg naloga pružanjem njegovog jedinstvenog identifikatora (nesigurni direktni referenci objekata).
- Pristupanje API-ju bez kontrola pristupa za POST, PUT i DELETE zahteve.
- Povećanje privilegija. Delovanje kao korisnik bez prijavljivanja ili delovanje kao administrator kada ste prijavljeni kao korisnik.
- Manipulacija metapodacima, kao što je ponavljanje ili manipulacija JSON Web Token (JWT) tokenom za kontrolu pristupa, kolačićem ili skrivenim poljem da bi se povećale privilegije ili zloupotreba poništenja JWT.
- CORS pogrešna konfiguracija omogućava pristup API-ju sa neautorizovanih/nepouzdanih izvora.
- Forsirano pregledavanje ka stranicama koje zahtevaju autentifikaciju kao neautentifikovani korisnik ili ka stranicama sa privilegijama kao standardni korisni

Moja implementacija: Upravljanje pristupom koristeći RBAC. Ograničavanje pristupa resursima na osnovu uloga korisnika u sistemu

2. A07:2021-Identification and Authentication Failures

- Dozvoljava automatizovane napade kao što je ubacivanje akreditiva (credential stuffing), gde napadač ima listu validnih korisničkih imena i lozinki.
- Dozvoljava brute force ili druge automatizovane napade.
- Dozvoljava korišćenje podrazumevanih, slabih ili poznatih lozinki, kao što su "Password1" ili "admin/admin".

- Koristi slabe ili neefikasne procese za oporavak akreditiva i zaboravljene lozinke, kao što su "odgovori zasnovani na znanju," koji ne mogu biti sigurni.
- Koristi skladištenje lozinki u običnom tekstu, enkriptovanim, ili slabo haširanim formama (pogledati A02:2021-Kriptografski neuspesi).
- Nedostaje ili je neefikasna višefaktorska autentifikacija.
- Izlaže identifikator sesije u URL-u.
- Ponovo koristi identifikator sesije nakon uspešnog prijavljivanja.
- Ne ispravno poništava ID sesije. Korisničke sesije ili tokeni za autentifikaciju (uglavnom tokeni za jednokratnu prijavu - SSO) nisu pravilno poništeni tokom odjave ili perioda neaktivnosti.

Moja implementacija: Politika lozinki pri registraciji. Zahtevanje kompleksnih lozinki i onemogućavanje poznatih kompromitovanih lozinki.