

Analiza Securitatii

Analiza riscurilor si tactici pentru adresarea lor

- Autentificare nesigura: utilizat Identity pentru hashing al parolelor si impunerea parolelor sigure (lungime minima, existenta majuscula, litera mica, cifra, non-alfanumeric)
- Session hijacking: token-urile expira dupa 3 ore si sunt invalidate la logout
- Accesul utilizatorilor neautorizati la resurse restrictionate: endpoint-urile respective pot fi accesate doar de un utilizator cu rol de admin, un utilizator normal nu poate dobandi rol de admin decat daca este promovat de un alt admin
- Sql injection: am utilizat orm-ul Entity Framework pentru a interactiona cu baza de date, nu scriem sql
- Expunere a datelor personale: folosit https pentru a cripta datele transferate