# Testrapport av Secureme CRM-system

Här sammanfattas resultaten för testningen av appen Secureme, ett CRM-system med primär funktionalitet mot kundärendehantering. För tydlighetens skull har jag delat upp varje avsnitt i tre underkategorier baserade på vilken typ av testning som är gjord. För samtliga detaljer se kalkylarket Testplanering\_Testfall.xlsx.

## Genomförda tester

### API-tester

Inom API-testningen genomfördes 16, vilket motsvarar samtliga endpoints. Testresultatet av dessa fördelade sig enligt nedan:

* Utan anmärkning: 4
* Med behov av refaktorering/bugg: 4
* Innehållande säkerhetsbrister: 8

Däremot fungerade den grundläggande funktionaliteten i alla API som förväntat. För samtliga API saknas DTO (Data Transfer Object) och i många fall skickas en hel klass med data till frontend. I ett fåtal fall finns ett anpassat objekt i returen.

### Enhetstester

### Gränssnittstestning

## Resultat

## Identifierade buggar och säkerhetsbrister

Vid testningen saknades restriktioner på API-endpoints, vilket gör att samtliga endpoints går att komma åt utan att vara inloggad

## Rekommendationer och reflektioner

Saknad funktionalitet i appen: API som sätter ärendehandläggare på ett ärende, skalbarhet till flera företag, eftersom databasen och därmed backend har byggt kategorier baserat på enum, vilka är svårare att anpassa till andra typer av företag. Hantera meddelandeavsändare genom session istället för komponenter i frontend. Säkerhetsperspektiv: Sätta fler checkar både i backend och frontend, så att t.ex. en inaktiv medarbetare inte kan logga in.

Enhetlighet i namnkonventioner, exempelvis namngivning av klassvariabler.

Saknad funktionalitet i backend: DTO för att hantera vilken data som skickas till frontend.

Saknad funktionalitet i frontend: Inloggningshantering

Lärdomar som jag drar av att testa ett system är flera men primärt att i en funktionalitet tänka ur fler perspektiv, inte bara att något ska fungera utan att det måste finnas ett säkerhetsperspektiv på flera nivåer: Vilken data är tillgänglig och för vem? Hur mycket data behövs för att frontend ska fungera? Vilken data returneras när en API-endpoint är lyckad?