Sikkerhetskrav

- Systemet skal benytte https
- En bruker/angriper skal ikke kunne laste opp noe annet enn png/jpg filer som profilbilde
- Systemet skal ikke kjøre filer av feil filtype som er blitt lastet opp som bilder
- En bruker/angriper skal ikke kunne starte reset passord prosessen mer enn X ganger i timen
- En angriper skal ikke kunne gjennomføre DoS på loggsystemet
- En bruker/angriper skal ikke kunne sende kommentarer mer enn X ganger i timen
- En angriper skal ikke kunne finne PIN-kode til gjesteside gjennom bruteforce
    - En bruker/angriper skal ikke kunne skrive feil PIN-kode mer enn X ganger i timen
- Systemet skal være beskyttet mot SQL-injections ved å validere og sanitere all brukerinput brukt til SQL-setninger
- Systemet skal ha ulike brukere med begrensede brukerprivileger i databasen
- Systemet skal ha en sentral logg med oversikt over hele systemet

Abuse Cases

- En angriper lager et script som går gjennom alle 4-sifrede tall og tester de mot gjestesiden for å finne PIN-kodene
- En angriper lager en php-fil med .png ending og oppretter en bruker med filen som profilbilde
- En angriper avlytter PIN-koder og brukeropplysninger som går gjennom åpen http-trafikk
- En angriper bruker et script for å spamme reset passord funksjonen på en mengde epost-adresser
- En angriper som har fått seg inn på en emne-side bruker et script for å spamme kommentarer