Risikovurdering av prosjektet Ung-økonom

Denne vurderingen identifiserer de mest relevante truslene som kan påvirke prototypen vår Ung-økonom, og foreslår tiltak for å redusere disse risikoene. Selv om løsningen ikke behandler sensitive personopplysninger, håndterer den brukerdata, økonomiske beregninger og en enkel innloggingsfunksjon. Derfor må prototypen være solid nok til å forhindre feil og misbruk, samtidig som sikkerhetsnivået tilpasses prosjektets omfang og kompleksitet.

Relevante risikoer og trusler

Risikoer / trusler	Beskrivelse
Uautorisert tilgang til brukerdata	Kan oppstå dersom innlogging eller database ikke sikres tilstrekkelig.
Lekkasje av passord pga. manglende hashing	Kan oppstå dersom passord lagres i klartekst uten hashing.
Manglende kryptering (HTTP i stedet for HTTPS)	Trafikk kan avlyttes eller manipuleres dersom siden hostes uten HTTPS.
Enkle input-angrep som XSS eller SQL Injection	Kan bli et problem dersom brukerinput ikke valideres, eller hvis databasen bruker spørringer uten parameterisering.
Manipulering av input	Brukere kan legge inn ekstreme eller ugyldige verdier som fører til feil i beregningene.
Misforståelse av økonomiske tall og begrep	Brukere kan feiltolke tall eller begreper dersom informasjonen presenteres uklart eller uten forklaring.

Det totale risikonivået

Risiko	Sannsynlighet	Impact	Risikonivå (S x I)
Uautorisert tilgang til brukerdata	Lav (1)	Moderat (2)	Lav (2)
Lekkasje av passord	Moderat(2)	Høy (3)	Høy (6)
Input-angrep som XSS eller SQL Injection	Moderat (2)	Moderat (2)	Moderat (4)
Manglende kryptering	Moderat (2)	Moderat (2)	Moderat (4)
Manipulering av input	Høy (3)	Lav (1)	Moderat (3)
Misforståelse av økonomiske tall og begrep	Moderat (2)	Lav (1)	Lav (2)

Det ble brukt en risikomatrise fra AuditBoard (2024) for å identifisere og rangere risikonivået.

Figur 1 Risikomatrise hentet fra AuditBoard (2024).

Tiltak som kan implementeres

Uautorisert tilgang til brukerdata

- Sørg for at brukere kun får tilgang til sine egne data, ingen åpne eller delte endepunkt.
- Unngå å lagre brukerdata i frontend.

Manglende kryptering

- Prototypen kan hostes på en tjeneste som automatisk bruker HTTPS (f.eks. GitHub Pages). Dette sikrer at all trafikk mellom bruker og løsning er kryptert uten ekstra konfigurasjon.

Lekkasje av passord

- Passord som lagres i databasen bør hashes før lagring, f.eks. med bcrypt. Unngå lagring av passord i klartekst under enhver omstendighet.
- Still krav om sterke passord (f.eks. minimum lengde, tall, store og små bokstaver)

Input-angrep som XSS eller SQL Injection

- Valider all brukerinput.
- Bruk parameteriserte spørringer i databasen for å hindre SQL Injection.

Manipulering av input

- Sett fornuftige maksimumsgrenser på tallfelter (eks: pris < 20 millioner, rente < 25 %, år < 50).
- Håndter feilinput med tydelige feilmeldinger slik at kalkulasjoner ikke krasjer eller gir rare resultater.

Misforståelse av økonomiske tall og begrep

- Gi korte forklaringer på økonomiske begrep.
- Bruk visuelle elementer som farger eller symboler for å gjøre resultatene lettere å tolke riktig.
- Ikke bruk kompliserte grafer uten forklaring, hold det forståelig.

Risikovurderingen fokuserer på funksjonene som inngår i prototypen. Målet er å identifisere realistiske trusler og tiltak som kan gjennomføres innenfor prosjektets omfang og tidsramme.

Referanseliste:

Vicente, V. (2024, 15. februar). Risk Assessment Matrix: Overview and Guid. Auditboard. https://auditboard.com/blog/what-is-a-risk-assessment-matrix