Delinnlevering 2   
Innlogging, databasemodell og administrators del av applikasjonen

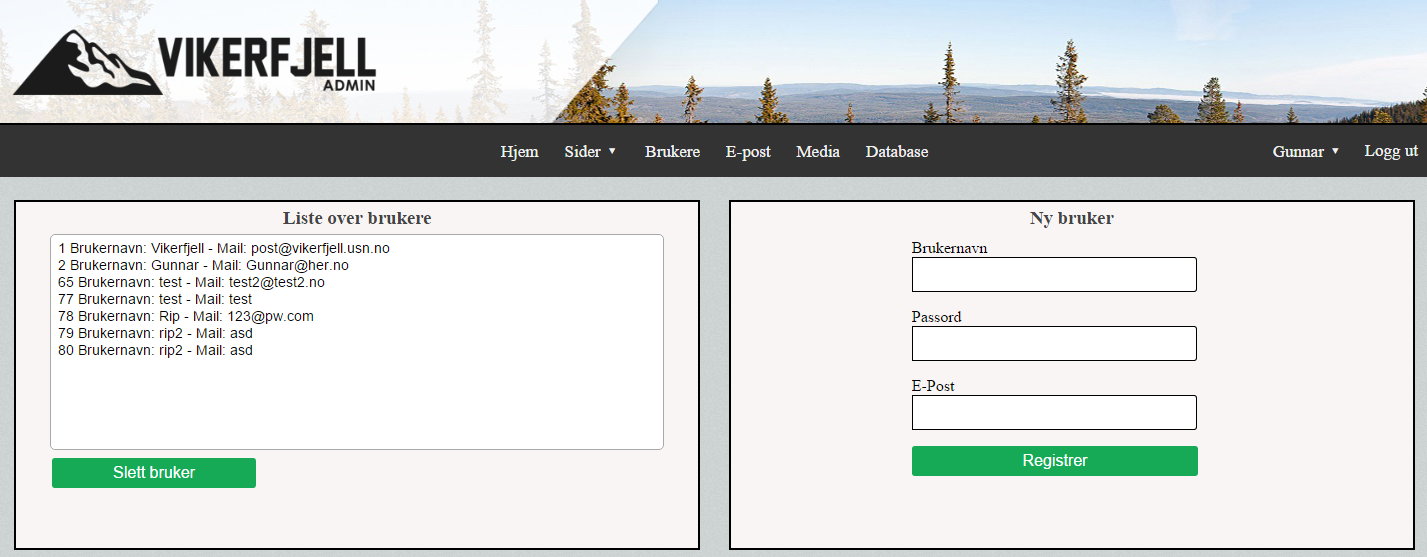
av Gruppe 5

**Utviklere Studentnummer E-post**

Alex Petterssen   
Erik Hellerslien  
Erlend Andreas Hall  
Sindre Østby

139953  
139964  
139960  
139936

alex1990pettersen@gmail.com  
erik\_hellerslien@hotmail.com  
erlendahall@gmail.com  
sindreoestby1@gmail.com



Innholdsfortegnelse

[Innledning 3](#_Toc476418935)

[Back-end 4](#_Toc476418936)

[Session 4](#_Toc476418937)

[Hashing 4](#_Toc476418938)

[Brukeradministrering 4](#_Toc476418939)

[Kobling mot MySQL 5](#_Toc476418940)

[Front-end 6](#_Toc476418941)

[Designendringer 6](#_Toc476418942)

[Forslag til ny datamodell 7](#_Toc476418943)

[Testing 8](#_Toc476418944)

[Kilder og vedlegg 9](#_Toc476418945)

## Innledning

For delinnlevering 2 har gruppe 5 gjort følgende:

* Designet en side for innlogging til back-end
* Designet en underside i back-end for å administrere brukere
* Mulighet for å legge inn nye brukere
* Innloggingsfunksjon og session
* Knapp for «glemt passord» funksjon
* Kobling mot MySQL
* Menybar-generering med PHP
* Passord hashing med SHA-1 og statisk salt
* Videre front-end design
* Egen fil med SQL setninger for meny-elementene.

I henhold til oppgaveteksten har vi oppfylt alle kriterier i delinnlevering 2. Vi har gått ut i fra at back-end ikke skal brukes på mobil med tanke på at dette ikke er en enhet som er vanlig å jobbe fra. Derfor har vi fokusert på at back-end skal kunne fungere på tablets og større skjermer. Det er fortsatt mulig å kunne logge på igjennom mobil, men brukeren vil kunne oppleve at noe ikke passer skjermen.

## Back-end

### Session

I denne delinnleveringen har vi brukt sessions til å føre variabler fra side til side. Dette har vært i bruk under innlogging og når brukeren er inne i selve administrasjonsdelen av nettsiden. Ved bruk av sessions kan vi passe på at ingen får tilgang til back-end med mindre brukeren er logget inn, det gjør at vi slipper at uvedkommende kommer inn i back-end. Vi har også brukt sessions når det kommer til «time out» på siden, etter 15 minutter inaktiv-tid blir brukeren kastet ut av back-end og er nødt til å logge på igjen.

### Hashing

Ved sending av passord mellom nettleser og database har vi valgt å ta i bruk krypteringen SHA1 og lagt til en salt, en blanding av dette vil generere en kryptering av passordet. Dette krypterte passordet blir lagret til databasen, noe som gjør at de som har tilgang til databasen ikke kan se passordet til brukerne i klartekst. Selve krypteringen skjer i PHP, f.eks. når en bruker logger inn bruker den sitt ordinære passord og PHP gjør om dette til krypteringen som gjelder for nettstedet. Det gjør at PHP kan sammenligne dette krypterte passordet som brukeren har skrevet inn og sammenligne dette med det som ligger i databasen.

### Brukeradministrering

Det vi har laget hittil på brukeradministrering er:

* Sletting av bruker
* Ny bruker
* Endre passord
* Glemt passord

Vi har laget en mulighet til å slette en bruker. Grunnen til at vi gjorde det er fordi vi tenker oss at det er mulig at personer som jobber med administrering av siden kan slutte eller lignende. Her sjekker vi også på BrukerID’en så adminbrukeren ikke kan bli slettet.

Ved laging av ny bruker sjekker vi at brukernavnet ikke finnes fra før av, så det ikke blir noen konflikt med innloggingen. Vi både salter og hasher passordet

Ved endring av passord krever vi først at brukeren skriver inn sitt gamle passord, og så det nye to ganger for å sjekke at det ikke blir skrevet noe feil. Dette igjen blir saltet og hashet.

Vi har laget en knapp for glemt passord. Funksjonen til denne så langt er bare at den sender en mail til den bestemte e-posten, men det vi mangler er at den sender passord.

### Kobling mot MySQL

Kobling mot MySQL gjøres der vi har behov for å hente informasjon fra databasen. Vi bruker det først og fremst ved innlogging. Som nevnt tidligere henter vi det krypterte passordet fra databasen og sammenligner dette med det brukere skriver inn, som blir saltet og hashet før sammenligningen. For å administrere brukere gjør vi spørringer til databasen og henter ut de brukerne som er laget under back-end og her har vi også mulighet til å slette brukere. Ved feil kombinasjon av brukernavn og passord, vil det bli lagt til en teller på det brukernavnet. Går den telleren over 5, vil den brukeren få en timeout på 15 minutter hvor det ikke er mulig med flere innloggingsforsøk. Det er også mulighet til å legge til nye brukere.

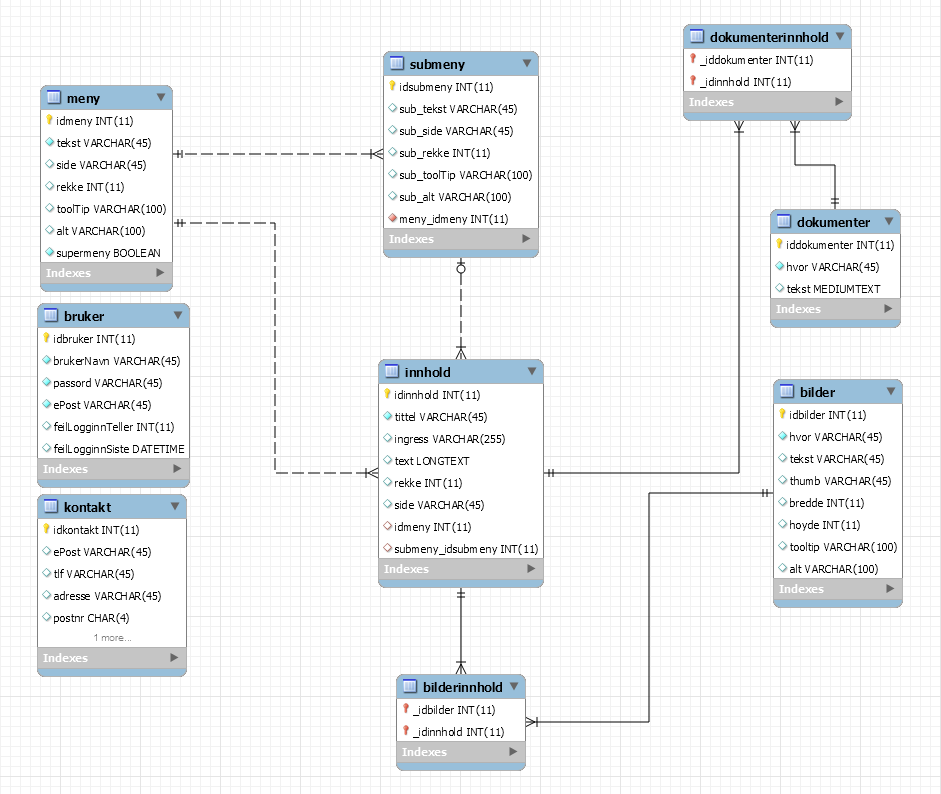
## Front-end

### Designendringer

Det er noen små endringer som har blitt gjort på front-end siden. Vi har blant annet endret alle bildene til bilder av Vikerfjell. Slideren er også endret, slik at brukeren selv kan bla fram og tilbake mellom bildene som er vist. Det er også satt en timer på slider-bildene, men denne blir fjernet når en bruker selv trykker på en av pilene. Det har også blitt gjort endringer på skalering på bildene, slik at de passer til forskjellige skjermoppløsninger. En vær-rapport har også blitt lagt til, men den er ikke helt ferdig med tanke på egenskaper for skalering til siden. Mangler å style den.

## Forslag til ny datamodell

Vi har gått inn for å ha nedtrekksmenyer i applikasjonen, men den eksisterende modellen tillater ikke dette. Modellen tillater heller ikke sideinnhold som ikke er navigerbar fra menybaren. (Det er en sterk relasjon mellom tabellene innhold og meny)



Løsningen med nedtrekksmenyer demonstrerer at datamodellen fungerer i praksis, men en svakhet er at tabellen «innhold» vil få en del nullmerker på fremmednøkkelen «submeny\_idsubmeny»

## Testing

## Kilder og vedlegg

**Include**

Vi har noen forskjellige filer og nivåer for henting av disse.  
Helt bakerst i en egen include mappe har vi:

* Mysqlcon.php
* Meny.php
* Header.php
* Glemtpassordsend.php
* Listebruker.php
* Weather.php

Disse har vi valgt å ha i egen egen mappe da disse ikke krever å hente noen filer bakover i mappesystemet.

I PHP mappen har vi:

* Startsession.php

Denne hadde vi ikke mulighet til å legge i include mapppen da denne krever en fil som ville da ligget bakover et nivå.

**Session variabler**

* LastActivity:
  + «LastActivity» brukes til å holde på tiden på den siste utførte aktiviteten.
* Name:
  + «Name» brukes til å vise hvem som er logget inn på de forskjellige sidene.
* UserID:
  + «UserID» er for å kunne spare på bruker ID. Denne kan brukes til å identifisere hvem som har gjort hva i databasen. F.eks. om noen lager en bruker så kan man sette bruker id fra den som lagde brukern som FK på den nye brukeren.