Review van
Mick Bosman's code

Diaquiño Fortmeier

Database connectie
Ze gebruiken PDO en een 'Try catch' om de connectie vast te leggen.

CMS
Register
Er worden verschillende checks gebruikt zoals:

- Het checken of alle velden ingevuld zijn en daarna of de velden niet leeg gelaten zijn.
- Het checken of de email juist is met FILTER_VALIDATE_EMAIL.
- Een preg_match() check op de gebruikersnaam die alleen kleine letters, hoofdletters en nummers doorlaat.
- Een lengte check die kijkt of het wachtwoord minimaal 5 tekens heeft en niet langer dan 20 is.
- Een preg_match() check voor het wachtwoord die hetzelfde toelaat als de gebruikersnaam.
- Kijkt of het wachtwoord hetzelfde is als het 'herhaal wachtwoord' veld.
- Kijkt of de gebruikersnaam al bestaat.
- Het wachtwoord hashen met password_hash().

Nadat alle checks goed zijn gekeurd en de user de database ingestuurd is sturen ze een verificatie link naar het geregistreerde email voor een laatste authenticatie check.

Login
Als de gebruiker al ingelogd is word hij naar home pagina gestuurd ook als er cookies voor 'remember me' zijn wordt de gebruiker naar de home pagina gestuurd.

Ze hebben ook een anti brute force functie die ervoor zorgt dat een ip maar 5 kansen heeft om in te loggen, als alle 5 kansen gebruikt zijn moet de gebruiker één dag wachten om het opnieuw te proberen.

Het is voor mij niet duidelijk waar de login functie zelf staat.

Upload
Op het moment van deze review is er nog geen beveiliging voor het uploaden van posts.

Conclusie

Ze zijn duidelijk bezig met het nadenken over de veiligheid van hun website en dat is goed te zien met hoeveel checks ze doen in hun code.

Wat ik wel jammer vond, was dat ik de login functie niet had gevonden en dat er nog geen beveiliging was voor de upload functie.